Chapter 1

Preface

These are the lecture notes for the class MTH 818 which I’m currently teaching at Michigan State University. The text book used for this class is Hungerford’ Algebra [Hun]. Much of the contents follows Hungerford’s book but the proofs given here often diverge from Hungerford’s.
# Contents

1. **Preface** 3

2. **Group Theory** 7
   2.1 Latin Squares ........................................... 7
   2.2 Semigroups, monoids and groups ............................ 9
   2.3 The projective plane of order 2 ............................ 14
   2.4 Subgroups, cosets and counting ............................ 15
   2.5 Normal subgroups and the isomorphism theorem .......... 17
   2.6 Cyclic groups ............................................. 22
   2.7 Simplicity of the alternating groups ........................ 23
   2.8 Direct products and direct sums ............................ 28
   2.9 Free products ............................................ 33
   2.10 Group Actions ............................................ 41
   2.11 Sylow $p$-subgroup ...................................... 47

3. **Rings** 53
   3.1 Rings ..................................................... 53
   3.2 Ideals and homomorphisms .................................. 60
   3.3 Factorizations in commutative rings ........................ 66
   3.4 Localization .............................................. 74
   3.5 Polynomials rings, power series and free rings .......... 80
   3.6 Factorizations in polynomial rings ........................ 85

4. **Modules** 93
   4.1 Modules and Homomorphism ................................ 93
   4.2 Exact Sequences .......................................... 97
   4.3 Projective and injective modules .......................... 101
   4.4 The Functor Hom .......................................... 109
   4.5 Tensor products .......................................... 113
   4.6 Free modules and torsion modules ........................ 120
   4.7 Modules over PID’s ....................................... 124
   4.8 Composition series ....................................... 128
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.9</td>
<td>Matrices</td>
<td>136</td>
</tr>
<tr>
<td>5</td>
<td>Fields</td>
<td>143</td>
</tr>
<tr>
<td>5.1</td>
<td>Extensions</td>
<td>143</td>
</tr>
<tr>
<td>5.2</td>
<td>Splitting fields, Normal Extensions and Separable Extensions</td>
<td>148</td>
</tr>
<tr>
<td>5.3</td>
<td>Galois Theory</td>
<td>155</td>
</tr>
<tr>
<td>5.4</td>
<td>The Fundamental Theorem of Algebra</td>
<td>161</td>
</tr>
<tr>
<td>5.5</td>
<td>Finite Fields</td>
<td>163</td>
</tr>
<tr>
<td>5.6</td>
<td>Transcendence Basis</td>
<td>164</td>
</tr>
<tr>
<td>5.7</td>
<td>Algebraically Closed Fields</td>
<td>167</td>
</tr>
<tr>
<td>6</td>
<td>Multilinear Algebra</td>
<td>171</td>
</tr>
<tr>
<td>6.1</td>
<td>Multilinear functions and Tensor products</td>
<td>171</td>
</tr>
<tr>
<td>6.2</td>
<td>Symmetric and Exterior Powers</td>
<td>178</td>
</tr>
<tr>
<td>6.3</td>
<td>Determinants and the Cayley-Hamilton Theorem</td>
<td>186</td>
</tr>
<tr>
<td>7</td>
<td>Hilbert’s Nullstellensatz</td>
<td>197</td>
</tr>
<tr>
<td>7.1</td>
<td>Ring Extensions</td>
<td>197</td>
</tr>
<tr>
<td>7.2</td>
<td>Going Up and Down</td>
<td>199</td>
</tr>
<tr>
<td>7.3</td>
<td>Noether’s Normalization Lemma</td>
<td>202</td>
</tr>
<tr>
<td>7.4</td>
<td>Affine Varieties</td>
<td>204</td>
</tr>
<tr>
<td>A</td>
<td>Zorn’s Lemma</td>
<td>207</td>
</tr>
<tr>
<td>B</td>
<td>Categories</td>
<td>213</td>
</tr>
</tbody>
</table>
Chapter 2

Group Theory

2.1 Latin Squares

Definition 2.1.1 Let $G$ be a set and $\phi : G \times G \to G$ a map.

(a) $\phi$ is called a binary operation on $G$. We write $ab$ for $\phi(a, b)$. $(G, \phi)$ is called a pre-group.

(b) $e \in G$ is called an identity element if $ea = ae = a$ for all $a \in G$.

(c) We say that $(G, \phi)$ is a Latin square if for all $a, b$ in $G$ there exist unique elements $x, y$ in $G$ so that

$$ax = b \text{ and } ya = b$$

(d) The multiplication table of $(G, \phi)$ is the matrix $(ab)_{a \in G, b \in G}$.

(e) The order of $(G, \phi)$ is the cardinality $|G|$ of $G$.

We remark that $(G, \phi)$ is a Latin square if and only if each $a \in G$ appears exactly once in each row and in each column of the multiplication table. If there is no confusion about the binary operation in mind, we will just write $G$ for $(G, \phi)$ and call $G$ a pre-group.

Definition 2.1.2 Let $G$ and $H$ be pre-groups and $\alpha : G \to H$ a map.

(a) $\alpha$ is called a (pre-group) homomorphism if $\alpha(ab) = \alpha(a)\alpha(b)$, for all $a, b \in G$.

(b) $\alpha$ is called an isomorphism if $\alpha$ is a homomorphism and there exists a homomorphism $\beta : H \to G$ with $\alpha\beta = \text{id}_H$ and $\beta\alpha = \text{id}_G$.

(c) $\alpha$ is an automorphism if $G = H$ and $\alpha$ is an isomorphism.
Let $G$ be a pre-group. The opposite pre-group $G^{\text{op}}$ is defined by $G^{\text{op}} = G$ has a set and $$g \cdot_{\text{op}} h = hg.$$ Let $G$ and $H$ be pre-groups. An pre-group anti homomorphism $\alpha : G \to H^{\text{op}}$ is a pre-group homomorphism $\alpha : G \to H^{\text{op}}$. So $\alpha(ab) = \alpha(b)\alpha(a)$.

**Lemma 2.1.3 [basicbinary]**

(a) Let $G$ be a pre-group. Then $G$ has at most one identity.

(b) Let $\alpha : G \to H$ be a pre-group homomorphism. Then $\alpha$ is a isomorphism if and only if $\alpha$ is a bijection.

**Proof:** (a) Let $e$ and $e^*$ be identities. Then $$e = ee^* = e^*$$

(b) Clearly any isomorphism is a bijection. Conversely, assume $\alpha$ is a bijection and let $\beta$ be its inverse map. We need to show that $\beta$ is an homomorphism. For this let $a, b \in H$.

Then as $\alpha$ is a homomorphism $$\alpha(\beta(a)\alpha(b)) = \alpha(\beta(a))\alpha(\beta(b)) = ab = \alpha(\beta(ab)).$$ Since $\alpha$ is one to one ( or by applying $\beta$) we get $$\beta(a)\beta(b).$$ So $\beta$ is an homomorphism. \[ \square \]

Below we list ( up to isomorphism) all Latin square of order at most 5 which have an identity element $e$. It is fairly straightforward to obtain this list ( although the case $|G| = 5$ is rather tedious). We leave the details to the reader, but indicate a case division which leads to the various Latin squares.

Order 1, 2 and 3:

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>e</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>e</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td>e</td>
<td>a</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>e</td>
<td>e</td>
<td>e</td>
</tr>
</tbody>
</table>

Order 4 Here we get two non-isomorphic Latin squares. One for the case that $a^2 \neq e$ for some $a \in G$ and one for the case that $a^2 = e$ for all $a \in G$.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>(2)</td>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>
2.2. SEMIGROUPS, MONOIDS AND GROUPS

Order 5 This time we get lots of cases:
Case 1: There exists \( e \neq a \neq b \) with \( a^2 = e = b^2 \).
Case 2 There exists \( e \neq a \) with \( a^2 \neq e, aa^2 = e \) and \((a^2a)^2 = e\).
Case 3 There exists \( e \neq a \) with \( a^2 \neq e, aa^2 = e \) and \((a^2a)^2 \neq e\).
Case 4 There exists \( e \neq a \) with \( a^2 \neq e, a^2a = e \) and \((aa^2)^2 = e\).

This Latin square is anti-isomorphic but not isomorphic to the one in case 2. Anti-isomorphic means that there exists bijection \( \alpha \) with \( \alpha(ab) = \alpha(b)\alpha(a) \).

Case 5 There exists \( e \neq a \) with \( a^2 \neq e, aa^2 = e \) and \((a^2)^2 \neq e\).

Case 6 There exists \( e \neq a \) with \( a^2 \neq e, a^2a = e \) and \((a^2)^2 \neq e\).

This Latin square is isomorphic and anti-isomorphic to the one in Case 3.

Case 7 There exists \( e \neq a \) with \( a^2 \neq e, a^2a = e \).
Case 8 There exists \( e \neq a \) with \( (a^2)^2 \neq e \).

In this case put \( c = aa^2 \). Then \( c^2 \neq e \) and either \( cc^2 = e \) or \( c^2c = e \). Moreover \((c^2c)^2 \neq e\) respectively \((cc^2)^2 \neq e\) and the Latin square is isomorphic to the one in Case 3.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
<td>d</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

(1)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>d</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>e</td>
<td>c</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

(2)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
</tbody>
</table>

(3)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>e</td>
<td>c</td>
<td>a</td>
<td>b</td>
</tr>
</tbody>
</table>

(4)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>e</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>d</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

(5)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>e</td>
<td>d</td>
<td>a</td>
<td>c</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

(6)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

(7)

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>d</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>e</td>
<td>d</td>
<td>b</td>
<td>a</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>e</td>
<td>y</td>
<td>x</td>
<td>c</td>
</tr>
</tbody>
</table>

(8)

\{x, y\} = \{a, b\}

2.2 Semigroups, monoids and groups

[smg]

Definition 2.2.1 Let \( G \) be a pre-group.

(a) The binary operation on \( G \) is called associative if

\[(ab)c = a(bc)\]

for all \( a, b, c \in G \). If this is the case we call \( G \) a semigroup.

(b) \( G \) is a monoid if it is a semigroup and has an identity.
(c) Suppose that $G$ is a monoid. Then $a \in G$ is called invertible if there exists $a^{-1} \in G$ with

$$aa^{-1} = e = a^{-1}a.$$  

Such an $a^{-1}$ is called an inverse of $a$.

(d) A group is a monoid in which every element is invertible.

(e) $G$ is called abelian (or commutative) if

$$ab = ba$$

for all $a, b \in G$.

Examples: Let $\mathbb{Z}^+$ denote the positive integers and $\mathbb{N}$ the non-negative integers. Then $(\mathbb{Z}^+, +)$ is a semigroup, $(\mathbb{N}, +)$ is a monoid and $(\mathbb{Z}, +)$ is a group. $(\mathbb{Z}, \cdot)$ and $(\mathbb{R}, \cdot)$ are monoids. Let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Then $(\mathbb{R}^*, \cdot)$ is a group. The integers modulo $n$ under addition is another example. We denote this group by $(\mathbb{Z}/n\mathbb{Z}, +)$. All the examples so far have been abelian.

Note that in a group $a^{-1}b$ is the unique solution of $ax = b$ and $ba^{-1}$ is the unique solution of $ya = b$. So every group is a Latin square with identity. The converse is not true. Indeed of the Latin squares listed in section 2.1 all the once or order less than five are groups. But of Latin squares of order five only the one labeled (6) is a group.

Let $\mathbb{K}$ be a field and $V$ a vector space over $\mathbb{V}$. Let $\text{End}_\mathbb{K}(V)$ the set of all $\mathbb{K}$-linear maps from $V$ to $V$. Then $\text{End}_\mathbb{K}(V)$ is a monoid under compositions. Let $\text{GL}_\mathbb{K}(V)$ be the set of $\mathbb{K}$-linear bijection from $V$ to $V$. Then $\text{GL}_\mathbb{K}(V)$ is a group under composition, called the general linear group of $V$. It is easy to verify that $\text{GL}_\mathbb{K}(V)$ is not abelian unless $V$ has dimension 0 or 1.

Let $I$ be a set. Then the set $\text{Sym}(I)$ of all bijection from $I$ be $I$ is a group under composition, called the symmetric group on $I$. If $I = \{1, \ldots, n\}$ we also write $\text{Sym}(n)$ for $\text{Sym}(I)$. $\text{Sym}(n)$ is called the symmetric group of degree $n$. $\text{Sym}(I)$ is not abelian as long as $I$ has at least three elements.

Above we obtained various examples of groups by starting with a monoid and then considered only the invertible elements. This works in general:

**Lemma 2.2.2** [basicmonoid] Let $G$ be a monoid.

(a) Suppose that $a, b, c \in G$, $a$ is a left inverse of $b$ and $c$ is right inverse of $b$. Then $a = c$ and $a$ is an inverse.

(b) An element in $G$ has an inverse if and only if it has a left inverse and a right inverse.

(c) Each element in $G$ has at most one inverse.

(d) If $x$ and $y$ are invertible, then $x^{-1}$ and $xy$ are invertible. Namely $x$ is an inverse of $x^{-1}$ and $y^{-1}x^{-1}$ is an inverse of $xy$. 

(e) Let $G^*$ be the set of invertible elements in $G$, then $G^*$ is a group.

**Proof:**

(a) 
$$ a = ae = a(bc) = (ab)c = ec = c $$

(b) and (c) follow immediately from (a).

(d) Clearly $x$ is an inverse of $x^{-1}$. Also 
$$ (y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}xy) = y^{-1}((x^{-1}x)y) = y^{-1}(ey) = y^{-1}y = e $$

Similarly $(xy)(y^{-1}x^{-1}) = e$ and so $y^{-1}x^{-1}$ is indeed an inverse for $xy$.

(e) By (d) we can restrict the binary operation $G \times G \to G$ to get a binary operation $G^* \times G^* \to G^*$. Clearly this is associative. Also $e \in G^*$ so $G^*$ is a monoid. By (d) $x^{-1} \in G^*$ for all $x \in G^*$ and so $G^*$ is a group. \qed

Every group $G$ is isomorphic to its opposite group $G^{\text{op}}$. Indeed the map $x \to x^{-1}$ is an anti-automorphism of $G$ and an isomorphism $G \to G^{\text{op}}$.

The associative law says that $(ab)c = (ab)c$ for all $a, b, c$ is a semigroup. Hence also 
$$ (a(bc))d = ((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d) $$

for all $a, b, c, d$ in $G$. That is for building products of four elements in a given order it does not matter how we place the parenthesis. We will show that this is true for products of arbitrary length. The tough part is to define what we really mean with a product of $(a_1, \ldots, a_n)$ where $a_i \in G$ for some pre-group $G$. We do this by induction on $n$.

For $n = 1$, $a_1$ is the only product of $(a_1)$.

For $n \geq 2$, $z$ is a product of $(a_1, \ldots, a_n)$ if and only if $z = xy$, where $x$ is a product of $(a_1, \ldots, a_m)$ and $y$ is a product of $(a_{m+1} \ldots a_n)$, for some $1 < m < n$.

The only product of $(a_1, a_2)$ is $a_1a_2$. The products of $(a_1, a_2, a_3)$ are $(a_1a_2)a_3$ and $a_1(a_2a_3)$. Associativity now just says that every 3-tuple as a unique product.

For later use, if $G$ has an identity we define $e$ to be the only product of the empty tuple.

For the proof of next theorem we also define the standard product of $(a_1, \ldots, a_n)$. For $n = 1$ this is $a_1$ while for $n \geq 2$ it is $xa_n$ where $x$ is the standard product of $(a_1, \ldots, a_{n-1})$.

**Theorem 2.2.3 (General Associativity Law)** Let $G$ be a semigroup. Then any (non-empty) tuple of elements has a unique product.

**Proof:** By induction on the length $n$ of the tuple. For $n = 1$ or 2 there is nothing to prove. So suppose $n \geq 3$. We will show that any product $z$ of $(a_1, \ldots, a_n)$ is the standard product. By definition of $z$, $z = xy$ where $x$ is product of $(a_1, \ldots, a_m)$ and $y$ is a product of $(a_{m+1}, \ldots, a_n)$.

Suppose first that $m = n - 1$. By induction $x$ is the standard product of $(a_1, \ldots, a_{n-1})$. Also $z = xa_n$ and so by definition $z$ is the standard product.
Suppose next that \( m < n - 1 \). Again by induction \( y \) is the standard product of \((a_{m+1}, \ldots, a_n)\) and so \( y = sa_n \) where \( s \) is the standard product of \((a_{m+1}, \ldots, a_{n-1})\). Hence

\[
z = xy = x(sa_n) = (xs)a_n
\]

As \( xs \) is a product of \((a_1, \ldots, a_{n-1})\), we are done by the \( m = n - 1 \) case. \( \square \)

One of the most common ways to define a group is as the group of automorphism of some object. For example above we used sets and vector spaces to define the symmetric groups and the general linear group.

If the object is a pre-group \( G \) we get a group which we denote by \( \text{Aut}(G) \). So \( \text{Aut}(G) \) is the set of all automorphisms of the pre-group \( G \). The binary operation on \( \text{Aut}(G) \) is the composition.

We will determine the automorphism for the Latin squares in 2.1. As the identity element is unique it is fixed by any automorphism. It follows that the Latin square of order 1 or 2, have no non-trivial automorphism (any structure as the trivial automorphism which sends every element to itself).

The Latin square of order three has one non-trivial automorphism. It sends

\[
e \to e \quad a \to b \quad b \to a.
\]

Consider the first Latin square of order 4. It has two elements with \( x^2 = 2e \), namely \( a \) and \( c \). So again we have a unique non-trivial automorphism:

\[
e \to e \quad a \to c \quad b \to b \quad c \to a.
\]

Consider the second Latin square of order 4. Here is an easy way to describe the multiplication: \( ex = x, xx = e \) and \( xy = z \) if \( \{x, y, z\} = \{a, b, c\} \). It follows that any permutation of \( \{e, a, b, c\} \) which fixes \( e \) is an automorphism. Hence the group of automorphism is isomorphic to \( \text{Sym}(3) \),

Consider the Latin square of order 5 labeled (1). The multiplication table was uniquely determine by any pair \( x \neq y \) of non-trivial elements with \( x^2 = y^2 = e \). But \( x^2 = e \) for all \( x \). So every \( e \neq x \neq y \neq e \) there exists a unique automorphism with

\[
a \to x \quad b \to y
\]

Thus the group of automorphisms has order 12. The reader might convince herself that also the set of bijection which are automorphisms or anti-automorphisms form a group. In this case it has order 24. That is any bijection fixing \( e \) is an automorphism or anti-automorphism.

Consider the Latin square of order five labeled (2). This multiplication table is uniquely determine by any element with \( x^2 \neq e, xx^2 = e \) and \( (x^2x)^2 = e \). \( a, b \) and \( d \) have this property and we get two non-trivial automorphism:

\[
e \to e, a \to b \quad b \to d, \quad c \to c \quad d \to a \quad \text{and} \quad e \to e, a \to d \quad b \to a, \quad c \to c \quad d \to b
\]
That is any permutation fixing $e$ and $c$ and cyclicly permuting $a, b, d$ is an automorphism. Consider the Latin square of order five labeled (3). This time only $a$ itself has the defining property. It follows that no non-trivial automorphism exists. But it has an anti-isomorphism fixing $a, b$ and $d$ and interchanging $a$ and $c$.

The Latin square (4) and (5) had been (anti-)isomorphic to (2) and (3). So consider (6). All non-trivial elements have the defining property. So there are 4 automorphisms. They fix $e$ and cyclicly permute $(a, b, c, d)$.

Finally consider the Latin square (7). Here $a, c, d$ have the defining property. So there are 3 automorphism. They fix $e$ and $b$ and cyclicly permuted $(a, c, d)$. Here all bijections fixing $a$ and $b$ are automorphism or anti-automorphism.

It might be interesting to look back and consider the isomorphism types of the groups we found as automorphism of Latin squares. $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4$, Sym(3) and a group of order 12. We will later see that Sym(4) has a unique subgroup of order 12 called Alt(4). So the group of order 12 must be isomorphic to Alt(4).

Another class of objects one can use are graphs. We define a graph to be a tuple $(\Gamma, -)$, where $\Gamma$ is a set and " - " is an anti-reflexive, symmetric relation on $\Gamma$. The elements are called vertices. If $a$ and $b$ are vertices with $a - b$ we say that $a$ and $b$ are adjacent. An edge is a pair of adjacent vertices. An automorphism of the graph $\Gamma$ is an bijection $\alpha \in \text{Sym}(\Gamma)$ such that $a - b$ if and only if $\alpha(a) - \alpha(b)$. In other words a bijection which maps edges to edges. Aut($\Gamma$) is the set of all automorphisms of $\Gamma$ under composition.

As an example let $\Gamma_4$ be a square:

![Graph](image)

The square has the following automorphisms: rotations by 0, 90, 180 and 270 degrees, and reflections on each of the four dotted lines. So Aut($\Gamma_4$) has order 8.

To describe Aut($\Gamma_4$) as a subset of Sym(4) we introduce the cycle notation for elements of Sym($I$) for a finite set $I$. We say that $\pi \in \text{Sym}(I)$ is a cycle of length if the exists $a_1 \ldots a_m \in I$ such that

$$\pi(a_1) = a_2, \pi(a_2) = a_3, \ldots, \pi(a_{m-1}) = a_m, \pi(a_m) = a_1$$

and $\pi(j) = j$ for all other $j \in I$.

Such a cycle will be denoted by

$$(a_1a_2a_3 \ldots a_m)$$

The set $\{a_1, \ldots a_m\}$ is called the support of the cycle. Two cycles are called disjoint if their supports are disjoint.
It is clear that every permutations can be uniquely written as a product of disjoint cycle.

\[ \pi = (a_1^1 a_2^1 \ldots a_{m_1}^1) (a_1^2 a_2^2 \ldots a_{m_2}^2) \ldots (a_1^k a_2^k \ldots a_{m_k}^k) \]

One should notice here that disjoint cycles commute and so the order of multiplication is irrelevant. Often we will not list the cycles of length 1.

So \((135)(26)\) is the permutation which sends 1 to 3, 3 to 5, 5 to 1, 2 to 6, 6 to 2 and fixes 4 and any number larger than 6.

With this notation we can explicitly list the elements of \(\text{Aut}(\Gamma_4)\):

The four rotations: \(e, (1234), (13)(24), (1432)\)
And the four reflections: \((14)(23), (13), (12)(34), (24)\).

### 2.3 The projective plane of order 2

In this section we will look at the automorphism group of the projective plane of order two.

To define a projective plane consider a 3-tuple \(E = (P, L, R)\) where \(P\) and \(L\) are non-empty sets and \(R \subseteq P \times R\). The elements of \(P\) are called points, the elements of \(L\) are called lines and we say a point \(P\) and a line \(l\) are incident if \((P, l) \in R\). \(E\) is called a projective plane if it has they following two properties

\[ \text{(PP1)} \quad \text{Any two distinct points are incident with a unique common line.} \]

\[ \text{(PP2)} \quad \text{Any two distinct lines are incident with unique common point.} \]

We say that a projective plane has order two if every point is incident with exactly three lines and every line is incident with exactly three points. Before studying the automorphism group will need to establish some facts about projective planes of order two.

Let \(P\) be any points. Then any other point lies on exactly one of the three lines through \(P\). Each of whose three lines has 2 points besides \(P\) and so we have \(1 + 3 \cdot 2 = 7\) points. By symmetry we also have seven lines.

A sets of points is called collinear if they points in the set are incident with a common line.

Now let \(A, B, C\) be any three points which are not collinear. We will show that the whole projective plane can be uniquely described in terms of the tuple \((A, B, C)\). Given two distinct points \(P\) and \(Q\), let \(PQ\) be the line incident to \(P\) and \(Q\). Also let \(P + Q\) be the unique point on \(PQ\) distinct from \(P\) and \(Q\). Since two distinct lines have exactly on point in common, \(A, B, C, A + B, A + C, B + C\) are pairwise distinct. Also the two lines \(A(B + C)\) and \(B(A + C)\) have a point in common and this point is not one of the six points we already found. Hence they intersect in \(A + (B + C) = B + (A + C) = C + (A + B)\), the seventh and last point.

Also \(AB, AC, BC, A(B + C), B(A + C), C(A + B)\) are six pairwise distinct lines.

Now \((A + B)(A + C)\) must intersect \(BC\). But \(B\) does not lie on \((A + B)(A + C)\) since otherwise \((A + B)(A + C) = (A + B)B = AB\). Similar \(C\) is not on \((A + B)(A + C)\). So
(B + C) lies on (A + B)(A + C) and B + C = (A + B) + (A + C) So the seventh line is incident with A + B, A + C and B + C. So we completely determined the projective plane:

An automorphism of E is a pair (α, β) ∈ Sym(P) × Sym(L) such that for each point P and each line l, P and l are incident if and only if α(P) and β(l) are incident. Clearly β is uniquely determined by α (namely if l = PQ then β(l) = α(P)α(Q)) and (after identifying a line with the set of incident points) an automorphism of the plane is just a permutation of the points which sends lines to lines.

Let Aut(E) be the set of automorphisms of E. Then Aut(E) is a group under composition.

Let ˜A, ˜B, ˜C be three non-collinear points. Its clear from the above that there exists a unique automorphism of E with

\[ A \to ˜A, \quad B \to ˜B, \quad C \to ˜C. \]

Now ˜A can be any one of the seven points, ˜B is any of the six points different from ˜A and ˜C is any of the four points not incident to ˜AB. Thus

\[ |Aut(E)| = 7 \cdot 6 \cdot 4 = 168.\]

We finish this section with a look at the operation + we have introduced on the points. Let G = \{e\} ∪ P. Here e is an arbitrary element not in P. Define a binary operation on G as follows:

\[ e + g = g + e, \quad P + P = e \]

and for distinct points P and Q, P + Q is as above.

It is easy to check that G is a group. Also the points correspond to the subgroup of order 2 in G and the lines to the subgroups of order 4. In particular there is an obvious isomorphism between Aut(E) and Aut(G).

### 2.4 Subgroups, cosets and counting

**Definition 2.4.1 [defsubgroup]** Let G be a group and H ⊆ G. We say that H is a subgroup of G and write H ≤ G if
(a) $e \in H$

(b) $H$ is closed under multiplication, that is for all $a, b \in H$, $ab \in H$

(c) $H$ is closed under inverses, that is for all $a \in H$, $a^{-1} \in H$.

Note that any subgroup of $G$ is itself a group, where the binary operation is given by restricting the one on $G$. We leave it as an exercise to the reader to verify that a subset $H$ of $G$ is a subgroup if and only if $H$ is not empty and for all $a, b \in H$, $ab^{-1} \in H$. The following lemma is of crucial importance to the theory of groups.

**Lemma 2.4.2 [leftcosets]** Let $H$ be a subgroup of $G$. The relation $\sim$ on $G \times G$ define by

$$a \sim b \quad \text{if and only if there exists } h \in H \text{ with } b = ah$$

is an equivalence relation.

**Proof:** Let $a \in G$ then $a = ae$ and so $\sim$ is reflexive.

Let $a \sim b$ and pick $h \in H$ with $b = ah$. Then

$$bh^{-1} = (ah)a^{-1} = a(hh^{-1}) = ae = a$$

Since $H$ is a subgroup of $G$, $h^{-1} \in H$ and so $b \sim a$. Hence $\sim$ is symmetric.

Suppose next that $a \sim b$ and $b \sim c$. Then $b = ah$ and $c = bk$ with $k, h \in H$. We compute

$$c = bk = (ah)k = a(hk)$$

Since $H$ is a subgroup, $hk \in H$ and so $a \sim c$ and $\sim$ is transitive. \hfill $\square$

The reader might have noticed that the reflexivity corresponds to $e \in H$, the symmetry to the closure under inverses and the transitivity to the closure under multiplication. Indeed $\sim$ can be defined for any subset of $G$, and its a equivalence relation if an only if the subset is a subgroup.

The equivalence classes of $\sim$ are called the (left) cosets of $H$. The coset containing $a \in G$ is denoted by $aH$ and so $aH = \{ah \mid h \in H\}$. The set of cosets of $H$ is denoted by $G/H$ and so $G/H = \{gH \mid g \in G\}$. Observe that the map $H \rightarrow gH \mid h \rightarrow gh$ is a bijection and so $|H| = |gH|$ for all $gH \in G/H$.

**Theorem 2.4.3 (Lagrange)** Let $H$ be a subgroup of $G$. Then $|G| = |G/H| \cdot |H|$. In particular if $G$ is finite, the order of $H$ divides the order of $G$.

**Proof:** Just observe that $|G/H|$ is the numbers of cosets, each coset contains $|H|$ elements and $G$ is the disjoint union of the cosets. \hfill $\square$

Let $\mathcal{P}(G)$ be the power set of $G$, that is the set of subsets. For $H, K \subset G$ put

$$HK = \{hk \mid h \in H, k \in K\}.$$
This binary operation is associative and \{e\} is an identity element. So \( \mathcal{P}(G) \) is a monoid.

If \( K \) is a subgroup then \( HK \) is a union of cosets of \( K \), namely \( HK = \bigcup_{h \in H} hK \). We write \( HK/K \) for the sets of cosets of \( K \) in \( HK \). In general if \( J \subseteq G \) is a union of cosets of \( H \), \( J/H \) denotes the sets of all those cosets. The same argument as in the proof of Lagrange’s Theorem shows \( |J| = |J/K| \cdot |K| \).

**Lemma 2.4.4** Let \( H \) and \( K \) be subgroups of \( G \).

(a) The map \( H/H \cap K \to HK/K, h(H \cap K) \to hK \) is a well defined bijection.

(b) \( |HK| = \frac{|H||K|}{|H \cap K|} \)

**Proof:** (a) Since \( (H \cap K)K = K \), \( hK = h((H \cap K)K) = (h(H \cap K))K \) and so is independent of the choice of \( h \in h(H \cap K) \). The map is clearly onto. Finally if \( hK = jK \) for some \( h, j \in H \), then \( h^{-1}jK = K \), \( h^{-1}j \in K \) and so \( h^{-1}j \in H \cap K \) and \( h(H \cap K) = j(H \cap K) \). Thus the map is one to one.

(b) By (a) we have \( |H/H \cap K| = |HK/K| \). So

\[
\frac{|H|}{|H \cap K|} = \frac{|KH|}{|K|}
\]

Thus (b) holds. \( \square \)

### 2.5 Normal subgroups and the isomorphism theorem

Just as we have defined (left) cosets one can define right cosets for a subgroup \( H \) of \( G \). The right cosets have the form \( Hz = \{hz | h \in H \} \). In general a left coset of \( H \) is not a right coset.

**Definition 2.5.1** [defnormal] Let \( G \) be a group.

(a) For \( a, b \in G \) put \( b^a = aba^{-1} \) and for \( I \subseteq G \) put \( I^a = aIa^{-1} = \{i^a | i \in I \} \). The map

\[
i_h : G \to G, b \to b^a
\]

is called conjugation be \( a \).

(b) A subgroup \( H \) of \( G \) is called a normal subgroup of \( G \) and we write \( H \trianglelefteq G \) if

\[
H = H^g \text{ for all } g \in G.
\]

**Lemma 2.5.2** [basicnormal] Let \( N \trianglelefteq G \). Then the following are equivalent:

(a) \( N \trianglelefteq G \).

(b) \( gN = Ng \) for all \( g \in G \).

(c) Every left coset is a right coset
(d) Every left coset is contained in a right coset.

(e) \( N^g \subseteq N \) for all \( g \in G \).

**Proof:** Suppose (a) holds. Then \( gNg^{-1} = N \) for all \( g \in G \). Multiplying with \( g \) from the right we get \( gN = Ng \).

Suppose (b) holds. Then the left cosets \( gN \) equals the right coset \( Ng \), so (c) holds.

Clearly (c) implies (d)

Suppose that (d) holds. Let \( g \in G \). Then \( gN \subseteq Nh \) for some \( h \in G \). Since \( g \in gN \) we conclude \( g \in Nh \) and so \( Ng = Nh \), as the right cosets partition \( G \). Thus \( gN \subseteq Ng \). Multiplying with \( g^{-1} \) from the right we get \( gNg^{-1} \subseteq N \). Thus (e) holds.

Finally suppose that (e) holds. Let \( g \in G \). Then also \( g^{-1} \in N \) and applying (e) to \( g^{-1} \) we obtain \( g^{-1}Ng \subseteq N \). Multiplying with \( g \) from the left and \( g^{-1} \) from the right we obtain \( N \subseteq gNg^{-1} = N^g \). Since also \( N^g \subseteq N \), \( N = N^g \) and so (a) holds.

We will now start to establish a connection between normal subgroups and homomorphism.

**Lemma 2.5.3 [basichom]** Let \( \phi : G \to H \) be a group homomorphism.

(a) \( \phi(e) = e \).

(b) \( \phi(a^{-1}) = \phi(a)^{-1} \).

(c) \( \phi(a^g) = \phi(a)^{\phi(g)} \).

(d) If \( A \leq G \) then \( \phi(A) \leq H \).

(e) If \( B \leq H \) then \( \phi^{-1}(B) \leq G \).

(f) Let \( \ker \phi = \{ g \in G \mid \phi(g) = e \} \). Then \( \ker \phi \) is a normal subgroup of \( G \).

(g) \( \phi \) is one to one if and only if \( \ker \phi = \{ e \} \).

(h) If \( N \leq G \), and \( \phi \) is onto, \( \phi(N) \leq H \).

(i) If \( M \leq H \), \( \phi^{-1}(M) \leq G \).

**Proof:** Straightforward. \( \square \)

For \( H \leq G \) define \( H^{-1} = \{ h^{-1} \mid h \in H \} \).

**Lemma 2.5.4 [basicG/N]** Let \( N \leq G \).

(a) The product of any two cosets of \( N \) is again a coset of \( N \). Namely \( (aN)(bN) = (ab)N \).

(b) For each \( g \in G \), \( (gN)^{-1} \) is a coset of \( N \), namely \( (gN)^{-1} = g^{-1}N \).
2.5. NORMAL SUBGROUPS AND THE ISOMORPHISM THEOREM

(c) $G/N$ is a group.

(d) The map $G \rightarrow G/N, \ g \rightarrow gN$ is an onto homomorphism with kernel $N$.

**Proof:**

(a) $(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN$

(b) $(aN)^{-1} = Na^{-1} = a^{-1}N$

(c) By (a) multiplication is binary operation on $G/N$. Clearly $N$ is an identity element and by (a) $g^{-1}N$ is an inverse for $gN$. Also multiplication of subsets is associative and so (c) holds.

(d) By (a) the map is a homomorphism. Clearly it is onto. $g$ is mapped to $e_{G/N} = N$ if and only if $gN = N$ and so if and only if $g \in N$. Thus $N$ is the kernel of the map. 

**Lemma 2.5.5 (The Isomorphism Theorem)** [IT] Let $\alpha : G \rightarrow H$ be a homomorphism of groups. The map

$$\bar{\alpha} : G/\ker \alpha \rightarrow \alpha(H), \ g \ker \alpha \rightarrow \alpha(g)$$

is a well-defined isomorphism.

**Proof:** Let $a \in \ker \alpha$ and $g \in G$. Then

$$\alpha(gn) = \alpha(g)\alpha(n) = \alpha(g)e = \alpha(g)$$

and so $\bar{\alpha}$ is well defined. By definition $\bar{\alpha}$ is onto.

Let $g \ker \alpha \in \ker \bar{\alpha}$. Then $\alpha(g) = e$ and so $g \in \ker \alpha$ and $g \ker \alpha = \ker \alpha = e_{G/\ker \alpha})$. Hence by 2.5.3g, $\bar{\alpha}$ is one to and so an isomorphism. 

From the two preceding lemmas we see that the normal subgroup of $G$ are exactly the kernels of homomorphism. Also every homomorphism $G \rightarrow H$ can be factorized as $\alpha = \rho \bar{\alpha} \pi$, where $\pi : G \rightarrow G/\ker \alpha$ is the canonical homomorphism from 2.5.4, $\bar{\alpha}$ is the isomorphism from 2.5.5 and $\rho : \alpha(H) \rightarrow H, h \rightarrow h$ is the inclusion map. Note here that $\pi$ is onto, $\bar{\alpha}$ an isomorphism and $\rho$ is one to one.

**Lemma 2.5.6** [capg] Let $G$ be a group and $(G_i, i \in I)$ a family of subgroups. Then $\bigcap_{i \in I} G_i$ is a subgroup. If all of the $G_i$ are normal in $G$, so is $\bigcap_{i \in I} G_i$.

**Proof:** Left as an exercise.

**Definition 2.5.7** Let $G$ be a group and $J \subseteq G$.

(a) The subgroup $\langle J \rangle$ of $G$ generated by $J$ is defined by

$$\langle J \rangle = \bigcap_{J \subseteq H \subseteq G} H$$
(b) The normal subgroup \( \langle J^g \rangle \) of \( G \) generated by \( J \) is defined by
\[
\langle J^g \rangle = \bigcap_{H \leq G} H
\]
If \( (J_i, i \in I) \) is a family of subsets we also write \( \langle J_i \mid i \in I \rangle \) for \( \bigcup_{i \in I} J_i \). \( J \subseteq G \) is called normal if \( J^g = J \) for all \( g \in G \).

Lemma 2.5.8 \([\text{basicgen}]\) Let \( I \) be a subset of \( G \).

(a) Let \( \alpha : G \to H \) be a group homomorphism. Then \( \alpha(\langle I \rangle) = \langle \alpha(I) \rangle \).

(b) Let \( g \in G \). Then \( \langle I \rangle^g = \langle I \rangle^g \).

(c) If \( I \) is normal in \( G \), so is \( \langle I \rangle \).

(d) \( \langle I \rangle \) consists of all products of elements in \( I \cup I^{-1} \).

(e) \( \langle I \rangle^g = \langle I^g \mid g \in G \rangle \) and consists of all products of elements in \( \bigcup_{g \in G} (I \cup I^{-1})^g \).

Proof: (a) Let \( A = \langle I \rangle \) and \( B = \langle \alpha(I) \rangle \). As \( \alpha(A) \) is a subgroup of \( H \) and contains \( \alpha(I) \) we have \( B \leq \alpha(A) \). Also \( \alpha^{-1}(B) \) is a subgroup of \( G \) and contains \( I \). Thus \( A \leq \alpha^{-1}(B) \) and so \( \alpha(A) \leq B \). Hence \( B = \alpha(A) \).

(b) Apply (a) to the homomorphism \( x \to x^g \).

(c) Follows from (b).

(d) Let \( H \) be the subset of \( G \) consists of all products of elements in \( I \cup I^{-1} \), that is all elements of the form \( a_1a_2 \ldots a_n \), with \( n \geq 0 \) and \( a_i \in I \cup I^{-1} \) for all \( 1 \leq i \leq n \). Then Clearly \( H \) is contained in any subgroup of \( G \) containing \( I \). Thus \( H \subseteq \langle I \rangle \). But \( H \) is also a subgroup containing \( I \) and so \( \langle I \rangle \leq H \).

(e) By (b) \( \langle I^g \mid g \in G \rangle \) is normal subgroup of \( G \). It is also contained in every normal subgroup containing \( I \) and we get \( \langle I^g \rangle = \langle I^g \mid g \in G \rangle \). The second statement follows from (c).

For \( a, b \in G \) put
\[
[a, b] = aba^{-1}b^{-1}
\]
and for \( A, B \subseteq G \) define
\[
[A, B] = \{[a, b] \mid a \in A, b \in B\}.
\]
\([a, b] \) is called the commutator of \( a \) and \( b \). Note that \([a, b] = e\) if and only if \( ab = ba \). Also
\[
[a, b] = b^a b^{-1} = ab^{-a}
\]
where we used the abbreviation \( b^{-a} = (b^{-1})^a \). Finally observe
\[
[a, b]^{-1} = bab^{-1} a^{-1} = [b, a]
\]
Hence \([A, B] = [B, A] \) for any \( A, B \subseteq G \).
Lemma 2.5.9 \[\text{[comnormal]}\] Let $G$ be a group.

(a) Let $N \leq G$. Then $N \leq G$ if and only if $[N, G] \leq N$

(b) Let $A, B \leq G$. Then $[A, B] \leq A \cap B$.

(c) Let $A, B \leq G$ with $A \cap B = \{e\}$. Then $[A, B] = \{e\}$ and $ab = ba$ for all $a \in A, b \in B$.

\textbf{Proof:} 

$n^g \in N \iff n^g n^{-1} \in N \iff [n, g] \in N$.

Thus (a) holds. (b) follows from (a), and (c) follows from (a) & (b). \[\Box\]

For $H \subseteq G$ define $N_G(H) = \{g \in H \mid H^g = H\}$. $N_G(H)$ is called the \textit{normalizer} of $H$ in $G$. If $K \subseteq G$ we say that $K$ \textit{normalizes} $H$ provided that $K \subseteq N_G(H)$.

Lemma 2.5.10 \[\text{[normalize]}\] Let $G$ be a group.

(a) Let $A, B$ be subgroups of $G$. Then $AB$ is a subgroup of $G$ if and only if $AB = BA$.

(b) Let $H \subseteq G$. Then $N_G(H)$ is a subgroup of $G$.

(c) If $K, H \leq G$ and $K \leq N_G(H)$, then $\langle K, H \rangle = KH$.

(d) Let $K_i, i \in I$ be a family of subsets if $G$. If each $K_i$ normalizes $H$, so does $\langle K_i \mid i \in I \rangle$.

\textbf{Proof:} (a) If $AB$ is a subgroup of $G$, then

$AB = (AB)^{-1} = B^{-1}A^{-1} = BA$

Conversely suppose that $AB = BA$. The above equation shows that $AB$ is closed under inverses. Also $e = ee \in AB$ and

$(AB)(AB) = A(BA)B = A(AB)B = A^2B^2 = AB$

So $AB$ is closed under multiplication.

(b) Readily verified.

(c) Let $k \in K$. Then $kH = Hk$ and so $HK = KH$. So by (a) $HK$ is a subgroup of $G$.

(d) Follows directly from (b). \[\Box\]
2.6 Cyclic groups

A group is cyclic if $G = \langle x \rangle$ for some $x \in G$. In this section we will determine all cyclic groups up to isomorphism and investigate their subgroups and homomorphisms.

Lemma 2.6.1 [subgroups\(\mathbb{Z}\)]

(a) Let $H$ be a subgroup of $(\mathbb{Z}, +)$ Then $H = n\mathbb{Z}$ for some $n \in \mathbb{N}$.

(b) Let $n, m \in \mathbb{N}$. Then $n\mathbb{Z} \leq m\mathbb{Z}$ if and only if $m$ divides $n$.

Proof: (a) If $H = \{0\}$, then $H = 0\mathbb{Z}$. So we may assume that $H \neq \{0\}$. Since $H$ is a subgroup, $m \in H$ implies $-m \in H$. So $H$ contains some positive integer. Let $n$ be the smallest such. Let $m \in H$ and write $m = rn + s$, $r, s \in \mathbb{Z}$ with $0 \leq s < n$. We claim that $rn \in H$. Then $rn \in H$ if and only if $-rn \in H$. So we may assume $r > 0$. But then

$$rn = n + n + \ldots + n$$

$r$-times

and as $n \in H$, $rn \in H$. So also $s = m - rn \in H$. Since $0 \leq s < n$, the minimal choice of $n$ implies $s = 0$. Thus $m = rn \in n\mathbb{Z}$ and $H = n\mathbb{Z}$.

(b) $n\mathbb{Z} \leq m\mathbb{Z}$ if and only if $n \in m\mathbb{Z}$. So if and only if $m$ divides $n$. \qed

Lemma 2.6.2 [free1] Let $G$ be a group and $g \in G$. Then $\phi : \mathbb{Z} \to G, \ n \to g^n$ is the unique homomorphism from $(\mathbb{Z}, +)$ to $G$ which sends 1 to $g$.

Proof: More or less obvious. \qed

For $r \in \mathbb{Z}^+ \cup \{\infty\}$ define $r^* = \begin{cases} r & \text{if } r < \infty \\ 0 & \text{if } r = \infty \end{cases}$.

This definition is motivated by the fact that $|\mathbb{Z}/n\mathbb{Z}|^* = n$.

Lemma 2.6.3 [clf cyclic] Let $G = \langle x \rangle$ be a cyclic group and put $n = |G|^*$

(a) The map

$$\mathbb{Z}/n\mathbb{Z} \to G, \ m + n\mathbb{Z} \to x^m$$

is a well-defined isomorphism.

(b) Let $H \leq G$ and put $m = |G/H|^*$. Then $m$ divides $n$, and $H = \langle x^m \rangle$.

Proof: By 2.6.2 the map $\phi : \mathbb{Z} \to G, m \to g^m$ is a homomorphism. As $G = \langle x \rangle$, $\phi$ is onto. By 2.6.1 ker $\phi = t\mathbb{Z}$ for some non-negative integer $t$. By the isomorphism theorem the map

$$\mathbb{Z}/t\mathbb{Z} \to G, m + t\mathbb{Z} \to x^m$$
is a well defined isomorphism. Hence \( \mathbb{Z}/t\mathbb{Z} \cong G \). Hence \( t = |\mathbb{Z}/t\mathbb{Z}|^* = |G|^* = n \) and (a) is proved.

(b) By 2.6.1 \( \phi^{-1}(H) = s\mathbb{Z} \) for some \( s \in N \). Since \( n\mathbb{Z} \leq s\mathbb{Z} \), 2.6.1 implies that \( s \) divides \( n \). As \( \phi \) is onto, \( \phi(s\mathbb{Z}) = H \) and so \( H = \langle \phi(s) \rangle = (x^s) \). Moreover

\[
G/H \cong (\mathbb{Z}/n\mathbb{Z})/(s\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/s\mathbb{Z}.
\]

Thus \( s = m \) and (b) is proved.

\[\square\]

Lemma 2.6.4 Let \( G = \langle x \rangle \) be a cyclic. Let \( H \) be any group and \( y \in H \). Put \( n = |G|^* \) and \( m = |x|^* \). Then there exists a homomorphism \( G \to H \) with \( x \to y \) if and only if \( m \) divides \( n \).

Proof: Exercise.

\[\square\]

2.7 Simplicity of the alternating groups

In this section we will investigate the normal subgroups of symmetric group \( \text{Sym}(n) \), \( n \) a positive integer. We start by defining a particular normal subgroup called the alternating group \( \text{Alt}(n) \). Let \( \mathbb{R} \) be the field of real numbers and \( \text{GL}_n(\mathbb{R}) \) the group of invertible linear transformation of the vector space \( \mathbb{R}^n \). Define \( \alpha : \text{Sym}(n) \to \text{GL}_n(\mathbb{R}) \) by

\[
\alpha(\pi)(r_1, \ldots, r_n) = (r_{\pi^{-1}(1)}, \ldots, r_{\pi^{-1}(n)}).
\]

It is easy to check that \( \alpha \) is a homomorphism. Now define \( \text{sgn} = \det \circ \alpha \). As the determinant is a homomorphism from \( \text{GL}_n(\mathbb{R}) \) to \( \mathbb{R} \), \( \text{sgn} \) is a homomorphism from \( \text{Sym}(n) \) to \( \mathbb{R} \). Also if \( x = (i, j) \in \text{Sym}(n) \) is a 2-cycle, we see that \( \text{sgn}(x) = -1 \). So if \( x = (a_1, a_2, \ldots, a_m) \in \text{Sym}(n) \) is a \( m \)-cycle then

\[
\text{sgn}(x) = \text{sgn}((a_1, a_2)(a_2, a_3)\ldots(a_{m-1}, a_m)) = (-1)^{m-1}.
\]

So we conclude that

\[
\text{sgn}(x) = \begin{cases} 
1 & \text{if } x \text{ has an even number of even cycles} \\
-1 & \text{if } x \text{ has an odd number of even cycles}
\end{cases}
\]

Define \( \text{Alt}(n) = \ker \text{sgn} \). Then \( \text{Alt}(n) \) is a normal subgroup of \( \text{Sym}(n) \), \( \text{Alt}(n) \) consists of all permutation which have an even number of even cycles and

\[
\text{Sym}(n)/\text{Alt}(n) \cong \text{sgn}(\text{Sym}(n)) = \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}.
\]

In particular,

\[
|\text{Alt}(n)| = \frac{n!}{2}
\]
Before continuing to investigate the normal subgroup of $\text{Sym}(n)$ we wish to define conjugacy classes in an arbitrary group $G$. We say that two elements $x, y$ in $G$ are conjugate if $y = x^g = gxg^{-1}$ for some $g \in G$. It is an easy exercise to verify that this is an equivalence relation. The equivalence classes are called the conjugacy classes of $G$. The conjugacy class containing $x$ is $x^G = \{x^g \mid g \in G\}$.

**Proposition 2.7.1** A subgroup of $G$ is normal if and only if it is the union of conjugacy classes of $G$.

**Proof:** Let $N \leq G$. The following are clearly equivalent:

- $N \trianglelefteq G$
- $N^g \leq N$ for all $g \in G$
- $n^g \in N$ for all $n \in N, g \in G$
- $n^G \subseteq N$ for all $n \in N$
- $N = \bigcup_{n \in N} n^G$
- $N$ is a union of conjugacy classes

To apply this to $\text{Sym}(n)$ we need to determine its conjugacy classes. For $x \in \text{Sym}(n)$ define the cycle type of $x$ to be sequence $(m_i)_{i \geq 1}$, where $m_i$ is the numbers of cycles of $x$ of length $i$. So the cycle type keeps track of the lengths of the cycles of $x$, counting multiplicities.

**Proposition 2.7.2** Two elements in $\text{Sym}(n)$ are conjugate if and only if they have the same cycle type.

**Proof:** We will show that the conjugate of the cycle $g = (a_1, \ldots, a_m)$ by the element $\pi \in \text{Sym}(n)$ is the cycle $(\pi(a_1), \pi(a_2), \ldots, \pi(a_m))$.

Let $1 \leq k \leq n$. If $k \neq \pi(a_j)$ for some $j$, then $\pi^{-1}(k)$ is fixed by $g$. So $(\pi g \pi^{-1})(k) = \pi(\pi^{-1}(k)) = k$.

If $k = \pi(a_j)$ then

$$(\pi g \pi^{-1})(\pi(a_j)) = \pi(g(a_j)) = \pi(a_{j+1})$$

Suppose now that $g$ has cycle type $(m_i)$. Then

$$g = \prod_{i \geq 1 \leq j \leq m_i} g_{ij}$$

where $g_{ij} = (a_1(ij), \ldots, a_i(ij))$ is a cycle of length $i$. Moreover for each $1 \leq l \leq n$ there exists uniquely determined $i, j$ and $k$ with $l = a_k(ij)$.

In particular,

$$g^\pi = \prod_{i \geq 1 \leq j \leq m_i} g_{ij}^\pi$$
2.7. SIMPLICITY OF THE ALTERNATING GROUPS

where \( g_{ij}^\pi = (\pi(a_1(ij)), \ldots, \pi(a_i(ij))) \) is a cycle of length \( i \). So also \( g^\pi \) has cycle type \( (m_i) \).

Conversely, suppose also \( h \) has cycle type \( (m_i) \). so

\[
\prod_{i \geq 1} \prod_{1 \leq j \leq m_i} h_{ij}
\]

where \( h_{ij} = (b_1(ij), \ldots, b_i(ij)) \) is a cycle of length \( i \).

Define \( \pi \in \text{Sym}(n) \) by

\[
\pi(a_k(ij)) = b_k(ij)
\]

But then \( g^\pi = h \) and \( g \) and \( h \) are conjugate.

Let’s now investigate the normal subgroups of \( \text{Sym}(3) \). We start by listing the conjugacy classes

- \( e \) 1 element
- \( (123), (132) \) 2 elements
- \( (12), (13), (23) \) 3 elements

Let \( e \neq N \leq \text{Sym}(3) \). If \( N \) contains the 2-cycles, then \( |N| \geq 4 \). Since \( |N| \) divides \( |\text{Sym}(3)| = 6 \) we get \( |N| = 6 \) and \( N = \text{Sym}(3) \).

If \( N \) does not contain the 2-cycles we get \( N = \{ e, (123), (132) \} = \text{Alt}(3) \).

So \( \text{Alt}(3) \) is the only proper normal subgroup of \( \text{Sym}(3) \).

Let’s move on to \( \text{Sym}(4) \). The conjugacy classes are:

- \( e \) 1 element
- \( (123), (132), (124), (142), (134), (143), (234), (243) \) 3 elements
- \( (12), (13), (14), (23), (24), (34) \) 6 elements
- \( (1234), (1243), (1324), (1342), (1423), (1432) \) 8 elements

Let \( N \) be a proper normal subgroup of \( \text{Sym}(4) \) then \( |N| \) divides \( 24 = |\text{Sym}(4)| \), Thus \( |N| = 2, 3, 4, 6, 8 \) or 12. So \( N \) contains 1, 2, 3, 5, 7 or 11 non-trivial elements. As \( N \setminus \{ e \} \) is a union of conjugacy classes, \( |N| - 1 \geq 3 \). So \( |N| - 1 \in \{ 3, 5, 7, 11 \} \). In particular \( |N| - 1 \) is odd. But \( \text{Sym}(3) \) has a unique non-trivial conjugacy class of odd length, namely the double 2-cycles. So \( K \subseteq N \), where \( K = \{ e, (12)(34), (13)(24), (14)(23) \} \). Then \( |N \setminus K| \in \{ 0, 3, 8 \} \) All remaining conjugacy classes have length 6 or 8 and we conclude that \( N = K \) or \( |N \setminus K| = 8 \).

In the second case, \( N \) consist of \( K \) and the 3-cycles and so \( N = \text{Alt}(4) \). Note also that \( (12)(34)(13)(24) = (14)(23) \) and so \( K \) is indeed a normal subgroup of \( \text{Sym}(4) \).

Thus the proper normal subgroups of \( \text{Sym}(4) \) are \( \text{Alt}(4) \) and \( K \).

Just for fun let’s as determine the quotient group \( \text{Sym}(4)/K \). No non-trivial element of \( K \) fixes "4". So \( \text{Sym}(3) \cap K = \{ e \} \) and

\[
|\text{Sym}(3)K| = \frac{|\text{Sym}(3)||K|}{|\text{Sym}(3) \cap K|} = \frac{6 \cdot 4}{1} = 24 = |\text{Sym}(4)|.
\]
Thus \( \text{Sym}(3)K = \text{Sym}(4) \). And

\[
\text{Sym}(4)/K = \text{Sym}(3)K/K \cong \text{Sym}(3)/(\text{Sym}(3) \cap K) = \text{Sym}(3)/\{e\} \cong \text{Sym}(3)
\]

So the quotient of \( \text{Sym}(4) \) by \( K \) is isomorphic to \( \text{Sym}(3) \).

Counting arguments as above can be used to determine the normal subgroups in all the \( \text{Sym}(n) \)'s, but we prefer to take a different approach.

**Lemma 2.7.3 [3cycles]**

(a) \( \text{Alt}(n) \) is the subgroup of \( \text{Sym}(n) \) generated by all the 3-cycles.

(b) If \( n \geq 5 \) then \( \text{Alt}(n) \) is the subgroup of \( \text{Sym}(n) \) generated by all the double 2-cycles.

(c) Let \( N \) be a normal subgroup of \( \text{Alt}(n) \) containing a 3-cycle. Then \( N = \text{Alt}(n) \).

(d) Let \( n \geq 5 \) and \( N \) a normal subgroup of \( \text{Alt}(n) \) containing a double 2-cycle. Then \( N = \text{Alt}(n) \).

**Proof:**

(a) By induction on \( n \). If \( n \leq 3 \), all non-trivial elements in \( \text{Alt}(n) \) are 3-cycles. So we may assume \( n \geq 4 \). Let \( H \) be the subgroup of \( \text{Sym}(n) \) generated by all the 3-cycles. By induction \( \text{Alt}(n-1) \leq H \). Let \( g \in \text{Alt}(n) \). If \( g(n) = n \), \( n \in \text{Alt}(n-1) \leq H \). So suppose \( g(n) \neq n \) and let \( a < n \) with \( a \neq g(n) \). Let \( h \) be the 3-cycle \( (g(n), n, a) \). Then \( (hg)(n) = h(g(n)) = n \). Hence \( hg \in \text{Alt}(n-1) \leq H \) and so also \( g = h^{-1}(hg) \in H \).

(b) Let \( h = (a, b, c) \) be a 3-cycle in \( \text{Sym}(n) \). Since \( n \geq 5 \), there exist \( 1 \leq d < e \leq n \) distinct from \( a, b \) and \( c \). Note that

\[
(a, b, c) = (a, b)(d, e)(b, c)(d, e)
\]

and so the subgroup generated by the double 2-cycles contains all the 3-cycles. Hence (b) follows from (a).

(c) Let \( h = (a, b, c) \) by a 3-cycle in \( N \) and \( g \) any 3-cycle in \( \text{Sym}(n) \). By (a) it suffices to prove that \( g \in N \). Since all 3-cycles are conjugate in \( \text{Sym}(n) \) there exists \( t \in \text{Sym}(n) \) with \( h^t = g \). If \( t \in \text{Alt}(n) \) we get \( g = h^t \in N^t = N \), as \( N \) is normal in \( \text{Alt}(n) \).

So suppose that \( t \not\in \text{Alt}(n) \). Then \( t(a, b) \in \text{Alt}(n) \). Note that \( h^{-1} = (c, b, a) = (b, a, c) \) and so \((h^{-1})(a, b) = (b, a, c)(a, b) = (a, b, c) = h \). Thus

\[
(h^{-1})^t(a, b) = ((h^{-1})(a, b))^t = h^t = g
\]

As the left hand side is in \( N \) we get \( g \in N \).

(d) A similar argument as in (c) shows that (b) implies (d).

**Theorem 2.7.4 [altnsimple]** Let \( n \geq 5 \). Then \( \text{Alt}(n) \) has no proper normal subgroup.
2.7. SIMPLICITY OF THE ALTERNATING GROUPS

Proof: If \( n > 5 \) we assume by induction that the theorem is true for \( n - 1 \). Let \( N \) be a non-trivial normal subgroup of \( \text{Alt}(n) \).

Case 1: \( N \) contains an element \( g \neq e \) with \( g(i) = i \) for some \( 1 \leq i \leq n \).

Let \( H = \{ h \in \text{Alt}(n) \mid h(i) = i \} \). Then \( H \cong \text{Alt}(n - 1) \), \( g \in H \cap N \) and so \( H \cap N \) is a non-trivial normal subgroup. We claim the \( H \cap N \) contains a 3-cycle or a double 2-cycle. Indeed if \( n = 5 \), then \( n - 1 = 4 \) and the claim holds as every non-trivial element in \( \text{Alt}(4) \) is either a 3-cycle or a double 2-cycle. It is also true for \( n > 5 \) since then by induction \( H \cap N = H \).

By the claim and 2.7.3c,d we conclude \( N = \text{Alt}(n) \).

Case 2: \( N \) contains a element \( g \) with a cycle of length at least 3.

Let \( (a, b, c, \ldots) \) be a cycle of \( g \) of length at least 3. Let \( 1 \leq d \leq n \) be distinct from \( a, b \) and \( c \). Put \( h = g^{(abc)} \). Then \( h \) has the cycle \( (d, b, a, \ldots) \). Also as \( N \) is normal in \( \text{Alt}(n) \), \( h \in N \). So also \( hg \in N \).

We compute \( (hg)(a) = h(b) = a \) and \( (hg)(b) = h(c) \neq h(d) = b \). So \( hg \neq e \) and \( hg \) fixes "a". So by case 1, \( N = \text{Alt}(n) \).

Case 3: \( N \) contains an element \( g \) with at least two 2-cycles.

Such a \( g \) has the form \( (ab)(cd)t \) where \( t \) is a product of cycles disjoint from \( \{ a, b, c, d \} \). Let \( h = g^{(abc)} \). Then \( h = (bc)(ad)t \) Thus

\[
gh^{-1} = (ab)(cd)t \cdot (bc)(ad) = (ac)(bd).
\]

As \( h \) and \( gh^{-1} \) are in \( N \), Case 1 (or 2.7.3d) shows that \( N = \text{Alt}(n) \).

Now let \( e \neq g \in N \). As \( n \geq 4 \), \( g \) must fulfill one of the three above cases and so \( N = \text{Alt}(n) \).

A group without proper normal subgroups is called simple. So the previous theorem can be rephrased as:

For all \( n \geq 5 \), \( \text{Alt}(n) \) is simple.

Proposition 2.7.5 [normalsym] Let \( N \trianglelefteq \text{Sym}(n) \). Then either \( M = \{ e \}, \text{Alt}(n) \) or \( \text{Sym}(n) \), or \( n = 4 \) and \( N = \{ e, (12)(34), (13)(24), (14)(23) \} \).

Proof: The case \( n \leq 4 \) was dealt with above. So suppose \( n \geq 5 \). Then \( N \cap \text{Alt}(n) \) is a normal subgroup of \( \text{Alt}(n) \) and so by 2.7.4, \( N \cap \text{Alt}(n) = \text{Alt}(n) \) or \( \{ e \} \).

In the first case \( \text{Alt}(n) \leq N \leq \text{Sym}(n) \). Since \( |\text{Sym}(n) / \text{Alt}(n)| = 2 \), we conclude \( N = \text{Alt}(n) \) or \( N = \text{Sym}(n) \).

In the second case we get

\[
|N| = |N / N \cap \text{Alt}(n)| = |N \text{Alt}(N) / \text{Alt}(N)| \leq |\text{Sym}(n) / \text{Alt}(n)| \leq 2
\]

Suppose that \( |N| = 2 \) and let \( e \neq n \in N \). As \( n^2 = e \), \( n \) has a 2-cycle \( (ab) \). Let \( a \neq c \neq b \) with \( 1 \leq c \leq n \). The \( n^{(abc)} \) has cycle \( (bc) \) and so \( n \neq n^{(abc)} \). A contradiction to \( N = \{ e, n \} \) and \( N \trianglelefteq \text{Sym}(n) \). □
Lemma 2.7.6 \[\text{absim}\] The abelian simple groups are exactly cyclic groups of prime order.

Proof: Let $A$ be an abelian simple group and $e \neq a \in A$. Then $\langle a \rangle \leq A$ and so $A = \langle a \rangle$ is cyclic. Hence $A \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \geq 0$. If $m = 0$, $\mathbb{Z}$ is a normal subgroup. Hence $m > 0$. If $m$ is not a prime we can pick a divisor $1 < k < m$. But then $k\mathbb{Z}/m\mathbb{Z}$ is a proper normal subgroup. $\square$

2.8 Direct products and direct sums

Let $G_1$ and $G_2$ be groups. Then $G = G_1 \times G_2$ is a group where the binary operation is given by

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2).$$

Consider the projection maps

$$\pi_1 : G \to G_1, (a_1, a_2) \to a_1 \quad \text{and} \quad \pi_2 : G \to G_2, (a_1, a_2) \to a_2$$

Note that each $g \in G$ is uniquely determined by its images under $\pi_1$ and $\pi_2$. Indeed we have $g = (\pi_1(g), \pi_2(g))$. We exploit this fact in the following abstract definition.

Definition 2.8.1 Let $(G_i, i \in I)$ be a family of groups. The direct product of the $(G_i, i \in I)$ is a group $G$ together with a family of homomorphism $(\pi_i : G \to G_i, i \in I)$ such that:

Whenever $H$ is a group and $(\alpha_i : H \to H_i, i \in I)$ is family of homomorphism, then there exists a unique homomorphism $\alpha : H \to G$ such that the diagram:

$$\begin{array}{c}
G \xrightarrow{\alpha} H \\
\pi_i \downarrow \quad \alpha_i \\
G_i
\end{array}$$

commutes for all $i \in I$.

We will now show that the direct product (in the above sense) always exists. As a set let $G = \prod_{i \in I} G_i$, the set theoretic product of the $G_i$s. That is $G$ consists of all function $f : I \to \bigcup_{i \in I} G_i$ with $f(i) \in G_i$ for all $i \in I$. The binary operation is defined by

$$(fh)(i) = f(i)h(i).$$

It is easy to check that $G$ is a group. Define

$$\pi_i : \prod_{i \in I} G_i \to G_i, f \to f(i).$$

Obviously $\pi_i$ is a homomorphism. Let $H$ a group and $\alpha_i : H \to G_i$ a family of homomorphism. Define $\alpha : H \to G$ by
\[ \alpha(h)(i) := \alpha_i(h) \text{ for all } i \in I \]

But this is equivalent to
\[ \pi_i(\alpha(h)) = \alpha_i(h) \]

and so to
\[ \pi_i \alpha = \alpha_i. \]

In other words, \( \alpha \) is the unique map which makes the above diagram commutative. It trivial to verify that \( \alpha \) is a homomorphism and so \((\pi_i, i \in I)\) meets the definition of the direct product.

Lets go back to the above example \( G = G_1 \times G_2 \). This time we consider the inclusion maps:
\[ \rho_1 : G_1 \to G, g_1 \to (g_1, e) \text{ and } \rho_2 : G_2 \to G, g_2 \to (e, g_2) \]

Note also that \([\rho_1(G_1), \rho_2(G_2)] = \{e\}\).

Given a group \( H \). A family of commuting homomorphism is a family of homomorphism \((\alpha_i : G_i \to H, i \in I)\) such that
\[ \alpha_i(g_i)\alpha_j(g_j) = \alpha_j(g_j)\alpha_i(g_i) \]

for all \( i \neq j \in I, g_i \in G_i \) and \( g_j \in G_j \).

**Definition 2.8.2** A direct sum of the family of groups \((G_i, i \in I)\) is a group \( G \) together with a family of commuting homomorphism \((\rho_i : G_i \to G, i \in I)\) such that:

Whenever \( H \) is a group and \((\alpha_i : G_i \to H, i \in I)\) is a family of commuting homomorphism, then there exists a unique homomorphism \( \alpha : G \to H \) so that the diagram

\[
\begin{array}{ccc}
G & \xrightarrow{\alpha} & H \\
\downarrow{\rho_i} & & \downarrow{\alpha_i} \\
G_i & & 
\end{array}
\]

commutes for all \( i \in I \).

Before we proceed and show that directs sums exists we prove a couple of lemmas, which are useful in the construction.

**Lemma 2.8.3** [directsumgen] Let \((\rho_i : G_i \to G, i \in I)\) be a direct sum of \((G_i, i \in I)\). Then

(a) Each \( \rho_i, i \in I \), is one to one.

(b) \( G = \langle \rho_i(G_i) \mid i \in I \rangle \).
CHAPTER 2. GROUP THEORY

Proof: (a) For $i, j \in I$ define

$$\alpha_{ij} : G_i \to G_j, g \mapsto \begin{cases} g & \text{if } i = j \\ e & \text{if } i \neq j \end{cases}$$

Then for each $j \in I$, $(\alpha_{ij} \mid i \in I)$ is a family of commuting homomorphisms. So there exists $\alpha_j : G \to G_j$ with $\alpha_{ij} = \alpha_j \rho_i$.

As $\alpha_{ii} = \text{id}_{G_i}$ is one to one, also $\rho_i$ is to one.

(b) Let $H = \langle \rho_i(G_i) \mid i \in I \rangle$. Define $\tilde{\rho}_i : G_i \to H, g \mapsto \rho_i(g)$. Hence there exists map $\tilde{\beta} : G \to H$ with $\beta \rho_i = \tilde{\rho}_i$. $\tilde{\beta}$ defines a map $G \to G, g \mapsto \beta(g)$. Then $\beta \rho_i = \rho_i$ for all $i \in I$.

Now also $\text{id}_G$ is a map from $G \to G$ with $\text{id}_G \rho_i = \rho_i$, so the uniqueness part in the definition of the direct sum implies $\beta = \text{id}_G$. Thus for all $g \in G$, $g = \text{id}_G(G) = \beta(g) \in H$. $\blacksquare$

Lemma 2.8.4 [alphaunique] Let $\alpha, \beta : G \to H$ be group homomorphism. Let $(G_i, i \in I)$ be a family of subgroups of $G$. Suppose that

(a) $\alpha \mid G_i = \beta \mid G_i$ for all $i \in I$.

(b) $G = \langle G_i \mid i \in I \rangle$.

Then $\alpha = \beta$

Proof: Let $D = \{ g \in G \mid \alpha(g) = \beta(g) \}$. Clearly $D$ is a subgroup of $G$. By (a) $G_i \leq D$ for all $i \in I$. Thus by (b), $G \leq D$ and so $D = G$. $\blacksquare$

It follows from the two preceding lemmas that the uniqueness statement in the definition of the direct sum can be equivalently replaced by the condition $G = \langle \rho_i(G_i) \mid i \in I \rangle$.

We will construct the direct sum as a subgroup of the direct product $\prod_{i \in I} G_i$. We will view the elements of the direct products as tuples $g = (g_i)_{i \in I}$, with $g_i \in G_i$ for all $i \in I$. Define the support $\text{supp}(g)$ of $g$ by

$$\text{supp}(g) = \{ i \in I \mid g_i \neq e \}.$$ 

Let

$$\bigoplus_{i \in I} G_i = \{ g \in \prod_{i \in I} G_i \mid \text{supp}(g) \text{ is finite} \}.$$ 

Now $\text{supp}(e) = \emptyset$, $\text{supp}(g) = \text{supp}(g^{-1})$ and $\text{supp}(gh) \subseteq \text{supp}(g) \cup \text{supp}(h)$. So $\bigoplus_{i \in I} G_i$ is a subgroup of $\prod_{i \in I} G_i$. Define $\rho_i : G_i \to \bigoplus_{i \in I} G_i$ by

$$\rho_i(g)_j = \begin{cases} e & \text{if } j \neq i \\
 g & \text{if } j = i \end{cases}$$
Then for all \( i \neq j \)

\[
(\rho_i(g_i)\rho_j(g_j))_k = \begin{cases} 
  g_i & \text{if } k = i \\
  g_j & \text{if } k = j \\
  e & \text{if } i \neq k \neq j
\end{cases} = (\rho_j(g_j)\rho_i(g_i))_k
\]

and so \((\rho_i, i \in I)\) is a family of commuting homomorphism. Note that \( \bigoplus_{i \in I} G_i \) is exactly the subgroup of \( \prod_{i \in I} G_i \) generated by the \( \rho_i(G_i), i \in I \).

Let \( H \) be a group and \((\alpha_i : G_i \to H, i \in I)\) a family of commuting homomorphism. Define \( \alpha : \bigoplus_{i \in I} G_i \to H \) by

\[
\alpha((g_i)_{i \in I}) = \prod_{i \in I} \alpha_i(g_i)
\]

The product on the right hand side does not seem to make sense at first. But all but finitely many of the \( g_i \)'s (and so also of \( \alpha_i(g_i) \)'s) are trivial. So the product is effectively a finite product. Secondly since the \( \alpha_i(G_i) \) commute with each other, the order in which the product is taken does not matter. To verify that \( \alpha \) is homomorphism we compute

\[
\alpha(g)\alpha(h) = \prod_{i \in I} \alpha_i(g_i) \prod_{i \in I} \alpha_i(h_i) = \prod_{i \in I} \alpha_i(g_i)\alpha_i(h_i) = \prod_{i \in I} \alpha_i(g_ih_i) = \alpha(gh)
\]

Let \( g \in G_i \). Then \( \rho_i(g)_j = e \) for all \( j \neq 1 \) and \( \alpha(\rho_i(g)) = \alpha_i(g) \). Thus \( \alpha \rho_i = \alpha_i \).

The uniqueness of \( \alpha \) follows from \( G = \langle \phi_i(G_i) \rangle \) and 2.8.4

We say that \( G \) is the internal direct sum of \((G_i, i \in I)\) provided that each \( G_i \) is a subgroup of \( G \) and that \( G \), together with the inclusion map from \( G_i \) to \( G \), is a direct sum of \((G_i, i \in I)\). In particular this means that for each family \( \alpha_i : G_i \to H \) of commuting homomorphism there exists a unique homomorphism \( \alpha : G \to H \) with \( \alpha \big|_{G_i} = \alpha_i \).

**Proposition 2.8.5 [internal sum]** Let \( G \) be a group and \((G_i, i \in I)\) a family of subgroups. The following are equivalent:

1. \( G \) is the internal direct sum of the \((G_i, i \in I)\).

2. Each of following three statement hold:
   
   (a) Each \( G_i \) is normal in \( G \).
   
   (b) \( G = \langle G_i \mid i \in I \rangle \).
   
   (c) For each \( i \), \( G_i \cap \langle G_j \mid i \neq j \in I \rangle = \{e\} \).

3. \([G_i, G_j] = e \) for all \( i \neq j \in G \) and each \( g \in G \) can be uniquely written as \( \prod_{i \in I} g_i \), there \( g_i \in G_i \) and all but finitely many \( g_i \)'s are trivial.
Proof: (1) $\Rightarrow$ (2)
Suppose (1) holds. By 2.8.3b, 2b holds.
As the inclusion maps commute, $[G_i, G_j] = \{e\}$ for all $i \neq j$. In particular $G_j \leq N_{G_i}(G_i)$ for all $j \in I$. So 2a follows from 2b.
Let $\alpha_{ij}$ and $\alpha_i$ be as in the proof of 2.8.3a. Then $\alpha_i(g) = g$ for all $g \in G_i$. In particular, $G_i \cap \ker \alpha_i = \{e\}$. For all $j \neq i$, $G_j \leq \ker \alpha_i$ so 2c holds.
(2) $\Rightarrow$ (3)
Suppose (2) holds. $H_i = G_i \cap \langle G_j \mid i \neq j \in I \rangle$. By assumption each $G_j$ is normal in $G$ so both $G_i$ and $H_i$ are normal in $G$. Moreover by assumption $G_i \cap H_i = e$ and so $[G_i, H_i] \leq G_i \cap H_i = e$.
Thus $[G_i, G_j] = e$ for all $i \neq j \in I$. By assumption $G$ is generated by the $G_i$'s and so $g \in G$ can be written as $\prod_{i \in I} g_i$.
Suppose that
$$
\prod_{i \in I} g_i = \prod_{i \in I} a_i
$$
for some $g_i, a_i \in G_i$. Then
$$
a_i g_i^{-1} = \prod_{i \neq j \in I} a_j^{-1} g_j
$$
As the left side lies in $G_i$ and the right side in $H_i$ we conclude that $a_i g_i^{-1} = e$ and so $a_i = g_i$. Thus (3) holds.
(3) $\Rightarrow$ (1)
Suppose that (3) holds. Let $(\alpha_i : G_i \to H, i \in I)$ be a family of commuting homomorphism. Define $\alpha : G \to H$ by $\alpha(g) = \prod_{i \in I} \alpha_i(g_i)$, where $g = \prod_{i \in I} g_i$ and $g_i \in G_i$. Hence (1) holds. $\square$

The direct sums are slightly more natural in the category of abelian groups, namely every family of homomorphisms is automatically a family of commuting homomorphisms. In particular we see that the direct sum of a family of abelian groups is the coproduct in the category of abelian groups.

The direct sum can also be used to define the free abelian group $FA(I)$ on a set $I$. Namely put
$$
FA(I) = \bigoplus_{i \in I} \mathbb{Z}.
$$
Identify $i$ with $\rho_i(1)$. Then we see that every element in $FA(I)$ can be uniquely written as
$$
\sum_{i \in I} n_i i
$$
where $n_i \in \mathbb{Z}$ and almost all $n_i$'s are 0. Note here that in an abelian group we write $na$ for $a^n$. $FA(I)$ as the following universal property:
Theorem 2.8.6 [freeabelian] Let $A$ be an abelian group and $(a_i, i \in I)$ a family of elements in $A$. Then there exists a unique homomorphism
\[
\alpha : FA(I) \rightarrow A \text{ with } i \mapsto a_i.
\]
for all $i \in I$.

Proof: This follows from 2.6.2 and the definition of the direct sum. $\alpha$ is given by
\[
\alpha(\sum_{i \in I} n_i i) = \sum_{i \in I} n_i a_i.
\]

Direct products and direct can also be defined for semigroups and monoids. Direct sums cause a slight problem for semigroups since then the condition $g_i = e$ for almost all $i$ makes no sense. Maybe the easiest way to go around this problem is to embed each semigroup $G_i$ into a monoid $G_i^+ = G_i \cup \{e_i\}$ where $e_i$ is an identity in $G_i^+$. Then define
\[
\bigoplus_{i \in I} G_i = \bigoplus_{i \in I} G_i^+ \setminus \{(e_i)_{i \in I}\}
\]

The free abelian monoid on a set $I$ is
\[
\bigoplus_{i \in I} \mathbb{N}
\]
and removing the identity from this we get the free abelian semigroup.

2.9 Free products

Let $(G_i, i \in I)$ be a family of groups. In this section we will construct a group called the free product of the $(G_i, i \in I)$ and denoted by $\coprod_{i \in I} G_i$. On an intuitive level this group is the largest group which contains the $G_i$’s and is generated by them. On a formal level it is the coproduct of the $G_i$’s in the category of groups. (See theorem 2.9.5 below). To simplify notation we will assume (without loss of generality)

Hypothesis 2.9.1
(i) $(G_i, i \in I)$ is a family of groups.
(ii) $e_{G_i} = e_{G_j}$ for all $i, j \in I$. Call this common identity element $e$.
(iii) $G_i \cap G_j = \{e\}$ for all $i \neq j \in I$.

Let $X = \bigcup_{i \in I} G_i$. For $x \in X$ with $x \neq e$ let $i_x \in I$ be defined by $x \in G_{i_x}$. Note that by (iii) of our Hypothesis $i_x$ is well defined. Let $n \in \mathbb{N}$. A word of length $n$ in $X$ is a tuple
(\(x_1, x_2, \ldots, x_n\)) with \(x_m \in X\) for all \(1 \leq m \leq n\). \(W\) denotes the set of all words. The empty tuple \((n = 0)\) is denoted by \(w_0\). Define a binary operation "\(*\)" on \(W\) by

\[
(x_1, x_2, \ldots, x_n) * (y_1, y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m).
\]

Clearly "\(*\)" is associative. As \(w_0\) is an identity, \(W\) is a monoid.

Identify each \(x \in X\) with the word \((x)\). Call \(a, b \in X\) comparable if there exists \(i \in I\) with \(a, b \in G_i\). (So either \(a = e\), or \(b = e\), or \(i = i_a = i_b\). We would like that \(ab = a * b\) for such \(a, b\), but this is nonsense, since \((ab)\) is a word of length \(1\) and \(a * b = (a, b)\) is of length \(2\). To fix this problem we will introduce an equivalence relation on \(W\).

Let \(v, w \in W\). Write \(v < w\) if one of the following holds:

1. There exists \(x, y \in W\) and comparable \(a, b \in X\) with \(w = x*a*b*y\) and \(v = x*ab*y\)\).
2. There exists \(x, y \in W\) so that \(w = x*e*y\) and \(v = x*y\).

Note that \(v < w\) is only possible if \(l(v) = l(w) = 1\), where \(l(v)\) denotes the length of the word \(v\). Also since \(e\) is comparable with any \(x \in X\), condition \((< 2)\) implies condition \((< 1)\), with one exception though:

If \(x\) and \(y\) are both the empty word \(w_0\) we see from \((< 2)\) that \(w_0 < e\).

As \(< \) is not symmetric we define \(v - w\) if \(v < w\) or \(w < v\). Finally to achieve transitivity define \(v \sim w\) if

\[
v = v_0 - v_1 - v_2 - \ldots - v_{n-1} - v_n = w
\]

for some \(v_k \in W\). Here we allow \(n = 0\), so \(v \sim v\) for all words \(v\). The minimal such \(n\) is called the distance of \(v\) and \(w\).

**Lemma 2.9.2** [basicsim] \(\sim\) is an equivalence relation and

1. \(ab \sim a*b\) for all comparable \(a, b \in X\)
2. If \(t, v, w \in W\) with \(v \sim w\) then \(t*v \sim t*w\).
3. If \(t, v, w \in W\) with \(v \sim w\) then \(v*t \sim w*t\).

**Proof:** By \((< 1)\) with \(x = y = w_0\), \(ab < a*b\) for all comparable pairs \(a, b\). So \((\sim 1)\) holds.

To prove \((\sim 2)\) let \(v \sim w\). By induction on the distance of \(v\) and \(w\) we may assume that \(v - w\), say \(v < w\).

So \(w = x*a*b*y\) and \(v = x*ab*y\) for appropriate \(x, y, a\) and \(b\).

Thus \(t*w = (t*x)*a*b*y\) and \(t*v = (t*w)*ab*y\).

Hence \(t*v < t*w\) and in particular \(t*v \sim t*w\).

\((\sim 3)\) is proved with a similar argument.

For \(w \in W\) let \(\bar{w}\) be the equivalence class of "\(\sim\)" containing \(w\). Let \(\bar{W}\) be the set of all such equivalence classes. Define a binary operation on \(\bar{W}\) by \(\bar{v} * \bar{w} = \bar{v* w}\). We need to verify that this is well defined:

So let \(v_1 \sim v_2\) and \(w_1 \sim w_2\). Then the previous lemma 2.9.2 \(v_1 * w_1 \sim v_2 * w_1\) and \(v_2 * w_1 \sim v_2 * w_2\). So by transitivity of \(\sim\), \(v_1 * v_2 \sim w_1 * w_2\), as required.
Lemma 2.9.3 [tildewgroup]

(a) \( \tilde{W} \) is a group.

(b) Let \( i \in I \). Then map \( \rho_i : G_i \to W, a \to (\tilde{a}) \) is a homomorphism.

(c) \( \tilde{W} = \langle \rho_i(G_i) \mid i \in I \rangle \).

Proof: As \( W \) is a monoid so is \( \tilde{W} \). By (\( \sim 1 \)), \( \rho_i \) is a homomorphism of monoids. Also \( \rho_i(e) = \tilde{e} = \tilde{w}_0 \) is the identity of \( \tilde{W} \) and it follows that \( \tilde{a} \) is invertible for all \( a \in G_i \), that is for all \( a \in X \). But every element in \( \tilde{W} \) is product of elements in \( \tilde{X} \). Thus (c) holds and all elements in \( \tilde{W} \) are invertible. Hence also (a) is proved.

We have found the group we were looking for. Next we will proceed to find a canonical representative for each of the equivalence classes.

Call a word \( w = (x_1, \ldots, x_n) \) reduced if \( x_k \neq e \) (for all \( 1 \leq k \leq n \)) and \( x_k \) and \( x_{k+1} \) are not comparable (for all \( 1 \leq k < n \)). So \( w \) is not reduced if and only if there exists \( v \in W \) with \( v < w \). Also each \( e \neq a \in G_i \) is reduced. We will show that every equivalence class contains a unique reduced word.

For this we consider one further relation on \( W \). Define \( v \ll w \) if \( v = v_0 < v_1 < v_2 \ldots v_{n-1} < v_n = w \) for some \( v_k \in W \). Again allow for \( n = 0 \) and so \( v \ll v \). Also note that \( v \ll w \) implies \( v \sim w \) (but not vice versa).

Lemma 2.9.4 [reducedwords]

(a) For each \( w \in W \) there exists a unique reduced word \( w_r \in W \) with \( w_r \ll w \). \( w_r \) is called the reduction of \( w \).

(b) \( v \sim w \) if and only \( v_r = w_r \).

(c) Each \( \tilde{w} \) contains a unique reduced word, namely \( w_r \).

Proof: (a) Choose a word \( z \) of minimal length with respect to \( z \ll w \). If \( v < z \) for some \( v \) we conclude \( v \ll w \) and \( l(v) = l(z) - 1 < l(z) \), a contradiction to the minimal choice of \( z \). Hence no such \( v \) exists and \( z \) is reduced. This establishes the existence part. To show uniqueness let \( z_1 \) and \( z_2 \) be reduced with \( z_i \ll w \).

If \( z_1 = w \) then \( w \) is reduced and \( z_2 \ll w \) implies \( z_2 = w = z_1 \). So we may assume that \( z_1 \neq w \neq z_2 \).

By definition of \( " \ll " \) there exists \( v_i \in W \) with \( z_i \ll v_i < w \).

Suppose that \( v_i = w_0 \) for some \( i \in \{1, 2\} \). Then \( w = e \) and \( z_1 = w_0 = z_2 \).

Suppose next that \( v_1 \neq w_0 \neq v_2 \). Then \( v_i < w \) fulfills (1) and there exist \( x_i, y_i \) and comparable \( a_i, b_i \in X \) with

\[
\begin{align*}
v_i &= x_i * a_i b_i * y_i \\
w &= x_i * a_i * b_i * y_i
\end{align*}
\]
Let $l_i$ be the length of $z_i$. Without loss $l_1 \leq l_2$. We will consider various cases.

If $l_1 = l_2$ we get $v_1 = v_2$. As $x_i \prec v_1 = v_2$ and $l(v_1) < l(w)$ we can apply induction and conclude $x_1 = x_2$.

Suppose next that $l_2 = l_1 + 1$. Then $x_2 = x_1 \ast a_1$, $b_1 = a_2$ and $y_1 = b_2 \ast y_2$. So

$$v_1 = x_1 \ast (a_1 a_2) \ast b_2 \ast y_2 \quad \quad v_2 = x_1 \ast a_1 \ast (a_2 b_2) \ast y_2$$

If $a_2 = e$, then $v_1 = x_1 \ast a_1 \ast b_2 \ast y_2 = v_2$ and as above $x_1 = x_2$.

So suppose $a_2 \neq e$. Then $a_1, a_2 = b_1$ and $b_2$ all lie in a common $G_i$. In particular $a_1 a_2$ and $b_2$ are comparable. The same holds for $a_1$ and $a_2 b_2$. Put $u = x_1 \ast (a_1 a_2 b_2) \ast y_2$. It follows that $u < v_1$ and $u < v_2$. Then $x_i \prec v_1, u_r \prec v_i$ and by induction $x_1 = u_r = x_2$.

Finally suppose that $l_1 + 1 < l_2$. Then $x_2 = x_1 \ast a_1 \ast b_1 \ast d$ and $y_1 = e \ast a_2 \ast b_2 \ast y_2$ for some (maybe empty) words $e$ and $d$.

Hence

$$v_1 = x_1 \ast (a_1 a_2) \ast d \ast e \ast a_2 \ast b_2 \ast y_2 \quad \quad v_2 = x_1 \ast a_1 \ast a_2 \ast d \ast e \ast a_2 b_2 \ast y_2$$

Put $u = x_1 \ast (a_1 a_2) \ast d \ast e \ast a_2 b_2 \ast y_2$. Then again $u < v_1$, $u < v_2$ and $x_1 = u_r = x_2$.

This completes the proof of (a).

Let $v, w$ be words. If $v_r = w_r$, then $v \sim v_r = w_r \sim w$ and so $v \sim w$. Conversely suppose that $v \sim w$. By induction on the distance of $v$ and $w$ we may assume that $v - w$ and say $v < w$. Then $v_r \prec w$ and so by (a), $v_r = w_r$. Thus (b) holds.

Let $v$ be any reduced element in $\tilde{w}$. Then $v \sim w$ and so by (b) $v = v_r = w_r$. Thus also (c) holds.

Let $W_r$ be the set of reduced words. By the previous lemma the map $W_r \to \tilde{W}$, $w \to \tilde{w}$ is a bijection. Unfortunately, $W_r$ is not closed under multiplication, that is the product of two reduced words usually is not reduced. But it is not difficult to figure out what the reduction of the product is. Indeed let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_m)$ be reduced words. Let $s$ be maximal with $y_t^{-1} = x_{n-t}$ for all $1 \leq t < s$. Then

$$x \ast y \sim (x_1, \ldots, x_{n-s}, y_s, \ldots, y_m).$$

If $x_{n-s}$ and $y_s$ are not comparable, this is the reduction of $x \ast y$.

On the other hand if $x_{n-s}$ and $y_s$ are comparable we have

$$x \ast y \sim (x_1, \ldots, x_{n-s-1}, x_{n-s} y_s, y_{s+1} \ldots, y_m)$$

and this is the reduction of $x \ast y$.

We now define the free product $\prod_{i \in I} G_i$ of $(G_i, i \in I)$ to be the group $\tilde{W}$ together with the family of homomorphism $(\rho_i, i \in I)$. The free product has the following important property (which we could have used to define the free product).
Theorem 2.9.5 [CoGr] Let $H$ be a group and $(\alpha_i : i \rightarrow H_i)$ a family of homomorphisms. Then there exists a unique homomorphism $\tilde{\alpha} : \coprod_{i \in I} G_i \rightarrow H$ so that the diagram

\[
\begin{array}{ccc}
\coprod_{i \in I} G_i & \xrightarrow{\tilde{\alpha}} & H \\
\rho_i & \downarrow & \\
G_i & \xrightarrow{\alpha_i} & \\
\end{array}
\]

commutes for all $i \in I$.

Proof: We define a map $\alpha : W \rightarrow H$ by induction on length of the words. Put $\alpha(w_0) = e$ and if $w = y \ast g_i$ with $g_i \in G_i$ define $\alpha(w) = \alpha(y)\alpha_i(g_i)$. Clearly $\alpha$ is a homomorphism of monoids. We claim that $\alpha(v) = \alpha(w)$ whenever $v \sim w$. Indeed it suffices to show this for $v \prec w$. Then $w = x \ast a \ast b \ast y$ and $v = x \ast ab \ast y$ with $a, b \in G_i$ for some $i$. Hence

\[
\alpha(w) = \alpha(x)\alpha(a)\alpha(b)\alpha(y) = \alpha(x)(\alpha_i(a)\alpha_i(b)\alpha(y) = \alpha(x)\alpha_i(ab)\alpha(y) = \alpha(x)\alpha(ab)\alpha(y) = \alpha(v).
\]

By the claim we get a well defined map $\tilde{\alpha} : \tilde{W} \rightarrow H, \tilde{w} \rightarrow \alpha(w)$. Also as $\alpha$ is a homomorphism, $\tilde{\alpha}$ is, too. $\tilde{\alpha}$ is unique, as the restriction of $\tilde{\alpha}$ to $\rho_i(G_i)$ is determined by the commuting diagram and as the $\rho_i(G_i)$ generate $\tilde{W}$ (see 2.8.4).

We remark that free products also exists in the categories of semigroups and of monoids. Indeed, everything we did for groups carries over word for word, with one exception though. In case of semigroups we do not include $w_0$ in the sets of words and omit $(<2)$ in the definition of $v \prec w$. Recall that the only role $(<2)$ played was to identify $(e)$ with $w_0$.

A relation in $X$ is an expression of the form $w = e$ where $w$ is a word in $X$. Let $\mathcal{R}$ be a set of words. Define

\[
\coprod_{i \in I} G_i \langle w = e, w \in \mathcal{R} \rangle
\]

to be the group $\tilde{W}/N$, where $N = \langle \mathcal{R} \tilde{W} \rangle$. $\tilde{W}/N$ is called the group generated by $(G_i, i \in I)$ with relation $w = e, w \in \mathcal{R}$. Put

\[
\tilde{\rho}_i : G_i \rightarrow \coprod_{i \in I} G_i \langle w = e, w \in \mathcal{R} \rangle, \quad g \rightarrow \rho_i(g)N
\]

Let $H$ be a group and $(\alpha_i : G_i \rightarrow H, i \in I)$ a family of homomorphism. We say that the family fulfills the relations $w = e, w \in \mathcal{R}$ if $\alpha(w) = e$ for all $w \in W$. Here $\alpha$ is as in the proof of 2.9.5, that is

\[
\alpha((w_1, \ldots, w_n) = \alpha_{i_1}(w_1) \ldots \alpha_{i_n}(w_n)
\]

where $w_j \in G_{i_j}$.
Theorem 2.9.6 [productrelation] Let $H$ be a group and $(\alpha_i : G_i \to H, i \in I)$ a family of homomorphism which fulfills the relations $w = e, w \in R$. Then there exists a unique homomorphism

$$\tilde{\alpha} : \prod_{i \in I} G_i/\langle w = e, w \in R \rangle \to H$$

with $\tilde{\rho}(g_i) = \alpha_i(g_i)$

for all $g_i \in G_i, i \in I$.

**Proof:** By 2.9.5 there exists a unique homomorphism $\bar{\alpha} : \prod_{i \in I} G_i \to H$ with $\bar{\alpha}(\rho(g_i)) = \alpha_i(g_i)$. Since $(\alpha_i, i \in I)$ fulfills the relations, $R \leq \ker \alpha$ and so $N \leq \ker \bar{\alpha}$. Thus the map $\bar{\alpha} : \tilde{W}/N \to H, gN \to \alpha(g)$ is well defined and has all the desired properties. The uniqueness of $\bar{\alpha}$ follows from the uniqueness of $\tilde{\alpha}$. \hfill \Box

We will now work out an easy example. Let $I = 1, 2$ and suppose $G_1$ and $G_2$ are both of order 2. Let $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$. Then it is easy to list all the reduced words:

\[
\begin{align*}
& w_0 \\
& (a*b)*(a*b)*\ldots*(a*b) \\
& \quad \text{\underbrace{\quad \text{n times}}} \\
& (b*a)*(b*a)*\ldots*(b*a) \\
& \quad \text{\underbrace{\quad \text{n times}}} \\
& (a*b)*(a*b)*\ldots*(a*b)*a \\
& \quad \text{\underbrace{\quad \text{n times}}} \\
& (b*a)*(b*a)*\ldots*(b*a)*b \\
& \quad \text{\underbrace{\quad \text{n times}}}
\end{align*}
\]

Put $z = a*b$. Then $z^{-1} = b^{-1}a^{-1} = b*a$. So the above list now reads $z^n, z^{-n}, z^n*a$ and $z^{-n}*b$. The last words is equivalent to $z^{-n}*b*(a*a) = z^{-(n+1)}*a$. Let $D = \prod_{i \in \{1, 2\}} G_i$. We conclude that

$$D = \{z^n, z^n*a \mid n \in \mathbb{Z}\}.$$ 

Let $Z = \langle z \rangle$. Then $Z \cong (\mathbb{Z}, +)$ and $Z$ has index two in $G_1 * G_2$. In particular $Z \trianglelefteq D$. Also $z^a = aza = aaba = ba = z^{-1}$. Thus

$$z^a = z^{-n} \quad \text{and} \quad z^n*a = az^{-n}.$$ 

In particular, if $A \leq Z$ then both $Z$ and $a$ normalize $D$ and $A \trianglelefteq G$.

Here is a property of $D$ which will come in handy later on:

All elements in $D \setminus Z$ are conjugate to $a$ or $b$.

Indeed $z^naz^{-n} = z^n z^n*a = z^{2n}a$ and $z^n b z^{-n} = z^{2n}b = z^{2n}baa = z^{2n+1}a$. So $z^{2n}a$ is conjugate to $a$ and $z^{2n+1}a$ is conjugate to $b$. 


Fix \( n \in \mathbb{Z} \). Consider the relation \( z^n = e \). Put \( N = \langle z^n \rangle \). Then \( N \trianglelefteq D \) and so

\[
\prod_{i \in \{1, 2\}} G_i / \langle (ab)^n = e \rangle = D / N
\]

Since \( Z / D \cong \mathbb{Z} / n\mathbb{Z} \), \( D / N \) has order \( 2n \). \( D / N \) is called the dihedral group of order \( 2n \), or the dihedral group of degree \( n \).

Suppose now that \( \bar{D} \) is any group generated by two elements of order two, \( \bar{a} \) and \( \bar{b} \). Then there exists a homomorphism \( \alpha : D \to \bar{D} \) sending \( a \) to \( \bar{a} \) and \( b \) to \( \bar{b} \). Let \( \bar{z} = \bar{a}\bar{b} \) and \( \bar{z} = \langle \bar{z} \rangle \). Since neither \( a \) nor \( b \) are in \( \ker \alpha \) and all elements in \( D \setminus Z \) are conjugate to \( a \) or \( b \), \( \ker \alpha \leq Z \). Thus \( \ker \alpha = \langle z^n \rangle \) for some \( n \in \mathbb{N} \) and so \( \bar{D} \cong D / \ker \alpha = D / N \). So any group generated by two elements of order 2 is a dihedral group.

Next we will use the free products of groups to define the free group \( F(I) \) on a set \( I \).

First for each \( i \in I \) pick a group \( G_i \) with \( i \in G_i \), \( G_i \cong (\mathbb{Z}, +) \) and \( G_i = \langle i \rangle \). So

\[
G_i = \{ i^n \mid n \in \mathbb{Z} \}.
\]

Then let

\[
F(I) = \prod_{i \in I} G_i.
\]

and define

\[
\rho : I \to F(I), \quad i \to \tilde{i}.
\]

Identify \( i \) and \( \tilde{i} \). Then every element in \( F(I) \) can by uniquely written as

\[
i_1^{n_1}i_2^{n_2} \ldots i_m^{n_m}
\]

where \( m \in \mathbb{N} \), \( i_k \in I \), \( i_k \neq i_{k+1} \) and \( 0 \neq n_k \in \mathbb{Z} \). Indeed these are exactly the reduced words.

**Theorem 2.9.7** [freegroup] Let \( I \) be a set and \( H \) a group. For \( i \in I \) let \( h_i \in H \). Then there exists a unique homomorphism \( \alpha : F(I) \to H \) with \( \alpha(i) = h_i \).

**Proof:** Define \( \alpha_i : G_i \to H, i^n \to h_i^n \). The theorem now follows from 2.9.5 \( \square \)

The concept of relations also carries over. For \( \mathcal{R} \) a set of words define

\[
F(I) / \langle w = e, w \in \mathcal{R} \rangle := F(I) / N,
\]

where \( N = \langle \tilde{R}^{F(I)} \rangle \). \( F(I) / \langle w = e, w \in \mathcal{R} \rangle \) is called the groups defined by the generators \( i \in I \) and relations \( w = e, w \in \mathcal{R} \). Often this group is also denoted by

\[
\langle I \mid w = e, w \in \mathcal{R} \rangle
\]

For \( i \in I \), put \( \tilde{i} = iN \).
CHAPTER 2. GROUP THEORY

Let $H$ be a group, and $h_i \in H$. We say that $(h_i, i \in I)$ fulfills the relations $w = e$ provide that

$$h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = e$$

where $w = (i_1^{n_1}, i_2^{n_2}, \ldots, i_m^{n_m})$.

**Theorem 2.9.8** [genrel] Let $H$ be a group and $(h_i, i \in I)$ a family of elements in $H$ fulfilling the relations $w = e, w \in \mathcal{R}$. Then there exists a unique homomorphism

$$\bar{\alpha} : \langle I \mid w = e, w \in \mathcal{R} \rangle \to H$$

with $\bar{i} \to h_i$ for all $i \in I$. $\bar{\alpha}$ is onto, if and only if $H = \langle h_i \mid i \in I \rangle$.

**Proof:** The first statement follows directly from 2.9.6. The second one follows from 2.5.8.

**Some examples:**

The group

$$\langle a, b \mid a^2 = e, b^2 = e \rangle$$

is the infinite dihedral group.

$$\langle a, b \mid a^2 = 2, b^2 = e, (ab)^n = e \rangle$$

is the dihedral group of degree $n$.

If $v$ and $w$ are words, we also call $v = w$ relations. It just stands for $vw^{-1} = e$, where $(i_1^{n_1}, \ldots, i_m^{n_m})^{-1} = (i_m^{-n_m}, \ldots, i_1^{-n_1})$.

$$\langle a, b, c \mid ab = c, ab = ba, c^2 = a, c^3 = b, c^5 = e \rangle$$

is the trivial group. Indeed, $c = ab = c^2 c^3 = c^5 = e$. Hence also $a = c^2 = e$ and $b = c^2 = e$.

$$\langle a, b \mid a^3 = b^3 = (ab)^2 = e \rangle$$

is isomorphic to $Alt(4)$. To see this let $G$ be this group and put $z = ab$. Then $z^2 = 1$. Put $K = \langle z, z^a \rangle$. Since both $z$ and $z^a$ have order two (or 1), $K$ is a dihedral group. We compute

$$z^a z^a z = (a^2 (ab)a^{-2}) a(ab)a^{-1} ab = a^3 b(a^{-2}a^2)b(a^{-1}a)b = a^3 b^2 = e.$$  

Thus $z^2 = z^{-a^2} = z a^2$. In particular $(z^a z)^2 = 1$ and so $K$ is a quotient of the dihedral group of order 4. Thus $K = \{e, z, z^a, z^{a^2}\}$. Now $(z^{a^2})^a = z^{a^3} = z^e = z$ and so $a \in N_G(K)$. Thus $\langle a \rangle K$ is a subgroup of $G$. It contains $a$ and $z = ab$ and so also $b = a^{-1} z$.

Thus $G = \langle a \rangle K$. As $K$ has order dividing 4 and $\langle a \rangle$ has order dividing 3, $G$ has order dividing 12. Thus to show that $G$ is isomorphic to $Alt(4)$ it suffices to show that $Alt(4)$ is a homomorphic image of $G$. I.e we need to verify that $Alt(4)$ fulfills the relations.
For this let \( a^* = (123) \) and \( b^* = (124) \). Then \( a^*b^* = (13)(24) \) and so \((a^*b^*)^2 = e\). Thus there exists a homomorphism \( \phi : G \to \text{Alt}(4) \) with \( \phi(a) = a^* \) and \( \phi(b) = b^* \). As \( a^* \) and \( b^* \) generate \( \text{Alt}(4) \), \( \phi \) is onto. As \( |G| \leq |\text{Alt}(4)| \) we conclude that \( \phi \) is an isomorphism.

Similarly to the free group on a set one can define the free semigroup and the free monoid on a set \( I \). If \( |I| = 1 \) these are \( (\mathbb{Z}^+, +) \) and \( (\mathbb{N}, +) \), respectively. In the general case every element in the free semigroup (free monoid) can be uniquely written as

\[ i_1^{n_1}i_2^{n_2} \ldots i_m^{n_m} \]

where \( i_k \in I, \ i_k \neq i_{k+1} \) and \( n_k \in \mathbb{Z}^+ \). Also \( m \in \mathbb{Z}^+ \) in the semigroup case and \( m \in \mathbb{N} \) in the monoid case.

### 2.10 Group Actions

#### Definition 2.10.1 [defgroupaction] An action of a group \( G \) on a set \( S \) is a function

\[ G \times S \to S, (a, s) \to as \]

such that

- \((GA1) \ es = s\) for all \( s \in S \).
- \((GA2) \ (ab)s = a(bs)\) for all \( a, b \in G, \ s \in S \).

Note the similarity with the group multiplication. In particular, the binary operation of a group defines an action of \( G \) on \( G \), called the action by left multiplication. The function \((a, s) \to a*s := sa\) is not an action (unless \( G \) is abelian) since \( ab*s = sab = (a*s)b = (b*a)s \). For this reason we define the action of \( G \) on \( G \) by right multiplication as \((a, s) \to sa^{-1}\).

There is a further action of \( G \) on itself, namely the conjugation \((a, s) \to s^a = asa^{-1}\).

It might be interesting to notice that an action of \( G \) on a set \( S \) can also be thought of as an homomorphism \( \phi : G \to \text{Sym}(S) \). Indeed given such a \( \phi \) define an action by \((a, s) \to \phi(a)(s)\). Since \( \phi(e) = e_{\text{Sym}(S)} = \text{id}_S \), \((GA1)\) holds. And \((GA2)\) follows directly from \( \phi(ab) = \phi(a) \circ \phi(b) \).

Conversely, given an action of \( G \) on \( S \) and \( a \in G \), define \( \phi(a) : S \to S, s \to as \). \((GA2)\) translates into \( \phi(ab) = \phi(a) \circ \phi(b) \) and \((GA1)\) into \( \phi(e) = \text{id}_S \). We still need to verify that \( \phi(a) \in \text{Sym}(S) \). But this follows from

\[ \text{id}_S = \phi(e) = \phi(aa^{-1}) = \phi(a) \circ \phi(a^{-1}) \]

For \( X \subseteq S \) define

\[ \text{Stab}_G(X) = \{ g \in G \mid gs = s \text{ for all } s \in X \} \]
Then \( \text{Stab}_G(S) \) is exactly the kernel of \( \phi \) and in particular it is a normal subgroup. By the isomorphism theorem,

\[
G / \text{Stab}_G(S) \cong \phi(G) \leq \text{Sym}(S).
\]

If \( \text{Stab}_G(S) = \{e\} \), we say that the action is faithful. This is the case if and only if \( \phi \) is one. So in some sense the groups acting faithfully on a set \( S \) are just the subgroups of \( \text{Sym}(S) \).

There are lots of actions of groups besides the actions on itself. For example \( \text{Sym}(S) \) acts on \( S \). The automorphism group of the square acts on the four corners of the square. The automorphism group of a projective plane acts on the points and also on the lines of the plane. The group of invertible matrices acts on the underlying vector space.

For the rest of the section we assume:

**Hypothesis 2.10.2** \( G \) is a group acting on a set \( S \).

**Lemma 2.10.3** [orbits] Define a relation \( \sim \) on \( S \) by \( s \sim t \) if and only if \( t = as \) for some \( a \in G \). Then \( \sim \) is an equivalence relation on \( S \).

**Proof:** Since \( s = es \), \( s \sim s \) and \( \sim \) is reflexive.

If \( t = as \), then

\[
a^{-1}t = a^{-1}(as) = (a^{-1}a)s = es = s
\]

Thus \( s \sim t \) implies \( t \sim s \) and \( \sim \) is symmetric.

Finally if \( s = at \) and \( t = br \) then \( s = at = a(br) = (ab)r \). Thus \( s \sim t \) and \( t \sim r \) implies \( s \sim r \) and \( \sim \) is reflexive. \( \Box \)

The equivalence classes of \( \sim \) are called the **orbits** of \( G \) on \( S \). The set of orbits is denoted by \( S/G \). The orbit of \( G \) containing \( s \) is \( Gs = \{gs : g \in G\} \). A subset \( T \) of \( S \) is called **\( G \)-invariant** if \( gt \in T \) for all \( t \in T \) and \( g \in G \). In this case \( G \) also acts on \( T \). Observe that the orbits of \( G \) on \( S \) are the minimal \( G \) invariant subsets. We say that \( G \) acts **transitively** on \( S \) if \( G \) has exactly one orbit on \( S \). That is for each \( s, t \in S \) there exists \( g \in G \) with \( t = gs \). Equivalently \( G \) is transitive on \( S \) if \( S = Gs \) for some (or all) \( s \in S \). So the \( G \)-orbits can be also described as subsets of \( S \) on which \( G \) acts transitively.

Some special cases of orbits: Let \( H \leq G \). The right cosets of \( H \) are the orbits for the action of \( H \) on \( G \) by left multiplication. The left cosets are the orbits for \( H \) by the right multiplication. Finally the conjugacy classes are the orbits for the action \( G \) on \( G \) by conjugation.

**Definition 2.10.4** Let \( G \) be acting on the sets \( S \) and \( T \) and \( \alpha : S \to T \) a function.

(a) \( \alpha \) is called **\( G \)-equivariant** if

\[
\alpha(gs) = g\alpha(s)
\]

for all \( g \in G \) and \( s \in S \).

(b) \( \alpha \) is called a **\( G \)-isomorphism** if \( \alpha \) is \( G \)-equivariant and an bijection.
If $G$ acts on a set $S$ it also acts on the power set $\mathcal{P}(S)$, that is the set of all subsets. Indeed for $T \subseteq S$ and $g \in G$ put $gT = \{gt | t \in T\}$.

If $H \leq G$ then $G$ acts on $G/H$ by $(a,bH) \rightarrow abH$. Clearly this is a transitive action. It turns out that any transitive action of $G$ is isomorphic to the action on the coset of a suitable subgroup.

**Lemma 2.10.5 [transorbits]** Let $s \in S$ and put $H = \text{Stab}_G(s)$.

(a) The map

$$\alpha : G/H \rightarrow S, aH \rightarrow as$$

is well defined, $G$-equivariant and one to one.

(b) $\alpha$ is an $G$-isomorphism if and only if $G$ acts transitively on $S$

(c) $\text{Stab}(as) = H^a$ for all $a \in G$.

(d) If $G$ is transitive on $S$, $|S| = |G/\text{Stab}_G(s)|$.

**Proof:**

(a) Let $h \in H$. Then $(ah)s = a(hs) = as$ and $\alpha$ is well defined. Also

$$\alpha(a(bH)) = \alpha((ab)H) = (ab)s = a(bs) = a\alpha(bH)$$

So $\alpha$ is $G$-equivariant. If $\alpha(aH) = \alpha(bH)$ we get $as = bs$ so $(a^{-1}b)s = s$. As $H = \text{Stab}_G(s)$ this implies $a^{-1}b \in H$ and so $b \in aH$ and $bH = aH$. Thus $\alpha$ is one to one and (a) is established.

(b) By (a) $\alpha$ is a $G$-isomorphism if and only if $\alpha$ is onto. But this is the case exactly then $S = Gs$ and so if and only if $G$ is transitive on $S$.

(c) $g(as) = as \iff a^{-1}gas = s \iff a^{-1}ga \in H \iff g \in aHa^{-1} = H^a$

(d) follows directly from (b) \qed

**Lemma 2.10.6** Suppose that $G$ acts transitively on the sets $S$ and $T$. Let $s \in S$ and $t \in T$. Then $S$ and $T$ are $G$-isomorphic if only if $\text{Stab}_G(s)$ and $\text{Stab}_G(t)$ are conjugate in $G$.

**Proof:** Suppose first that $\alpha : S \rightarrow T$ is a $G$-isomorphism. Since $\alpha(gs) = g\alpha(s)$ and $\alpha$ is one to one, $\text{Stab}_G(s) = \text{Stab}_G(\alpha(s))$. Since $G$ is transitive on $T$, there exists $h \in G$ with $ga(s) = t$. Thus

$$\text{Stab}_G(t) = \text{Stab}_G(g\alpha(s)) = \text{Stab}_G(\alpha(s))^g = \text{Stab}_G(s)^g.$$ 

Conversely suppose that $\text{Stab}_G(s)^g = \text{Stab}_G(t)$. Then $\text{Stab}_G(gs) = \text{Stab}_G(t)$ and so by 2.10.5b applied to $S$ and to $T$:

$$S \cong G/\text{Stab}_G(gs) = G/\text{Stab}_G(t) \cong T$$
A subset $R \subset S$ is called a set of representatives for the orbits on $S$, provided that $R$ contains exactly one element from each $G$-orbit. In other words the map $R \to S/G, r \to Gr$ is a bijection. An element $s \in S$ is called a fixed-point of $G$ if $gs = s$ for all $g \in G$. The fixed points correspond to the orbits of length 1 (the trivial orbits). $\text{Fix}_S(G)$ denotes the set of all fixed points. Note that $\text{Fix}_S(G) \subseteq R$ for any set of representatives $R$ for $S/G$ and $R \setminus \text{Fix}_G(R)$ is a set of representatives for the non-trivial $G$-orbits.

**Lemma 2.10.7** [orbiteq] Let $R \subset S$ be a set of representatives for $S/G$.

$$|S| = \sum_{r \in R} |G/\text{Stab}_G(r)| = |\text{Fix}_S(G)| + \sum_{r \in R \setminus \text{Fix}_S(G)} |G/\text{Stab}_G(r)|$$

**Proof:** Since $S$ is the disjoint unions of its orbits, $|S| = \sum_{r \in R} |Gr|$. By 2.10.5d, $|Gr| = |G/\text{Stab}_G(r)|$ and the lemma is proved. 

For the case of conjugation the equation in the preceding lemma is called the class equation. Define the center $Z(G)$ of a group by

$$Z(G) = \{ g \in G \mid gh = hg \text{ for all } h \in G \}.$$ 

Note that $g$ is a fixed-point for $G$ under conjugation if and only if $g = g^h = hgh^{-1}$ for all $h \in G$ and so if only if $gh = hg$ for all $h \in G$. That is $\text{Fix}_G(G) = Z(G)$. Also setting $C_G(a) = \{ b \in G \mid ba = ba \}$ we have $G_G(a) = \text{Stab}_G(a)$. With this notation we have:

**Lemma 2.10.8** (Class Equation) [classeq] Let $R$ be a set of representatives for the conjugacy classes of $G$. Then

$$G = \sum_{r \in R} |G/C_G(r)| = |Z(G)| + \sum_{r \in R \setminus Z(G)} |G/C_G(r)|$$

These formulas become particular powerful if $G$ is a finite $p$-group, that is $|G| = p^k$ for some non-negative integer $k$.

**Lemma 2.10.9** [Smodp] Let $p$ be a prime and $P$ a $p$-group acting on a set $S$. Then

$$|S| \equiv |\text{Fix}_S(P)| \pmod{p}.$$ 

**Proof:** If $s \in S$ is not a fixed-point, then $\text{Stab}_P(s) \leq P$ and so

$$|P/\text{Stab}_P(s)| = \frac{|P|}{|\text{Stab}_P(s)|} \equiv 0 \pmod{p}.$$
2.10. GROUP ACTIONS

The lemma now follows from 2.10.7. □

For $H \leq G$ define $N^*_G(H) = \{a \in G \mid H \leq H^a\}$. Note that $N^*_G(H)$ is submonoid of $G$, but not necessarily a subgroup, as it might not be closed under inverses.

Lemma 2.10.10 [HfixG] Let $H \leq G$.

(a) The fixed-points of $H$ acting by left multiplication on $G/H$ are $N^*_G(H)/H$.

(b) With respect to the action of $G$ on the subgroups of $G$ by conjugation, $\text{Stab}_G(H) = N_G(H)$.

(c) If $H$ is finite, then $N^*_G(H) = N_G(H)$.

Proof: (a) Clearly $gH = H$ if and only if $g \in H$. So $\text{Stab}_G(H) = H$ and $\text{Stab}_G(aH) = H^a$. Hence $H$ fixes $aH$ if and only if $H \leq H^a$, that is if and only if $a \in N^*_G(H)$. Thus (a) holds.

(b) Obvious.

(c) As conjugation is an bijection, $|H| = |H^g|$. So for finite $H$, $H \leq H^g$ implies $H = H^g$. □

Lemma 2.10.11 [CenterP] Let $P$ be a non-trivial $p$-group.

(a) $Z(P)$ is non-trivial.

(b) If $H \leq P$ then $H \leq N_P(H)$.

Proof: (a) Consider first the action by conjugation. By 2.10.9

$$0 \equiv |P| \equiv |Z(P)| \pmod{p}.$$ 

Thus $|Z(P)| \neq 1$.

(b) Consider the action of $H$ on $P/H$. By 2.10.10 and 2.10.9

$$0 \equiv |P/H| \equiv |N_P(H)/H| \pmod{p}.$$ 

So $|N_P(H)/H| \neq 1$. □

As a further example how actions an set can be used we give a second proof that $\text{Sym}(n)$ has normal subgroup of index two. For this we first establish the following lemma.

Lemma 2.10.12 [equivrep] Let $\Delta$ be a finite set and $\sim$ a non-trivial equivalence relation on $\Delta$ so that each equivalence class has size at most 2. Let

$$\Omega = \{R \subseteq \Delta \mid R \text{ contains exactly one element from each equivalence class of } \sim\}.$$ 

Define the relation $\approx$ on $\Omega$ by $R \approx S$ if and only if $|R \setminus S|$ is even. Then $\approx$ is an equivalence relation and has exactly two equivalence classes.
\textbf{Proof:} For $d \in \Delta$ let $\tilde{d}$ be the equivalence class of $\sim$ containing $d$ and let $\tilde{\Delta}$ be the set of equivalence classes. Let $A, B \in \Omega$ and define

$$\tilde{\Delta}_{AB} = \{X \in \tilde{\Delta} \mid A \cap X \neq B \cap X\}.$$ 

Let $d \in A$. Then $d \not\in B$ if and only if $A \cap \tilde{d} \neq B \cap \tilde{d}$. So $|A \setminus B| = |\tilde{\Delta}_{AB}|$ and

$$A \approx B \iff \tilde{\Delta}_{AB} \text{ is even}.$$ 

In particular, $\approx$ is reflexive and symmetric. Let $R, S, T \in \Omega$. Let $X \in \tilde{\Delta}$. Then $X \cap R \neq X \cap T$ exactly if either $X \cap R \neq X \cap S = X \cap T$ or $X \cap R = X \cap S \neq X \cap T$.

Thus

$$\tilde{\Delta}_{RT} = (\tilde{\Delta}_{RS} \setminus \tilde{\Delta}_{ST}) \cup (\tilde{\Delta}_{ST} \setminus \tilde{\Delta}_{RS}).$$

Hence

$$(*) \quad |\tilde{\Delta}_{RT}| = |\tilde{\Delta}_{RS}| + |\tilde{\Delta}_{ST}| - 2|\tilde{\Delta}_{RS} \cap \tilde{\Delta}_{ST}|.$$ 

If $R \approx S$ and $S \approx T$, the right side of $(*)$ is an even number. So also the left side is even and $R \approx T$.

So $\approx$ is an equivalence relation. Let $R \in \Omega$. As $\sim$ is not trivial there exist $r, t \in \Delta$ with $r \sim t$ and $r \neq t$. Exactly one of $r$ and $t$ is in $R$. Say $r \in R$. Let $T = (R \cup \{t\}) \setminus \{r\}$. Then $T \in \Omega$ and $|T \setminus R| = 1$. Thus $R$ and $T$ are not related under $\approx$. Let $S \in \Omega$. Then the left side of $(*)$ odd and so exactly one of $|\tilde{\Delta}_{RS}|$ and $|\tilde{\Delta}_{ST}|$ is even. Hence $S \approx R$ or $S \approx T$. Thus $\approx$ has exactly two equivalence classes and all the parts of the lemma are proved. \hfill \ensuremath{\Box}

Back to $\text{Sym}(n)$. Let $\Delta = \{(i, j) \mid 1 \leq i, j \leq n, i \neq j\}$. Then $\text{Sym}(n)$ acts on $\Delta$. Define $(i, j) \sim (k, l)$ iff $(k, l) = (i, j)$ or $(k, l) = (j, i)$. Define $\Omega$ as in the previous lemma. Clearly $\text{Sym}(n)$ acts on $\Omega$ and also on $\Omega/\approx$ (the set of equivalence classes of $\approx$). Let $R = \{(i, j) \mid 1 \leq i < j \leq n\}$. Then $R \in \Omega$. The 2-cycle $(1, 2)$ maps $R$ to $(R \cup \{(2, 1)\}) \setminus \{(1, 2)\}$. Thus $R$ and $(1, 2)R$ are not related under $\approx$ and so $\text{Sym}(n)$ acts non trivially on $\Omega/\approx$, which is a set of size 2. The kernel of the action is a normal subgroup of index two.

\textbf{Lemma 2.10.13 [2odd]} Let $G$ be a finite group of order $2n$ with $n$ odd. Then $G$ index a normal subgroup of index 2.

\textbf{Proof:} View $G$ has a subgroup of $\text{Sym}(G)$ via the action of $G$ on $G$ by right multiplication. Let $t \in G$ be an element of order 2. Since $t$ has no fix-points on $G$, $t$ has $n$ orbits of length 2. Thus $t$ is the product of an odd number of 2-cycles and so $\text{sgn}(t) = -1$. Hence $\ker \text{sgn} |G$ is a normal subgroup of index 2. \hfill \ensuremath{\Box}

The following lemma is an example how the actions on a subgroup can be used to identify the subgroup.

\textbf{Lemma 2.10.14 [sym5]}
(a) Let $H \leq \text{Sym}(6)$ with $|H| = 120$. Then $H \cong \text{Sym}(5)$.

(b) Let $H \leq \text{Alt}(6)$ with $|H| = 60$. Then $H \cong \text{Alt}(5)$.

Proof: Let $G = \text{Sym}(6)$ in (a) and $G = \text{Alt}(6)$ is case (b). In both cases $|G/H| = \frac{6!}{30} = 6$. Let $I = G/H$. Then $G$ acts on $I$ by left multiplication. Let $\phi : G \to \text{Sym}(I)$ be the resulting homomorphism. Since $\text{Stab}_G(H) = H$, ker $\phi \leq H$ and so ker $\phi \neq \text{Alt}(6)$ and ker $\phi \neq \text{Sym}(6)$. Also ker $\phi$ is a normal subgroup of $G$ and we conclude from 2.7.5 that ker $\phi = \{e\}$. Thus $\phi$ is one to one and so $|\phi(G)| = |G| \in \{6!, \frac{6!}{2}\}$. Since $\text{Sym}(I) \cong \text{Sym}(6)$ we conclude that $\phi(G)$ has index 1 or 2 in $\text{Sym}(I)$. Therefore $\phi(G) \leq G$. Thus $\phi(G) = \text{Sym}(I)$ in case (a) and $\phi(G) = \text{Alt}(I)$ in case (b). Note that $\phi(H)$ fixes an element $i$ in $I$, namely $i = H$. Thus $\phi(H) \leq \text{Stab}_{\text{Sym}(I)}(i)$.

Suppose that (a) holds. Note that $\text{Stab}_{\text{Sym}(I)}(i) \cong \text{Sym}(5)$, $|\text{Sym}(5)| = |H|$ and $\phi$ is one to one. Thus $\phi(H) = \text{Stab}_{\text{Sym}(I)}(i)$ and $H \cong \text{Sym}(5)$.

Suppose that (b) holds. The same argument as above shows $\phi(H) = \text{Stab}_{\text{Alt}(I)}(i)$ and $H \cong \text{Alt}(5)$. $\Box$

We remark that although any subgroup $H$ of order 120 in $\text{Sym}(6)$ is isomorphic to $\text{Sym}(5)$ it does not have to be one of $\text{Sym}(5)$’s in $\text{Sym}(6)$ which fix some $k$ in $\{1, 2, 3, 4, 5, 6\}$. Indeed there does exist one which acts transitively on the six elements. (To see this consider the action of $\text{Sym}(5)$ on its six cyclic subgroups of order 5).

On the other hand the above proof says that $H$ fixes a point $i$ in the set $I$. This seems to be contradictory, but isn’t. The set $I$ is a set with six elements on which $\text{Sym}(6)$ acts but it is not isomorphic to the set $\{1, 2, 3, 4, 5, 6\}$. $\text{Sym}(6)$ has two non-isomorphic action on sets of size six. Luckily this only happens for $\text{Sym}(6)$ and not for any other $\text{Sym}(n)$, but we will not prove this.

2.11 Sylow $p$-subgroup

In this section $G$ is a finite group and $p$ a prime. A $p$-subgroup of $G$ is a subgroup $P \leq G$ which is a $p$-group. A Sylow $p$-subgroup $P$ of $G$ is a maximal $p$-subgroup of $G$. That is $P$ is a $p$-subgroup and if $P \leq Q$ for some $p$-subgroup $Q$, then $P = Q$. Let $\text{Syl}_p(G)$ be the set of all Sylow $p$-subgroups of $G$. For the following it will be important to realize that $G$ acts on $\text{Syl}_p(G)$ by conjugation. The following lemma implies that $G$ acts on $\text{Syl}_p(G)$ by conjugation.

Lemma 2.11.1 Let $P \in \text{Syl}_p(G)$ and $\alpha \in \text{Aut}(G)$. Then $\alpha(P) \in \text{Syl}_p(G)$.

Proof: Since $\alpha$ is an bijection, $|P| = |\alpha(P)|$ and so $\alpha(P)$ is a $p$-group. Let $\alpha(P) \leq Q$, $Q \leq G$ a $p$-group. Then $P \leq \alpha^{-1}(Q)$ and the maximality of $P$ implies $P = \alpha^{-1}(Q)$. Thus $\alpha(P) = Q$ and $\alpha(P)$ is indeed a maximal $p$-subgroup of $G$. $\Box$
Theorem 2.11.2 (Cauchy) \[ \text{Cauchy} \] Let \( G \) be a finite group, and \( p \) a prime dividing the order of \( G \). Then \( G \) has an element of order \( p \).

Proof: Let \( X = \langle x \rangle \) be any cyclic group of order \( p \). Then \( X \) acts on \( G^p \) by

\[
x^k \ast (a_1, \ldots, a_p) = (a_{1+k}, a_{2+k}, \ldots, a_p, a_1, \ldots, a_k).
\]

Consider the subset

\[
S = \{(a_1, \ldots, a_p) \in G^p \mid a_1 a_2 \ldots a_p = e\}.
\]

Note that we can choose the first \( p - 1 \) coordinates freely and then the last one is uniquely determined. So \( |S| = |G|^{p-1} \).

We claim that \( S \) is \( X \)-invariant. For this note that

\[
(a_1 a_2 \ldots a_p)^{a_1^{-1}} = a_1^{-1}(a_1 \ldots a_p) a_1 = a_2 \ldots a_p a_1.
\]

Thus \( a_1 a_2 \ldots a_p = e \) if and only if \( a_2 \ldots a_p a_1 = e \). So \( X \) acts on \( S \).

From 2.10.9 we have

\[
|S| \equiv |\text{Fix}_S(X)| \pmod{p}
\]

As \( p \) divides \( |G| \), it divides \( |S| \) and so also \( |\text{Fix}_S(X)| \). Hence there exists some \((a_1, a_2, \ldots, a_p) \in \text{Fix}_S(X)\) distinct from \((e, e, \ldots, e)\). But being in \( \text{Fix}_S(X) \) just means \( a_1 = a_2 = \ldots a_p \). Being in \( S \) implies \( a_1^p = a_1 a_2 \ldots a_p = e \). Therefore \( a_1 \) has order \( p \).

\[ \square \]

Theorem 2.11.3 (Sylow) \[ \text{sylow} \] Let \( G \) be a finite group, \( p \) a prime and \( P \in \text{Syl}_p(G) \).

(a) All Sylow \( p \)-subgroups are conjugate in \( G \).

(b) \( |\text{Syl}_p(G)| = |G/N_G(P)| \equiv 1 \pmod{p} \).

(c) \( |P| \) is the largest power of \( p \) dividing \( |G| \).

(d) Every \( p \)-subgroup of \( G \) is contained in a Sylow \( p \)-subgroup of \( G \).

Proof: Let \( S = P^G = \{P^g \mid g \in G\} \), the set of Sylow \( p \)-subgroups conjugate to \( P \). First we show

1. \( P \) has a unique fixed point on \( S \) and on \( \text{Syl}_p(G) \), namely \( P \) itself.

   Indeed, suppose that \( P \) fixes \( Q \in \text{Syl}_p(G) \). Then \( P \leq N_G(Q) \) and \( PQ \) is a subgroup of \( G \). Now \(|PQ| = \frac{|P||Q|}{|P \cap Q|}\) and so \( PQ \) is a \( p \)-group. Hence by maximality of \( P \) and \( Q \) \( P = PQ = Q \).

2. \( S \equiv 1 \pmod{p} \)

   By (1) \( \text{Fix}_S(P) = 1 \) and so (2) follows from 2.10.9.
(3) \( \text{Syl}_p(G) = \mathcal{S} \)

Let \( Q \in \text{Syl}_p(G) \). Then \(|\text{Fix}_G(Q)| \equiv |\mathcal{S}| \equiv 1 \pmod{p}\). Hence \( Q \) has a fixed point \( T \in \mathcal{S} \). By (2) applied to \( Q \), this fixed-point is \( Q \). So \( Q = T \in \mathcal{S} \).

Note that \( N_G(P) \) is the stabilizer of \( P \) in \( G \) with respect to conjugation. As \( G \) is transitive on \( \mathcal{S} \) we conclude \(|\mathcal{S}| = |G/N_G(P)|\). Thus (2) and (3) imply (a) and (b).

(4) \( p \) does not divides \(|N_G(P)/P|\).

Suppose it does. Then by Cauchy’s theorem \( N_G(P)/P \) has a non-trivial \( p \)-subgroup \(|Q/P|\). Since \(|Q| = |Q/P||P|\), \( Q \) is a \( p \)-group with \( P \leq Q \), a contradiction to the maximality of \( P \).

By (b) and (4) \( p \) divides neither \(|G/N_G(P)|\) nor \(|N_G(P)/P|\). Since

\[|G| = |G/N_G(P)|\cdot|N_G(P)/P||P|\]

(c) holds.

\(|G|\) is finite so any \( p \)-subgroup of \( G \) lies in a maximal \( p \)-subgroup, proving (d). \(\square\)

As an application of Sylow’s theorem we will investigate groups of order 12,15,30 and 120. We start with a couple of general observation.

**Lemma 2.11.4 [easysylow]** Let \( G \) be a finite group, \( p \) a prime, and \( P \in \text{Syl}_p(G) \). Also let \( N \) the kernel of the action of \( G \) on \( \text{Syl}_p(G) \).

(a) \(|\text{Syl}_p(G)|\) divides \(|G|\) and equals \(|G/P|\) \pmod{p}.

(b) \( P \leq PN \). In particular, \( P \) is the unique Sylow \( p \)-subgroup of \( PN \).

(c) \( N \cap P \in \text{Syl}_p(N) \) and \( N \cap P \leq G \). In particular \( P \leq N \) if and only if \( P \leq G \).

(d) \( PN/N \in \text{Syl}_p(G/N) \). Moreover the map

\[\text{Syl}_p(G) \to \text{Syl}_p(G/N) \quad Q \to QN/N\]

is a bijection.

**Proof:**

(a) Follows directly from 2.11.3b.

(b) Just note that \( N \leq N_G(P) \).

(c) Since \( P \leq mPN, N \cap P \leq N \). Also \(|N/N \cap P| = |NP/P|\) and so \( p \) does not divide \(|N/N \cap P|\). So \( N \cap P \) is Sylow \( p \)-subgroup of \( N \). As \( N \cap P \leq N \) it is the only Sylow \( p \)-subgroup of \( N \). Thus \( N \cap P \leq G \).

(d) \( |G/N| = |G/P_N|\). The latter number is not divisible by \( p \) and so \( PN/N \) is a Sylow \( p \)-subgroup of \( GN/N \).

Since every Sylow \( p \)-subgroup of \( G/N \) is of the form \((PN/N)^gN = P^gN/N\) the map is onto. Suppose that \( PN/N = QN/N \). Then \( Q \leq PN \) and so by (b) \( Q = P \). Thus the map is also one to one. \(\square\)
Lemma 2.11.5 [order30]

(a) Let $G$ be a group of order 12. Then either $G$ has unique Sylow 3-subgroup or $G \cong \text{Alt}(4)$.

(b) Let $G$ be group of order 15. Then $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(c) Let $G$ be a group of order 30. Then $G$ has a unique Sylow 3-subgroup and a unique Sylow 5-subgroup.

Proof: (a) By 2.11.4a the number of Sylow 3 subgroups divides $\frac{12}{3}$ and is $1 \pmod{3}$. Thus $|\text{Syl}_3(G)| = 1$ or 4. In the first case we are done. In the second case let $N$ be the kernel of the action on $\text{Syl}_3(G)$. By 2.11.4, $G/N$ still has 4 Sylow 3-subgroups. Thus $|G/N| \geq 4 \cdot 2 = 12 = |G|$, $N = \{e\}$ and $G$ is isomorphic to a subgroup of order 12 in $\text{Sym}(4)$. Such a subgroup is normal and so $G \cong \text{Alt}(4)$ by 2.7.5.

(b) The numbers of Sylow 5 subgroups is $1 \pmod{5}$ and divides $\frac{15}{3} = 5$. Thus $G$ has a unique Sylow 5-subgroup $S_5$. Also the number of Sylow 3 subgroups is $1 \pmod{3}$ and divides $\frac{15}{3} = 5$. Thus $G$ has a unique Sylow 3-subgroup $S_3$. Then $S_3 \cap S_5 = 1$, $|S_3S_5| = 15$ and so $G = S_3S_5$. As both $S_3$ and $S_5$ are normal in $G$, $[S_3, S_5] \leq S_3 \cap S_5 = \{e\}$ and so $G \cong S_3 \times S_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(c) By 2.10.13 any group which as order twice an odd number has a normal subgroup of index two. Hence $G$ has a normal subgroup of order 15. This normal subgroup contains all the Sylow 3 and Sylow 5-subgroups of $G$ and so (c) follows from (b). \qed

Lemma 2.11.6 [order120] Let $G$ be a group of order 120. Then one of the following holds:

(a) $G$ has a unique Sylow 5-subgroup.

(b) $G \cong \text{Sym}(5)$.

(c) $|Z(G)| = 2$ and $G/Z(G) \cong \text{Alt}(5)$.

Proof: Let $P \leq \text{Syl}_5(G)$ and put $I = \text{Syl}_5(G)$.

If $|I| = 1$, (a) holds.

So suppose that $|I| > 1$. Then by 2.11.4a, $|I| \equiv 1 \pmod{5}$ and $|I|$ divides $|G/P| = 24$. The numbers larger than 1 and less or equal to 24 which are $1 \pmod{5}$ are 1, 6, 11, 16 and 21. Of these only 6 divides 24. Thus $|I| = 6$. Let $\phi : G \to \text{Sym}(I)$ be the homomorphism given by the action of $G$ on $I$. Put $N = \ker \phi$ and $H = \phi(G)$. The $H$ is subgroup of $\text{Sym}(I) \cong \text{Sym}(6)$ and $H \cong G/N$. By 2.11.4d, $G/N$ (and so also $H$) has exactly 6-Sylow 5 subgroups. In particular the order of $H$ is a multiple of 30. By 2.11.5c, $|H| \neq 30$.

Suppose next that $|H| = 120$. Note that $N = 1$ and so $G \cong H$ in this case. Now $H \leq \text{Sym}(I) \cong \text{Sym}(6)$. Thus 2.10.14a implies $G \cong H \cong \text{Sym}(5)$.
Suppose next that $|H| = 60$. If $H \not\leq \text{Alt}(I)$, then $H \cap \text{Alt}(I)$ is a group of order 30 with six Sylow 5-subgroups, a contradiction to 2.11.5. Thus $H \leq \text{Alt}(I) \cong \text{Alt}(6)$. So by 2.10.14b, $H \cong \text{Alt}(5)$. Since $|N| = 2$ and $N \trianglelefteq G$, $N \leq Z(G)$. Also $\phi(Z(G))$ is a abelian normal subgroup of $H \cong \text{Alt}(5)$ and so $\phi(Z(G)) = e$. Hence $N = Z(G)$ and

$$G/Z(G) = G/N \cong H \cong \text{Alt}(5).$$

\[\square\]
Chapter 3

Rings

3.1 Rings

Definition 3.1.1 A ring is a tuple \((R, +, \cdot)\) such that

(a) \((R, +)\) is an abelian group.

(b) \((R, \cdot)\) is a semigroup.

(c) For each \(r \in R\) both left and right multiplication by \(r\) are homomorphisms of \((R, +)\).

In other words a ring is a set \(R\) together with two binary operations \(+ : R \times R \to R\) \(a, b \to a + b\) and \(\cdot : R \times R \to R\) \((a, b) \to ab\) such that

(R1) \((a + b) + c = a + (b + c)\) so that for all \(a, b, c \in R\)

(R2) There exists \(0 \in R\) with \(0 + a = a = a + 0\) for all \(a \in R\).

(R3) For each \(a \in R\) there exists \(-a \in R\) with \(a + (-a) = 0 = (-a) + a\).

(R4) \(a + b = b + a\) for all \(a, b \in R\).

(R5) \(a(bc) = (ab)c\) for all \(a, b, c \in R\).

(R6) \(a(b + c) = ab + ac\) for all \(a, b, c \in R\).

(R7) \((a + b)c = ab + ac\) for all \(a, b, c \in R\).

Let \(R\) be a ring. The identity element of \((R, +)\) is denoted by \(0_R\) or 0. If \((R, \cdot)\) has an identity element we will denote it by \(1_R\) or 1. In this case we say that \(R\) is a ring with identity. \(R\) is commutative if \((R, \cdot)\) is.

Some examples: \((\mathbb{Z}, +, \cdot)\), \((\mathbb{Z}/n\mathbb{Z}, +, \cdot)\), \((\text{End}_G(V), +, \circ)\)

There is a unique ring with one element:
There are two rings of order two:

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array} \quad \begin{array}{c|cc}
\cdot & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & n \\
\end{array}
\]

Here \( n \in \{0, 1\} \) for \( n = 0 \) we have a ring with zero-multiplication, that is \( ab = 0 \) for all \( a, b \in R \). For \( n = 1 \) this is \((\mathbb{Z}/2\mathbb{Z}, +, \cdot)\).

There are the following rings of order 3:

\[
\begin{array}{c|ccc}
+ & 0 & 1 & -1 \\
0 & 0 & 1 & -1 \\
1 & 1 & -1 & 0 \\
-1 & -1 & 0 & 1 \\
\end{array} \quad \begin{array}{c|ccc}
\cdot & 0 & 1 & -1 \\
0 & 0 & 0 & 0 \\
1 & 0 & n & -n \\
-1 & 0 & -n & n \\
\end{array}
\]

Indeed if we define \( n = 1 \cdot 1 \), then \(-1 \cdot 1 = -(1 \cdot 1) = -n\). Here \( n \in \{0, 1, -1\} \). For \( n = 0 \) this is a ring with zero multiplication. For \( n = 1 \) this is \((\mathbb{Z}/3\mathbb{Z}, +, \cdot)\). If \( n = -1 \), this is isomorphic to the \( n = 1 \) case under the bijection \( 1 \leftrightarrow -1 \).

At the end of this section we will generalize these argument to find all rings whose additive group is cyclic.

Let \( A \) be an abelian group and \( \text{End}(A) \) the set of endomorphisms of \( A \), (that is the homomorphisms from \( A \) to \( A \)). Define \((\alpha + \beta)(a) = \alpha(a) + \beta(a)\) and \((\alpha \circ \beta)(a) = \alpha(\beta(a))\). Then \((\text{End}(A), +, \circ)\) is a ring.

Direct products and direct sums of rings are rings. Indeed, let \((R_i, i \in I)\) be a family of groups. For \( f, g \in \prod_{i \in I} R_i \) define \( f + g \) and \( fg \) by \((f + g)(i) = f(i) + g(i)\) and \((fg)(i) = f(i)g(i)\). With this definition both \( \prod_{i \in I} R_i \) and \( \sum_{i \in I} R_i \) are rings.

In the following lemma we collect a few elementary properties of rings.

**Lemma 3.1.2** [elementaryring] Let \( R \) be a ring.

(a) \( 0a = a0 = 0 \) for all \( a \in R \)

(b) \( (-a)b = a(-b) = -(ab) \) for all \( a, b \in R \).

(c) \( (-a)(-b) = ab \) for all \( a, b \in R \).

(d) \( (na)b = a(nb) = n(ab) \) for all \( a, b \in R, n \in \mathbb{Z} \).

(e) \( \left( \sum_{i=1}^{n} a_i \right) \left( \sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j \)

**Proof:** (a)-(e) hold since right and left multiplication are homomorphisms. For example any homomorphism sends 0 to 0. So (a) holds. We leave the details to the reader. \( \square \)
3.1. RINGS

Let \( R \) be a ring and \( G \) be semigroup. The semigroup ring \( R[G] \) of \( G \) over \( R \) is defined as follows:

As an abelian group \( R[G] = \bigoplus_{g \in G} R \). Define \((r_g) \cdot (s_g) = (t_g)\) where

\[
t_g = \sum_{\{(h,l) \in G \times G | hl = g\}} r_h s_l.
\]

Note that since the elements in \( \bigoplus_{g \in G} R \) have finite support all these sums are actual finite sums. Its straightforward to check that \( R[G] \) really is a ring. Here is an alternative description of the multiplication which makes the nature of this ring a little bit more transparent. For \( r \in R \) and \( g \in G \) write \( rg \) for the element in \( \bigoplus_{g \in G} R \) which has \( r \) in the \( g \)-th coordinate and 0 everywhere else. ( So \( rg = \rho_g(r) \) in the notation of section 2.8). Then

\[
(r_g)g = \sum_{g \in G} r_g g
\]

Also note that \( rg = sh \) implies \( r = s \) and is \( r \neq 0, g = h \).

If \( R[G] \) has an identity, then \( R \) has an identity. Indeed \( r = \sum r_g g \) is an identity in \( R[G] \).

Let \( a = \sum r_g \). We will show that \( a \) is an identity in \( R \). Let \( s \in R \) and \( g \in G \). Then

\[
sh = r(sh) = \sum (r_g s_g)gh.
\]

Summing up the coefficients we see that \( s = (\text{sum}_{g \in G} r_g) s = as \). Similarly \( sa = s \) and so \( a \) is an identity in \( R \). If \( R \) has an identity \( 1 \), we identify \( g \) with \( 1g \).

Here is an example of a semigroup \( G \) without an identity so that ( for any ring \( R \) with an identity) \( R[G] \) has an identity. As a set \( G = \{a, b, i\} \). Define the multiplication by

\[
xy = \begin{cases} 
  x & \text{if } x = y \\
  i & \text{if } x \neq y 
\end{cases}
\]

Then

\[
(xy)z = (xy)z = \begin{cases} 
  x & \text{if } x = y = z \\
  i & \text{otherwise}
\end{cases}
\]

Hence the binary operation is associative and \( G \) is a semigroup. Put \( r = a + b - i \in R[G] \). We claim that \( r \) is an identity. We compute \( ar = ra = a + ab - ai = a + i - i = a, \)

\( br = rb = ba + bb - bi = i + b - i = b \) and \( ir = ri = ia + ib - ii = i + i - i = i \). As \( R[G] \) fulfills both distributive laws this implies that \( r \) is an identity in \( R[G] \).

If \( R \) and \( G \) are commutative, \( R[G] \) is too.

The converse is not quite true:

Suppose \( R[G] \) is commutative, then

\[
\]
CHAPTER 3. RINGS

So if $rs \neq 0$ for some $r, s \in R$ we get $gh = hg$ and $G$ is commutative.

But if $rs = 0$ for all $r, s \in R$ then also $xy = 0$ for all $x, y \in R[G]$. So $R[G]$ is commutative, regardless whether $G$ is or not.

Here is an example for a semigroup ring. Let $G = (\mathbb{N}, +)$. Then $R[\mathbb{N}]$ is isomorphic to the polynomial ring over $R$. Indeed the map

$$\sum_{i=0}^{\infty} a_i x^i \to (a_i)_{i \in \mathbb{N}}$$

is clearly an isomorphism.

Put $R^\# = R \setminus \{0\}$, the nonzero elements.

**Definition 3.1.3** Let $R$ be a ring.

(a) A left (resp. right) zero divisor is an element $a \in R^\#$ such that there exists $b \in R^\#$ with $ab = 0$ (resp. $ba = 0$). A zero divisor is an element which is both a left and a right zero divisor.

(b) An nonzero element is called (left,right) invertible if it is (left,right) invertible in $(R^\#, \cdot)$. An invertible element is also called a unit.

(c) A non-zero commutative ring with identity and no zero-divisors is called an integral domain.

(d) A non-zero ring with identity all of whose nonzero elements are invertible is called a division ring. A field is a commutative division ring.

Note that a ring with identity is zero if and only if $1 = 0$. So in (c) and (d) the condition that $R$ is non-zero can be replaced by $1 \neq 0$.

We denote the sets of units in $R$ with $R^*$. Note that $(R^*, \cdot)$ is group (see 2.2.2c). A ring has no left zero divisors if and only if the left cancellation law

$$xa = ya \implies x = y$$

holds in $R^\#$. $\mathbb{R}$ is a field, $\mathbb{Z}$ is an integral domain. For which $n \in \mathbb{Z}^+$ is $\mathbb{Z}/n\mathbb{Z}$ an integral domain? It is if and only,

$$n \mid kl \implies n \mid k \text{ or } n \mid l$$

so if and only if $n$ is a prime. The following lemma implies that $\mathbb{Z}/p\mathbb{Z}$ is a field for all primes $p$.

**Lemma 3.1.4** [finiteidfield] All finite integral domains are fields
Proof: Let $R$ be a finite integral domain and $a \in R^\#$. As $R$ is an integral domain, multiplication by $a$ is a one to one map from $R^\# \to R^\#$. As $R$ is finite, this map is onto. Thus $ab = 1$ for some $b \in R$. So all non-zero elements are invertible.

\[ \square \]

**Definition 3.1.5** [ringhom] Let $R$ and $S$ be rings. A ring homomorphism is a map $\phi : R \to S$ so $\phi : (R, +) \to (S, +)$ and $\phi : (R, \cdot) \to (S, \cdot)$ are homomorphisms of semigroups.

Note that $\phi : R \to S$ is an homomorphism if and only if $\phi(r + s) = \phi(r) + \phi(s)$ and $\phi(rs) = \phi(r)\phi(s)$.

For a ring $R$ we define the opposite ring $R^{\text{op}}$ by $(R^{\text{op}}, +^{\text{op}}) = (R, +)$, and $a^{\text{op}} b = b \cdot a$. If $R$ and $S$ are rings then a map $\phi : R \to S$ is called an anti-homomorphism if $\phi : R \to S^{\text{op}}$ is ring homomorphism. So $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(b)\phi(a)$.

Let $\text{End}(R)$ be the set of ring homomorphism. Then $\text{End}(R)$ is monoid under composition. But as the sum of two ring homomorphisms usually is not a ring homomorphism, $\text{End}(R)$ has no natural structure as a ring.

The map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \to m + n\mathbb{Z}$ is a ring homomorphism.

For $r \in R$ let $\mathcal{R}_r : R \to R, s \to sr$ and $\mathcal{L}_r : R \to R, s \to rs$. By definition of a ring $\mathcal{R}_a$ and $\mathcal{L}_r$ are homomorphisms of $(R, +)$. But left and right multiplication usually is not a ring homomorphism. The map $\mathcal{L} : R \to \text{End}((R, +)), r \to \mathcal{L}_r$ is a homomorphism but the map $\mathcal{R} : R \to \text{End}((R, +)), r \to \mathcal{R}_r$ is an anti-homomorphism. Note that if $R$ has an identity, then both $\mathcal{R}$ and $\mathcal{L}$ are one to one.

**Theorem 3.1.6** [homgr] Let $\alpha : R \to S$ be a ring homomorphism, $G$ a semigroup and $\beta : G \to (S, \cdot)$ a semigroup homomorphism such that

\[ \alpha(r)\beta(g) = \beta(g)\alpha(r) \quad \forall r \in R, g \in G \]

Then

\[ \gamma : R[G] \to S \quad \sum_{g \in G} r_g g \to \sum_{g \in G} \alpha(r_g)\beta(g) \]

is a ring homomorphism.

Proof:

\[ \gamma\left(\sum_{g \in G} r_g g + \sum_{g \in G} s_g g\right) = \gamma\left(\sum_{g \in G} (r_g + s_g)g\right) = \sum_{g \in G} \alpha(r_g + s_g)\beta(g) = \]

\[ = \sum_{g \in G} (\alpha(r_g) + \alpha(s_g))\beta(g) = \sum_{g \in G} \alpha(r_g)\beta(g) + \sum_{g \in G} \alpha(s_g)\beta(g) = \gamma\left(\sum_{g \in G} r_g g\right) + \gamma\left(\sum_{g \in G} s_g g\right) \]

and

\[ \gamma\left(\sum_{g \in G} r_g \cdot \sum_{k \in K} s_k k\right) = \gamma\left(\sum_{g \in G} \sum_{k \in K} r_g s_k gk\right) = \sum_{g \in G} \sum_{k \in K} \alpha(r_g s_k)\beta(gk) = \]
\[
\sum_{g \in G} \sum_{k \in G} \alpha(r_g)\alpha(s_k)\beta(g)\beta(k) = \sum_{g \in G} \alpha(r_g)\beta(g) \cdot \sum_{k \in G} \alpha(s_k)\beta(k) = \gamma(\sum_{g \in G} r_g) \cdot \gamma(\sum_{k \in G} s_k) \]

Let \( A \) be an abelian group. Define \( \phi : \mathbb{Z} \to \text{End}(A) \) by \( \phi(n)(r) = nr \). Then \( \phi \) is a ring homomorphism. Since \( \ker \phi \) is an additive subgroup of \( \mathbb{Z} \), \( \ker \phi = n\mathbb{Z} \) for some \( n \in \mathbb{N} \). \( n \) is called the \textit{exponent} of \( A \) and denote by \( \exp(A) \). If \( n \neq 0 \), \( n \) is the smallest positive number such that \( na = 0 \) for all \( a \in A \) ( that is \( nA = 0 \)). And \( n = 0 \) if \( mA \neq 0 \) for all \( m \in \mathbb{Z}^+ \).

Let \( R \) be a ring. The \textit{characteristic} \( \text{char} R \) of \( R \) is the exponent of \((R, +)\). Suppose \( R \) has an identity. The map \( \rho : \mathbb{Z} \to R, \quad n \to n1 \) is a homomorphism of rings. We claim that \( \ker \rho = \ker \phi \). This can be verified directly or by observing that \( \phi = L \circ \rho \).

**Lemma 3.1.7** Suppose \( R \) is a non-zero ring with identity and no zero divisors. Then \( \text{char} R \) is 0 or a prime.

**Proof:** Let \( n = \text{char} R \) and suppose \( n \neq 0 \). If \( n = 1 \) then \( r = 1r = 0 \) for all \( r \in R \). So \( n > 1 \). Suppose \( n \) is not a prime, then \( n = st \) with \( s, t \in \mathbb{Z}^+ \). So

\[
(s1)(t1) = (st)1 = n1 = 0.
\]

As \( R \) has no zero divisors we conclude that \( s1 = 0 \) or \( t1 = 0 \). In each case the case the get a minimality of \( n \).

Let \( r \in R \). If \( R \) has an identity we define \( r^0 = 1 \). If \( R \) does not have an identity we will use the convention \( r^0s = s \) for all \( s \in R \).

**Lemma 3.1.8 (Binomial Theorem)** Let \( R \) be ring, \( a_1, a_2, \ldots, a_n \in R \) and \( m \in \mathbb{Z}^+ \).

(a) \[
\sum_{i_1=1}^{n} \cdots \sum_{i_m=1}^{n} a_{i_1}a_{i_2} \cdots a_{i_m} = \sum_{i=1}^{n} a_i^m
\]

(b) If \( a_ia_j = a_ja_i \) for all \( 1 \leq i, j \leq n \), then

\[
\sum_{i=1}^{n} a_i^m = \sum_{\{m_i \in \mathbb{N} \mid \sum_{i=1}^{n} m_i = m \}} \binom{m}{m_1, m_2, \ldots, m_n} a_1^{m_1}a_2^{m_2} \cdots a_n^{m_n}
\]

**Proof:** (a) follows form 3.1.2e and induction on \( m \).

For (b) notice that \( a_{i_1} \cdots a_{i_m} = a_1^{m_1}a_2^{m_2} \cdots a_n^{m_n} \), where \( m_k = |\{j \mid i_j = k\}| \). So (b) follows from (a) and a simple counting argument.

**Lemma 3.1.9** \( \text{easygcd} \) Let \( n, m, k \in \mathbb{Z}^+ \).

(a) If \( \gcd(m, k) = 1 \) or \( \gcd(n, m) = 1 \), then \( \gcd(f, k) = 1 \) for some \( f \in \mathbb{Z} \) with \( f \equiv n \pmod{m} \).
(b) There exists \( f \in \mathbb{Z} \) so that \( \gcd(f, k) = 1 \) and \( fn \equiv \gcd(n, m) \pmod{m} \)

Proof: (a) Suppose first that \( \gcd(m, k) = 1 \). Then \( 1 - n = lm + sk \) for some integers \( l, s \). Thus \( 1 = (n + lm) + sk \). Put \( f = n + lm \), then \( \gcd(n + lm, k) = 1 \).

Suppose next that \( \gcd(n, m) = 1 \). Write \( k = k_1k_2 \) where \( \gcd(k_1, m) = 1 \) and all primes dividing \( k_2 \) also divide \( m \). By the first part there exists \( l \in \mathbb{Z} \) with \( \gcd(n + lm, k_1) = 1 \).

(b) Let \( d = \gcd(n, m) \). Replacing \( n \) be \( \frac{n}{d} \) and \( m \) by \( \frac{m}{d} \) we may assume that \( d = 1 \). Then \( n^*n \equiv 1 \pmod{m} \) for some \( n^* \in \mathbb{Z} \). Since \( \gcd(n^*, m) = 1 \) we can apply (a) to \( n^*, m \) and \( k \). So there exists \( f \) with \( \gcd(f, k) = 1 \) and \( f \equiv n^* \pmod{m} \). Then also \( fn \equiv 1 \pmod{m} \). \( \square \)

Lemma 3.1.10 Let \( R \) be a ring with \((R, +)\) cyclic. Then \( R \) is isomorphic to exactly one of the following rings:

1. \( \mathbb{Z} \) with regular addition but zero-multiplication.

2. \( (n\mathbb{Z}/nm\mathbb{Z}, +, \cdot) \), where \( m \in \mathbb{N}, n \in \mathbb{Z}^+ \) and \( n \) divides \( m \).

Proof: Let \( m \in \mathbb{N} \) so that \( (R, +) \cong (\mathbb{Z}/m\mathbb{Z}, +) \) and let \( a \) be a generator for \((R, +)\). So \( a \cdot a = na \) for some \( n \in \mathbb{Z} \). Then for all \( k, l \in \mathbb{Z} \), \((ka) \cdot (la) = klna \) and so the multiplication is uniquely determined by \( n \). Note that \((-a)(-a) = na = (-n)(-a) \). So replacing \( a \) be \(-a \) we may assume that \( n \in \mathbb{N} \). Also if \( m > 0 \) we may choose \( 0 < n \leq m \).

Suppose first that \( n = 0 \). Then by our choice \( m = 0 \) as well. So \((R, +) \cong (\mathbb{Z}, +) \) and \( rs = 0 \) for all \( r, s \in R \).

Suppose next that \( n > 0 \). Then the map

\[
n\mathbb{Z}/nm\mathbb{Z} \to R, \quad nk + nm\mathbb{Z} \to ka
\]

is an isomorphism. If \( m = 0 \), these rings are non-isomorphic for different \( n \). Indeed \( R^2 = nR \) and so \( |R/R^2| = n \). Therefore \( n \) is determined by the isomorphism type \( R \).

For \( m > 0 \), various choices of \( n \) can lead to isomorphic rings. Namely the isomorphism type only depends on \( d = \gcd(n, m) \). To see this we apply 3.1.9 to obtain \( f \in \mathbb{Z} \) with \( \gcd(f, m) = 1 \) and \( fn \equiv d \pmod{m} \). Then \( 1 = ef + sm \) for some \( e, s \in \mathbb{Z} \) and so \( f + m\mathbb{Z} \) is invertible. Hence also \( fa \) is a generator for \((R, +)\) and

\[
(fa) \cdot (fa) = f^2na = (fn)(fa) = d(fa).
\]

Also \( R^2 = dR \) and \( |R/R^2| = \frac{m}{d} \). So \( d \) is determined by the isomorphism type of \( R \). \( \square \)
3.2 Ideals and homomorphisms

Definition 3.2.1 Let $R$ be a ring.

(a) A subring of $R$ is a subset $S \subseteq R$ so that $S$ is a subgroup of $(R, +)$ and a subsemigroup of $(R, \cdot)$.

(b) An left (right) ideal in $R$ is a subring $I$ of $R$ so that $rI \subseteq I$ $Ir \subseteq I$ for all $r \in R$.

(c) An ideal in $R$ is a left ideal which is also a right ideal.

$n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Let $V$ be a $\mathbb{K}$-vector space. Let $W \leq V$ be $\mathbb{K}$ subspace. Define

$$\text{Ann}(W) = \{ \alpha \in \text{End}_\mathbb{K}(V) \mid \alpha(w) = 0 \text{ for all } w \in W \}.$$  

Then $\text{Ann}(W)$ is an left ideal in $\text{End}_\mathbb{K}(V)$. Indeed it is clearly an additive subgroup and $(\beta \circ \alpha)(w) = \beta(\alpha(w)) = \beta(0) = 0$ for all $\beta \in \text{End}_\mathbb{K}(V)$ and $\alpha \in \text{Ann}(W)$. We will see later that $\text{End}_\mathbb{K}(V)$ is a simple ring, that is it has no proper ideals.

Lemma 3.2.2 [basicring hom] Let $\phi : R \rightarrow S$ be a ring homomorphism.

(a) If $T$ is a subring of $R$, $\phi(T)$ is a subring of $S$.

(b) If $T$ is a subring of $S$ then $\phi^{-1}(T)$ is a subring of $R$.

(c) $\ker \phi$ an ideal in $R$.

(d) If $I$ is an (left,right) ideal in $R$ and $\phi$ is onto, $\phi(I)$ is a (left,right) ideal in $S$.

(e) If $J$ is a (left,right) ideal in $S$, then $\phi^{-1}(J)$ is an (left,right) ideal on $R$.

Proof: Straight forward. □

Let $\alpha : R \rightarrow S$ be a ring homomorphism and $\beta : G \rightarrow H$ a semigroup homomorphism. Consider the ring homomorphism:

$$\gamma : R[G] \rightarrow S[H] \quad \sum_{g \in G} r_g g \rightarrow \sum_{g \in G} \alpha(r_g) \beta(g)$$

What is the image and the kernel of $\gamma$? Clearly $\gamma(R[G]) = \alpha(R) \beta(G)$. Let $I = \ker \alpha$. To compute $\ker \gamma$ note that

$$\gamma(\sum_{g \in G} r_g g) = \sum_{h \in H} \alpha(\sum_{g \in \beta^{-1}(h)} r_g) h$$

and so

$$\sum_{g \in G} r_g g \in \ker \gamma \iff \sum_{t \in \beta^{-1}(h)} r_t \in I \text{ for all } h \in \beta(G).$$
If $\beta$ is a group homomorphism we can describe $\ker \gamma$ just in terms of $I = \ker \alpha$ and $N := \ker \beta$. Indeed the $\beta^{-1}(h)'s$ $(h \in \beta(G))$ are just the cosets of $N$ and so
\[
\sum_{g \in G} r_g g \in \ker g \iff \sum_{t \in T} r_t \in I \text{ for all } T \in G/N.
\]

Let us consider the special case where $R = S$, $\alpha = \text{id}_R$ and $H = \{e\}$. Identify $R[e]$ with $R$ via $re \leftrightarrow r$. Then $\gamma$ is the map
\[
R[G] \to R, \sum r_g g \to \sum r_g.
\]
The kernel of $\gamma$ is the ideal
\[
R^e[G] = \{ \sum r_g g \mid \sum r_g = 0 \}
\]
$R^e[G]$, is called the augmentation ideal of $R[G]$.

For subsets $A, B$ of the ring $R$ define $A + B = \{a + b \mid a \in A, b \in B\}$. Let $\langle A \rangle$ be the additive subgroup of $R$ generated by $A$. Also put $AB = \langle ab \mid a \in A, b \in B\rangle$. More general define $A_1A_2\ldots A_n$ to be the additive subgroup generated by the products $a_1a_2\ldots a_n$, $a_i \in A_i$. If $A$ is a left ideal, then also $AB$ is a left ideal. If $B$ is a right ideal, then $AB$ is a right ideal. In particular, if $A$ is a left ideal and $dR$ is a right ideal, then $AB$ is an ideal. If $A, B$ are (right,left) ideals so is $A + B$ and $A \cap B$. Actually arbitrary intersection of (left,right) ideals are (left,right) ideals. So for $A \subseteq R$ we define the ideal $\langle A \rangle$ generated by $A$ to be
\[
\langle A \rangle = \bigcap \{ I \mid I \text{ is an ideal in } R, A \subseteq I \}
\]
The left ideal generated by $A$ is just $RA + \langle A \rangle$. If $R$ has an identity this is equal to $RA$. Also $\langle A \rangle = \langle A \rangle + RA + AR + RAR$ which simplifies to $RAR$ if $R$ has an identity.

**Lemma 3.2.3 [RmodI]** Let $I$ be an ideal in the ring $R$.

(a) The binary operation
\[
R/I \times R/I \to R/I, \quad (a + I, b + I) \to ab + I
\]
is well defined.

(b) $(R/I, +, \cdot)$ is a ring.

(c) The map
\[
\pi : R \to R/I, \quad r \to r + I
\]
is a ring homomorphism with kernel $I$. 

Proof: (a) Let $i, j \in I$. Then $(a + i)(b + j) = ab + ib + aj + ij$. As $I$ is an ideal, $ib + aj + ij \in I$ and so $(a + i)(b + j) + I = ab + I$.

(b) and (c) follow from the corresponding results for groups and (a).

Lemma 3.2.4 (The Isomorphism Theorem) [itr] Let $\phi : R \to S$ be a ring homomorphism. Then the map

$$\tilde{\phi} : R/\ker\phi \to \phi(R), \quad r + \ker\phi \to \phi(r)$$

is a well defined isomorphism of rings.

By the Isomorphism Theorem for groups 2.5.5, this is a well defined isomorphism for the additive groups. But clearly also $\tilde{\phi}(ab) = \tilde{\phi}(a)\tilde{\phi}(b)$ and $\tilde{\phi}$ is a ring isomorphism.

We will see below that any ring $R$ can be embedded into a ring $S$ with an identity. This embedding is somewhat unique. Namely suppose that $R \leq S$ and $S$ has an identity. Then for $n, m \in \mathbb{Z}$ and $r, s \in R$ we have $(n1 + r)(m1 + s) = (n + m)1 + (r + s)$ and $(n1 + r)(m1 + s) = (nm)1 + (mr + ns + rs)$. So already $\mathbb{Z}1 + R$ is a ring with 1, contains $R$ and the addition and multiplication on $\mathbb{Z}1 + R$ is uniquely determined. But there is some degree of freedom. Namely $\mathbb{Z}1 + R$ does not have to be a direct sum.

Let $\hat{R} = \mathbb{Z} \times R$ as abelian groups. We make $\hat{R}$ into a ring by defining

$$(n, r) \cdot (m, s) = (nm, ns + mr + rs).$$

Then $(1, 0)$ is an identity in $\hat{R}$. The map $\phi : \hat{R} \to S, (n, r) \to n1 + r$ is a homomorphism with image $\mathbb{Z}1 + R$. Let us investigate $\ker\phi$. $(n, r) \in \ker\phi$ iff $r = -n1$. Let $k\mathbb{Z}$ be the inverse image of $\mathbb{Z}1 \cap R$ in $\mathbb{Z}$. Also put $t = k1$ and $D_{k,t} = \{(lk, -lt) \mid l \in \mathbb{Z}\}$. Then $\ker\phi = D_{k,t}$. Hence $\hat{R}/D_{k,t} \cong \mathbb{Z}1 + R$.

Now which choices of $k \in \mathbb{Z}$ and $t \in R$ can really occur? Note that as $t = -n1$, $tr = kr = rt$. This necessary condition on $k$ and $t$ turns out to be sufficient:

Let $k \in \mathbb{Z}$. $t \in R$ is called an $k$-element if $tr = rt = kr$ for all $r \in R$. Note that a 1-element is an identity, while a 0-element is an element with $tR = Rt = 0$. Also if $a$ and $b$ are $k$-elements, then $a - b$ is a 0-element. So if a $k$-elements exists it unique modulo the zero elements.

Suppose now that $t$ is a $k$-element in $R$. Define $D_{t,k}$ has above. We claim that $D_{k,t} = \mathbb{Z}(k, -t)$ is an ideal in $R$. For this we compute( using $rt = kr$)

$$(n, r) \cdot (k, -t) = (nk, kr - nt - rt) = (nk, kr - nt - kr) = (nk, -nt) = n(k, -t).$$

So $D_{k,t}$ is a left ideal. Similarly, $D_{t,k}$ is a right ideal. Put $R_{k,t} = \hat{R}/D_{k,t}$. Then $R_{k,t}$ is a ring with identity, contains $R$ ( via the embedding $r \to (0, r) + D_{k,t}$) and fulfills $\mathbb{Z}1 \cap R = k\mathbb{Z}1 = \mathbb{Z}t$.

Note that if $t$ is an $k$-element and $s$ an $l$-element, then $-t$ is an $-k$ element and $t + s$ is an $(k + l)$-element. Therefore the sets of $k \in \mathbb{Z}$ for which there exists a $k$-element is a
subgroup of \( \mathbb{Z} \) and so of the form \( \mathbb{Z}^i \) for some \( i \in \mathbb{N} \). Let \( u \) be a \( i \)-element. \( R_{i,u} \) is in some sense the smallest ring with a identity which contains \( R \). Also if \( R \) has no 0-elements, \( u \) and so \( R_{i,u} \) is uniquely determined.

For example if \( R = n\mathbb{Z} \), then \( i = n = u \) and \( R_{i,u} \cong \mathbb{Z} \). Indeed \( \hat{R} = \mathbb{Z} \times n\mathbb{Z} \), \( D_{nn} = \{(jn, -jn) \mid j \in \mathbb{Z}\} \), \( \hat{R} = \mathbb{Z}(1,0) \oplus D_{n,n} \) and the map \( R_{n,n} \to \mathbb{Z} \), \((j,r) + D_{n,n} \to j + r\) is an isomorphism between \( R_{n,n} \) and \( \mathbb{Z} \).

Next we will show that \( R \) can be embedded into a ring with identity which has same characteristic as \( R \). Put \( n = \text{char} R \), then \( 0 \) is an \( n \)-element. Also \( D_{n,0} = n\mathbb{Z} \times \{0\} \) and \( R_{n,0} \cong \mathbb{Z} \times n\mathbb{Z} \times R \) as abelian groups. So \( R_{n,0} \) has characteristic \( n \). On the other hand \( \hat{R} = R_{0,0} \) always has characteristic 0.

**Definition 3.2.5** \([dprime]\) Let \( I \) be an ideal in the ring \( R \) with \( I \neq R \).

(a) \( I \) is prime ideal if for all ideals \( A, B \) in \( R \)

\[ AB \subseteq I \iff A \subseteq I \text{ or } B \subseteq I \]

(b) \( I \) is a maximal ideal if for each ideal \( A \) of \( R \)

\[ I \subseteq A \subseteq R \iff A = I \text{ or } A = R. \]

Note that \( n\mathbb{Z} \cong m\mathbb{Z} \) and so \( k\mathbb{Z} \) is a prime ideal in \( \mathbb{Z} \) if and only if \( k \) is prime. Also \( n\mathbb{Z} \subseteq m\mathbb{Z} \) if an only if \( m \) divides \( n \). So \( k\mathbb{Z} \) is maximal if and only if \( k \) is a prime. So for \( \mathbb{Z} \) the maximal ideals are the same as the prime ideals. This is not true in general.

**Lemma 3.2.6** \([basicprime]\) Let \( P \neq R \) be an ideal in the ring \( R \).

(a) If for all \( a, b \in R \),

\[ ab \in P \iff a \in P \text{ or } b \in P \]

then \( P \) is a prime ideal

(b) If \( R \) is commutative, the converse of (a) holds.

(c) If \( R \) is commutative, then \( P \) is a prime ideal if and only \( R/P \) has no zero divisors.

**Proof:** (a) Let \( A \) and \( B \) are ideals in \( R \) with \( AB \subseteq P \). We need to show that \( A \subseteq P \) or \( B \subseteq B \). So suppose \( A \nsubseteq P \) and pick \( a \in A \setminus P \). Since \( ab \in P \) for all \( b \in B \) we conclude \( b \in P \) and \( B \subseteq P \).

(b) Suppose that \( P \) is prime ideal and \( a, b \in R \) with \( ab \in P \). Then for all \( n, m\mathbb{Z} \) and \( r, s \in R \).

\[ (na + ra)(mb + sa) = (nm)ab + (ns + mr + rs)ab \]

and so \( (a)(b) \subseteq (ab) \subseteq P \). As \( P \) is prime, \( (a) \subseteq P \) or \( (b) \subseteq P \). Hence \( a \in P \) or \( b \in P \).

(c) Just note that the condition in (a) is equivalent to saying that \( R/P \) has no zero divisors. \( \Box \)
Lemma 3.2.7 [primeintegral] Let $R$ be a nonzero commutative ring with identity and $P$ an ideal. Then $P$ is prime ideal if and only if $R/P$ is an integral domain.

Proof: If $P$ is a prime ideal or if $R/P$ is an integral domain we have that $R \neq P$. So the lemma follows from 3.2.6c.

Theorem 3.2.8 [basicmaximal] Let $R$ be a ring with identity and $I \neq R$ be an ideal. Then $I$ is contained in a maximal ideal. In particular every nonzero ring with identity has a maximal ideal.

Proof: The second statement follows from the first applied to the zero ideal. To prove the first we apply Zorn’s lemma A.1. For this let $\mathcal{M}$ be the set of ideals $J$ of $R$ with $I \subseteq J \subseteq R$. Order $\mathcal{M}$ by inclusion and let $C$ be a nonempty chain in $\mathcal{M}$. Let $M = \bigcup C$. Then $M$ is an ideal and $I \subseteq M$. Also 1 is not contained in any member of $C$ and so $1 \notin M$. Hence $M \neq R$ and $M \in \mathcal{M}$. Thus every chain has an upper bound and so by Zorn’s Lemma $\mathcal{M}$ has a maximal element $M$. If $M \subset A$ for some ideal $A \neq R$, then $I \subseteq A$, $A \in \mathcal{M}$ and so by maximality of $M$ in $M$, $A = M$. Thus $M$ is a maximal ideal.

Theorem 3.2.9 [maximalprime] Let $M$ be a maximal ideal. Then $M$ is a prime ideal unless $R$ has no identity, $R \neq R^2$ and $R^2 \subseteq M$.

Proof: Suppose that $M$ is not prime. Then $AB \subseteq M$ for some ideals $A$ and $B$ with $A \not\subseteq M$ and $B \not\subseteq M$. The maximality of $M$ implies $R = A + M = B + M$. Thus $R^2 = (A + M)(B + M) \subseteq AB + M \subseteq M$. Has $M \neq M$ we get $R^2 \neq R$. In particular $R$ does not have an identity since otherwise $R = R1 \subseteq R^2$. We remark that an ideal $I \neq R$ is maximal if and only if $R/I$ is simple.

Lemma 3.2.10 [basicsimplerings]

(a) Let $R$ be a division ring. Then $R$ has non proper left or right ideals. In particular $R$ is simple.

(b) Let $R$ be a non-zero commutative ring with identity. The $R$ is simple if and only if $R$ is a field.

Proof: (a) Let $I$ be an nonzero left ideal in $R$ and pick $0 \neq i \in I$. Then $1 = i^{-1}i \in RI \subseteq R$ and so $R = R1 \subseteq I$.

(b) By (a) we only need to show that simple implies field. So suppose $R$ is simple and $0 \neq a \in R$. Since $R$ has an identity, $Ra$ is an non-zero ideal. As $R$ is simple $Ra = R$. Thus $ra = 1$ for some $r$. As $R$ is commutative, $ar = 1$ and so $r$ has an inverse.

If $I$ is an ideal we will sometimes write $a \equiv b \pmod{I}$ if $a + I = b + I$, that is if $a - b \in I$. If $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ then $a \equiv b \pmod{n\mathbb{Z}}$ is the same as $a \equiv b \pmod{n}$. 

3.2. IDEALS AND HOMOMORPHISMS

Theorem 3.2.11 (Chinese Remainder Theorem) [CRT] Let \((A_i, i \in I)\) be a family of ideals in the ring \(R\).

(a) The map \(\theta:\)

\[
R/\bigcap_{i \in I} A_i \to \prod_{i \in A_i} R/A_i
\]

\[
r + \bigcap_{i \in I} A_i \to (r + A_i)_{i \in I}
\]

is a well defined monomorphism.

(b) Suppose that \(I\) is finite, \(R = R^2 + A_i\) and \(R = A_i + A_j\) for all \(i \neq j \in I\). Then

(ba) If \(|I| > 1\), then \(R = A_i + \bigcap_{i \neq j \in I} A_j\).

(bb) \(\theta\) is an isomorphism.

(bc) For \(i \in I\) let \(b_i \in R\) be given. Then there exists \(b \in R\) with

\[
b \equiv b_i \pmod{A_i} \text{ for all } i \in I
\]

Moreover, \(b\) is unique \(\pmod{\bigcap_{i \in I} A_i}\).

Proof: (a) The map \(r \to (r + A_i)_{i \in I}\) is clearly a ring homomorphism with kernel \(\bigcap_{i \in I} A_i\). So (a) holds.

(ba) For \(\emptyset \neq J \subseteq I\) put \(A_J = \bigcap_{j \in J} A_j\). We will show by induction on \(|J|\) that

\[
R = A_i + A_J
\]

for all \(\emptyset \neq J \subseteq I \setminus \{i\}\). Indeed if \(|J| = 1\) this is part of the assumptions. So suppose \(|J| > 1\), pick \(j \in J\) and put \(K = J \setminus \{j\}\). Then by induction \(R = A_i + A_K\) and \(R = A_i + A_j\). Note that as \(A_j\) and \(A_K\) are ideals, \(A_jA_K \subseteq A_j \cap A_K = A_J\) Thus

\[
R^2 = (A_i + A_j)(A_i + A_K) \subseteq A_i + A_jA_K \subseteq A_i + A_J
\]

Hence \(R = A_i + R^2 = A_i + A_J\).

(bb) By (a) we just need to show that \(\theta\) is onto. For \(|I| = 1\), this is obvious. So suppose \(|I| \geq 2\). Let

\[
x = (x_i)_{i \in I} \in \prod_{i \in A_i} R/A_i.
\]

We need to show that \(x = \theta(b)\) for some \(b \in R\). Let \(x_i = b_i + A_i\) for some \(b_i \in R\). By (ba), we may choose \(b_i \in \bigcap_{j \in I \setminus i} A_j\). So \(b_i \in A_j\) for all \(j \neq i\). Thus

\[
\theta(b_i) = \begin{cases} 
  x_i & \text{if } j = i \\
  0 & \text{if } j \neq i
\end{cases}
\]

Put \(b \sum_{i \in I} b_i\). Then \(\theta(b)_j = x_j\) and so \(\theta(b) = x\). □
(bc) This is clearly equivalent to (bb) \hfill \Box

The special case $R = \mathbb{Z}$ is an elementary result from number theory which was known to Chinese mathematicians in the first century A.D. To state this result we first need to observe a couple of facts about ideals in $\mathbb{Z}$.

Let $n, m$ be positive integers. $\text{gcd}(n, m)$ denotes the greatest common divisor and $\text{lcm}(n, m)$ the least common multiple of $n$ and $m$. Then

$$n\mathbb{Z} \cap m\mathbb{Z} = \text{lcm}(n, m)\mathbb{Z}$$

and

$$n\mathbb{Z} + m\mathbb{Z} = \text{gcd}(n, m)\mathbb{Z}$$

In particular $n$ and $m$ are relatively prime if and only if $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. So part (bc) of the Chinese Remainder Theorem translates into:

**Corollary 3.2.12** Let $m_1, \ldots, m_n$ be positive integers which are pairwise relatively prime. Let $b_1, \ldots, b_n$ be integers. Then there exists an integer $b$ with

$$b \equiv b_i \pmod{m_i} \text{ for all } 1 \leq i \leq n$$

Moreover, $b$ is unique $\pmod{m_1 m_2 \ldots m_n}$ \hfill \Box

### 3.3 Factorizations in commutative rings

**Definition 3.3.1** Let $R$ be a commutative rings and $a, b \in R$.

(a) We say that $a$ divides $b$ and write $a \mid b$, if $(b) \subseteq (a)$.

(b) We say that $a$ and $b$ are associate and write $a \sim b$, if $(a) = (b)$

(c) We say that $a$ is proper if $\{0\} \neq (a) \neq R$.

Some remarks on this definition. First note that

$$a \sim b \iff a \mid b \text{ and } b \mid a$$

Also $a|b$ is a symmetric and transitive relation. $a \sim b$ is an equivalence relation. If $R$ has an identity, $a \mid b$ if and only if $b = ra$ for some $r \in R$.

**Lemma 3.3.2 [unitdivide]** Let $R$ be a commutative ring with identity and $u \in R$. The following are equivalent

1. $u$ is a unit.

2. $u \mid 1$
3.3. FACTORIZATIONS IN COMMUTATIVE RINGS

3. $u \mid r$ for all $r \in R$

4. $(u) = R$

5. $u$ is not contained in any maximal ideal of $R$.

6. $r \sim ur$ for all $r \in R$.

Proof: Straightforward. □

In particular, we see that if $R$ has an identity, $a$ is proper if and only if $a$ is neither 0 nor a unit.

Lemma 3.3.3 [r*orbits] Let $R$ be an integral domain. Let $a, b, u \in R^\#$ with $b = ua$. Then $b \sim a$ if and only if $u$ is a unit.

Proof: The "if" part follows from 3.3.2, part 6. So suppose that $b \sim a$. Then $a = vb$ for some $v \in R$. Thus $1b = b = ua = u(vb) = (uv)b$. Since the cancellations law hold in integral domains we conclude that $uv = 1$. So $u$ is a unit. □

Recall that $R^*$ denotes the (multiplicative) groups of units in $R$. $R^*$ acts on $R$ by left multiplication. The previous lemma now says that in an integral domain the orbits of $R^*$ are exactly the equivalence classes of $\sim$.

Definition 3.3.4 [dpid] Let $R$ be a ring.

(a) An ideal $I$ is called a principal ideal if its generated by one element, that is $I = (r)$ for some $r \in R$.

(b) $R$ is called a principal ideal ring if every ideal is a principal ideal.

(c) $R$ is principal ideal domain (PID), if $R$ is an integral domain and a principal ideal ring.

Definition 3.3.5 Let $R$ be a commutative ring with identity and $c$ a proper element.

(a) $c$ is called irreducible if for all $a, b \in R$

\[ c = ab \implies a \text{ or } b \text{ is a unit} \]

(b) $c$ is called a prime if for all $a, b \in R$

\[ p \mid ab \implies p \mid a \text{ or } p \mid b. \]

Lemma 3.3.6 [primeirr] Let $p$ and $c$ be nonzero elements in the integral domain $R$.

(a) The following are equivalent:
1. $p$ is a prime
2. $(p)$ is a prime ideal
3. $R/(p)$ is an integral domain

(b) The following are equivalent

1. $c$ is irreducible
2. For all $a \in R$, $a \mid c \implies a \sim u$ or $a$ is a unit
3. $(c)$ is maximal in the set of proper principal ideals.

(c) Every prime element in $R$ is irreducible.

(d) If $R$ is principal ideal then the following are equivalent

1. $p$ is a prime
2. $p$ is irreducible.
3. $(p)$ is a maximal ideal.
4. $R/(p)$ is a field.

(e) Every associate of a prime is a prime and every associate of an irreducible element is irreducible.

Proof: (a) This follows from 3.2.6a and 3.2.7.

(b) Suppose 1. holds and $a \mid c$. Then $c = ab$. If $a$ is not a unit, then $b$ is a unit and so $a \sim c$. Hence 2. holds.

Suppose 2. holds and $(c) \subseteq (a)$. Then $a \mid u$. If $a \sim c$, $(a) = (c)$ and if $a$ is a unit $(a) = R$. Thus 3. holds.

Suppose that 3. holds and $c = ab$. Then $(c) \subseteq (a)$ and so either $(a) = (c)$ or $(a) = R$. In the first case $a \sim c$ and so by 3.3.3 $b$ is a unit. In the second case $a$ is a unit. So 1. holds.

(c) Let $p$ be a prime and $p = ab$. So $p \mid a$ or $p \mid b$. Without loss $p \mid a$. Since also $a \mid p$ we get $p \sim a$. Thus 3.3.3 implies that $b$ is unit.

(d) By (c) 1. implies 2.

Suppose 2. holds. By (b3) says that $(p)$ is a maximal proper principal ideal. Since every ideal in a PID is a principal ideal, $(p)$ is a maximal ideal. So 3. holds.

By 3.2.10 3. implies 4.

Suppose 4. holds. Then by ??, $(p)$ is a prime ideal. So by (a), $p$ is a prime.

(e) By (a) and (b) the properties ”prime” and ”irreducible” of an element only depends on the ideal generated by the element. Thus (e) holds.

Lemma 3.3.7 [uniquefactor] Let $R$ be an integral domain and $a \in R$. Suppose that $a = p_1 \cdot \ldots \cdot p_n$ with each $p_i$ a prime in $R$. 
3.3. FACTORIZATIONS IN COMMUTATIVE RINGS

(a) If $q \in R$ is a prime with $q \mid a$, then $q \sim p_i$ for some $1 \leq i \leq n$.

(b) If $a = q_1 \ldots q_m$ with each $q_i$ a prime. Then $n = m$ and there exists $\pi \in \operatorname{Sym}(n)$ with $q_i \sim p_{\pi(i)}$.

(a) Put $b = p_2 \ldots p_n$. Then $a = p_1 b$ and $q \mid p_1 b$. Thus $q \mid p_1$ or $q \mid b$. In the first case as primes are irreducible $q \sim p_1$. In the second case induction implies $q \sim p_j$ for some $j \leq 2 \leq n$.

(b) By (a), $q_1 \sim p_j$ for some $j$. Without loss $q_1 = p_1$. As $R$ has no zero-divisor, $b = q_2 \ldots q_m$ and we are done by induction.

Definition 3.3.8 A unique factorization domain (UFD) is an integral domain in which every proper element is a product of primes.

Let $R$ be a UFD. Then each irreducible element is divisible by a prime and so equal to that prime. So primes and irreducibles are the same in UFD’s. Also 3.3.7 implies that the prime factorizations are unique up to associates.

Our next goals is to show that every PID is a UFD. For this we need a couple of preparatory lemmas.

Lemma 3.3.9 [chainideal] Let $I$ be chain of ideals in the ring $R$.

(a) $\bigcup I$ is an ideal.

(b) If $\bigcup I$ is finitely generated as an ideal, then $\bigcup I \in I$.

Proof: (a) is obvious.

(b) Suppose that $\bigcup I = (F)$ for some finite $F \subseteq \bigcup I$. For each $f \in F$ there exists $I_f \in I$ with $f \in I_f$. Since $I$ is totally ordered, the finite set $\{I_f \mid f \in F\}$ has a maximal element $I$ then $I \in I$, $F \subseteq I$ and so

$$\bigcup I = (F) \subseteq I \subseteq \bigcup I$$

Thus $I = \bigcup I$ and (b) is proved.

Lemma 3.3.10 [minchain] Let $R$ be an integral domain and $I$ a set of principal ideals. Then one of the following holds:

1. $\bigcap I = \{0\}$.

2. $I$ has a minimal element.

3. There exists an infinite strictly ascending series of principal ideals.
Proof: Suppose that neither 1. nor 2. hold. Then there exists an infinite descending series

\[ Ra_1 \supseteq Ra_2 \supseteq \ldots Ra_n \supseteq Ra_{n+1} \supseteq \ldots \]

and an element \( 0 \neq a \) contained in each \( Ra_n \). Let \( a = r_na_n \) with \( r_n \in R \). Since \( a_{n+1} \in Ra_n \), \( a_{n+1} = sa_n \) for some \( s \in R \). Thus

\[ r_na_n = a = r_{n+1}a_{n+1} = r_{n+1}sa_n \]

As \( R \) is an integral domain, \( r_n = r_{n+1}s \) and so \( Rr_n \subseteq Rr_{n+1} \). If \( Rr_{n+1} = Rr_n \), then \( Rr_{n+1} = Rsr_{n+1} \). So \( r_{n+1} \sim sr_{n+1} \) and by 3.3.3, \( s \) is a unit. As \( a_{n+1} = sa_n \) we conclude that \( Ra_n = Ra_{n+1} \), a contradiction. Thus

\[ Rr_1 \subsetneq Rr_2 \subsetneq \ldots Rr_n \subsetneq Rr_{n+1} \subsetneq \ldots \]

is an infinite strictly ascending series of ideals.

\[ \square \]

Lemma 3.3.11 \[\text{maxmin}\] Let \( R \) be a ring in which every ideal is finitely generated.

(a) Any nonempty set of ideals in \( R \) has a maximal member.

(b) Suppose in addition that \( R \) is an integral domain. Then every nonempty set of principal ideals with nonzero intersection has a minimal member.

Proof: (a) By 3.3.9, \( R \) has no strictly ascending series of ideals. Thus (a) holds. (b) follows from 3.3.9 and 3.3.10 \[\square\]

Lemma 3.3.12 \[\text{PIDUFD}\] Every principal ideal domain is a unique factorization domain.

Proof: Let \( S \) be the set of proper elements in \( R \) which can be written as a product of primes. Let \( a \) be proper in \( R \). Let

\[ S = \{(s) \mid a \in (s), s \in S\} \]

We claim that \( S \) is not empty. Indeed, let \( (s) \) be a maximal ideal with \( (a) \subset (s) \). Then \( s \) is irreducible and so by 3.3.6 \( s \) is a prime. Hence \( s \in S \) and \( (s) \in S \). As \( a \in \bigcap S \), \( \bigcap S \) is not empty. So by 3.3.12a, \( S \) has a minimal member, say \( (b) \) with \( b \in S \). Since \( a \in (b) \), \( a = ub \) for some \( u \in R \). Suppose that \( u \) is not a unit. Then as seen above there exists a prime \( p \) dividing \( u \). Then \( pb \) divides \( a \) and so \( a \in (pb) \). But \( pb \in S \) and \( b \not\in (pb) \subsetneq (b) \) a contradiction to the minimal choice of \( (b) \). \[\square\]
3.3. FACTORIZATIONS IN COMMUTATIVE RINGS

Definition 3.3.13 [deuklidring] An Euclidean ring is a commutative ring together with a function \( \phi : R^\# \to \mathbb{N} \) such that:

For all \( a, b \in R \) with \( b \neq 0 \), there exists \( q, r \in R \) with

\[
a = qb + r
\]

and either \( r = 0 \) or \( q(r) < q(b) \).

An Euclidean domain is an Euclidean ring which is also an integral domain.

Some examples:
- \( \mathbb{Z} \) is an Euclidean domain with \( \phi \) the absolute value function.
- Any field is a Euclidean domain with \( \phi = 0 \).
- The polynomial ring over any field is a Euclidean ring with \( \phi \) the degree function.

Lemma 3.3.14 [ERPR] Any Euclidean ring is a principal ring with identity. An Euclidean domain is a PID and a UFD.

Proof: Let \( I \) be a nonzero ideal and let \( 0 \neq a \in I \) with \( \phi(a) \) minimal. Let \( b \in I \). Then by ER2, \( b = qa + r \) for some \( q, r \in R \) with (if \( r \neq 0 \), \( \phi(r) < \phi(a) \)). Suppose that \( r \neq 0 \). Then \( r = b - qa \in I \), a contradiction to the minimal choice of \( \phi(a) \). Thus \( b = qa \in (a) \). Hence \( I = Ra = (a) \) and \( R \) is a principal ring.

To show that \( R \) has an identity note that \( R = Ra \) for some \( e \in R \). In particular, \( a = ea \) for some \( e \in R \). Now for all \( r \in R \), \( r = sa \) for some \( s \) and \( er = esa = sea = sa = r \) so \( e \) is an identity.

The last statement follows form 3.3.12.

Let \( R \) be an euclidean ring and \( \phi : R^\# \to \mathbb{N} \) the corresponding function. Let \( 0 \neq \tilde{a} \in (a) \) with \( \phi(\tilde{a}) \) minimal. From the proof of the previous lemma, \( (\tilde{a}) = (a) \) so \( a \sim \tilde{a} \). Define \( \phi^*(a) = \phi(\tilde{a}) \) We claim that:

(a) \( \phi^*(a) \leq \phi^*(ab) \) for all \( a, b \in R^\# \) with \( ab \neq 0 \).

(b) For all \( a, b \in R \) with \( b \neq 0 \), there exists \( q, r \in R \) with \( a = qb + r \) and either \( r = 0 \) or \( q^*(r) < q^*(b) \).

Let \( d = ab \). Then \( d \in (a) \) and so \( \tilde{d} \in (d) \subseteq (a) \). Thus \( \phi(\tilde{a}) \leq \phi(tilded) \). So (a) holds.

By definition of an euclidean domain, there exists \( r \) with \( s \in R \) and \( t = 0 \) or \( \phi(r) < \phi(b) \). Since \( a = u\tilde{a} \) and \( b = vb \) with \( u, v \) units we get

\[
a = (uvq)b + uvr
\]

. If \( r = 0, uvr = 0 \). Suppose \( r \neq 0 \). As \( u \) and \( v \) are units \( (uvr) = (r) \). Thus

\[
\phi^*(uvr) = \phi^*(r) \leq \phi(r) < \phi(\tilde{b}) = \phi^*(b)
\]

So (b) holds.
Next we introduce greatest common divisor in arbitrary commutative rings. But the reader should be aware that often no greatest common divisor exist.

**Definition 3.3.15** [dgcd] Let $X$ be a subset of the commutative ring $R$ and $d \in R$

(a) We say $d$ is a common divisor of $X$ and write $d \mid X$ if $X \subseteq (d)$, that is if $d \mid x$ for all $d \in X$.

(b) We say that $d$ is greatest common divisor of $X$ and write $d \sim \gcd(X)$ if $d \mid X$ and $e \mid d$ for all $e \in R$ with $e \mid X$.

(c) We say that $X$ is relatively prime if all commons divisors of $X$ are units.

Note that if a greatest common divisor exists it is unique up to associates. A common divisor exists if and only if $(X)$ is contained in a principal ideal. A greatest common divisor exists if and only if the intersection of all principal ideals containing $X$ is a principal ideal. (Here we define the intersection of the empty set of ideals to be the ring itself). The easiest case is then $(X)$ itself is a principal ideal. Then the greatest common divisors are just the generators of $(X)$. An element in $(X)$ generates $(X)$ if and only if it’s a common divisor. So if the ring has an identity, $(X)$ is a principal ideal if and only if $X$ has a common divisor of the form $\sum_{x \in X} r_xx$, where as usually all but finitely many $r_x$’s are supposed to be 0.

Note that from the above we have the following statement:

Every subset of $R$ has a greatest common divisor if and only if any intersection of principal ideals is a principal ideal. That is if and only if the set of principal ideals in $R$ is closed under intersections.

In particular, greatest common divisors exists in PID’s and can be expressed as a linear combination of the $X$.

Greatest common divisors still exists in UFD’s, but are no longer necessarily a linear combination of $X$. Indeed let $\mathcal{P}$ be a set of representatives for the associate classes of primes. For each $0 \ne r \in R$,

$$x = u_r \prod_{p \in \mathcal{P}} p^{m_p(r)}$$

for some $m_p(r) \in \mathbb{N}$ and a unit $u_r$. Let

$$m_p = \min_{x \in X} m_p(x).$$

Since $m_p \le m_p(x)$ only finitely many of the $m_p$ are nonzero. So we can define

$$d = \prod_{p \in \mathcal{P}} p^{m_p}.$$

A moments thought reveals that $d$ is a greatest common divisor.

Here are a couple of concrete examples which might help to understand some of the concepts we developed above.
3.3. FACTORIZATIONS IN COMMUTATIVE RINGS

First let \( R = \mathbb{Z}[i] \), the subring of \( \mathbb{C} \) generated by \( i \). \( \mathbb{R} \) is called the ring of Gaussian integers.

Note that \( R = \mathbb{Z} + \mathbb{Z}i \). We will first show that \( R \) is an Euclidean ring. Indeed, put 
\[
\phi(a_1 + a_2i) = a_1^2 + a_2^2.
\]
Then \( \phi(xy) = \phi(x)\phi(y) \) and \( \phi(x) \in \mathbb{Z}^+ \). So (ER1) holds. Let 
\( x, y \in R \) with \( x \neq 0 \). Put \( z = \frac{y}{x} \in \mathbb{C} \). Then \( y = zx \). Also there exists \( d = d_1 + d_2i \in \mathbb{C} \) with \( q := z - d \in \mathbb{R} \) and \( \lvert d_i \rvert \leq \frac{1}{2} \). In particular, \( \phi(d) \leq \frac{1}{2} + \frac{1}{2} = \frac{1}{2} \). Put \( r = y - qx \) then 
\[
r = zx - qx = (z - q)x = dx .
\]
So \( \phi(r) = \phi(d)\phi(x) \leq \frac{1}{2}\phi(x) \). Hence also (ER2) holds.

Let \( a \) be a prime in \( R \) and put \( P = (a) \). Since \( \phi(a) = aa \in P \), \( P \cap \mathbb{Z} \neq 0 \). Also \( 1 \notin P \) and so \( P \cap \mathbb{Z} \) is a proper ideal in \( \mathbb{Z} \). Since \( R / P \) has no zero divisors, \( \mathbb{Z} + P / P \cong \mathbb{Z} / P \cap \mathbb{Z} \) has no zero divisors. Thus \( P \cap \mathbb{Z} = p\mathbb{Z} \) for some prime integer \( p \). Let \( Q = pR \). Then \( Q \leq P \leq R \). We will determine the zero divisors in \( R/Q \). Indeed suppose that \( ab \in Q \) but neither \( a \) nor \( b \) are in \( Q \). Then \( p^2 \) divides \( \phi(ab) \). So we may assume that \( p \) divides \( \phi(a) \). Hence \( a_1^2 = a_2^2 \) (mod \( p \)). If \( p \) divides \( a_1 \) it also divides \( a_2 \), a contradiction to \( a \notin Q \). Therefore we can divide by \( a_2 \) (mod \( p \)) and conclude that the equation \( x^2 = -1 \) has a solution in \( \mathbb{Z}/p\mathbb{Z} \). Conversely, if \( n^2 \equiv -1 \) (mod \( p \)) for some integers \( n \) we see that (up to associates) \( n+i+Q \) and \( n-i+Q \) are the only zero divisors.

Suppose that no integer \( n \) with \( n^2 \equiv -1 \) (mod \( p \)) exists. Then \( R/Q \) is an integral domain and so a field. Hence \( Q = P \) and \( a \sim p \) in this case.

Suppose that \( n \) is an integer with \( n^2 \equiv -1 \) (mod \( p \)). As \( P \) is a prime ideal and \( (n+i)(n-i) \in Q \leq P \), one of \( n+i \) is in \( P \). We conclude that \( a \sim n+i \).

Next let \( R = \mathbb{Z}[\sqrt{10}] \). We will show that \( R \) has some irreducible elements which are not primes. In particular, \( R \) is neither UFD, PID or Euclidean. Note that \( R = \mathbb{Z} + \mathbb{Z}\sqrt{10} \). For \( r \in R \) define \( r_1, r_2 \in \mathbb{Z} \) by \( r = r_1 + r_2\sqrt{10} \). Define \( \tilde{r} = r_1 - r_2\sqrt{10} \) and \( N(r) = r\tilde{r} = r_1^2 - 10r_2^2 \). \( N(r) \) is called the norm of \( r \). We claim that \( r \rightarrow \tilde{r} \) is a ring automorphism of \( R \). Clearly it is an automorphism of \( (\mathbb{R}, +) \). Let \( r, s \in R \). Then 
\[
rs = (r_1 + r_2\sqrt{10})(s_1 + s_2\sqrt{10}) = (r_1s_1 + 10r_2s_2) + (r_1s_2 + r_2s_2)\sqrt{10}
\]
It follows that \( \tilde{r}s = \tilde{r}s \). In particular,
\[
N(rs) = rs\tilde{r}s = rs\tilde{r}s = r\tilde{r}s\tilde{s} = N(r)N(s)
\]
and \( N : R \rightarrow \mathbb{Z} \) is a multiplicative homomorphism. Let \( r \) be a unit in \( R \). Since \( N(1) = 1 \), we conclude that \( N(r) \) is unit in \( \mathbb{Z} \) and so \( N(r) = \pm 1 \). Conversely, if \( N(r) = \pm 1 \), then \( r^{-1} = \frac{\tilde{r}}{N(r)} = N(r)\tilde{r} \in R \) and \( r \) is a unit. For example \( 3 + \sqrt{10} \) is unit with inverse \( -3 + \sqrt{10} \). As \( \sqrt{10} \) is not rational, \( N(r) \neq 0 \) for \( r \in R^\# \).

We claim that all of \( 2, 3, f := 4 + \sqrt{10} \) and \( \tilde{f} \) are irreducible. Indeed suppose that \( ab \) is one of those numbers and neither \( a \) nor \( b \) are units. Then \( N(a)N(b) \in \{4, 9, 6\} \) and so \( N(a) \in \{\pm 2, \pm 3\} \) and 
\[
N(a) \equiv 2, 3 \pmod{5}
\]
But for any \( x \in R \) we have 
\[
N(a) \equiv a_1^2 \equiv 0, 1, 4 \pmod{5}
\]
So indeed 2, 3, f and \( \tilde{f} \) are primes. Note that 2 \cdot 3 = 6 = -f\tilde{f}. Hence 2 divides \( f\tilde{f} \) but (as \( f \) and \( \tilde{f} \) are irreducible) 2 divides neither \( f \) nor \( \tilde{f} \). So 2 is not a prime. With the same argument none of 3, \( f \) and \( \tilde{f} \) are not primes.

We claim that every proper element in \( R \) is a product of irreducible. Indeed let \( a \) be proper in \( R \) and suppose that \( a \) is not irreducible. Then \( a = bc \) with neither \( b \) nor \( c \) units. Then as \( N(a) = N(b)N(c) \) both \( b \) and \( c \) have smaller norm as \( a \). So by induction on the norm, both \( b \) and \( c \) can be factorized into irreducible.

Since \( R \) has irreducibles which are not primes, we know that \( R \) can not be a PID. But let us verify directly that \( I = (2, f) = 2R + fR \) is not a principal ideal. First note that \( f\tilde{f} = -6 \in 2R \). Since also \( 2f \in 2R \) we \( I\tilde{f} \in 2R \). Since 4 does not divide \( N(f) \), \( f \not\in 2R \) and so \( I \) does not contain a unit. Suppose now that \( h \) is a generator for \( I \). Then \( h \) is not a unit and divides \( f \). So as \( f \) is irreducible, \( h \sim f \) and \( I = (f) \). But every element in \( (f) \) has norm divisible by \( N(f) = 6 \), a contradiction to \( 2 \in I \) and \( N(2) = 4 \).

### 3.4 Localization

Let \( R \) be a commutative ring and \( \emptyset \neq S \subseteq R \). In this section we will answer the following question:

Does there exists a commutative ring with identity \( R' \) so that \( R \) is a subring of \( R' \) and all elements in \( S \) are invertible in \( R' \)?

Clearly this is not possible if \( 0 \in S \) or \( S \) contains zero divisors. It turns out that this condition is also sufficient. Note that if all elements in \( S \) are invertible in \( R' \), also all elements in the subsemigroup of \( (R, \cdot) \) generated by \( S \) are invertible in \( R' \). So we may assume that \( S \) is closed under multiplication:

**Definition 3.4.1 [dmult]** A multiplicative subset of the ring \( R \) is a nonempty subset \( S \) with \( st \in S \) for all \( s, t \in S \).

**Lemma 3.4.2 [fractions]** Let \( S \) be a multiplicative subset of the commutative ring \( R \). Define the relation \( \sim \) of \( R \times S \) by

\[
(r_1, s_1) \sim (r_2, s_2) \quad \text{if} \quad t(r_1s_2 - r_2s_1) = 0 \text{ for some } t \in S.
\]

Then \( \sim \) is an equivalence relation.

**Proof:** \( \sim \) is clearly reflexive and symmetric. Suppose now that \( (r_1, s_1) \sim (r_2, s_2) \) and \( (r_2, s_2) = (r_3, s_3) \). Pick \( t_1 \) and \( t_2 \) in \( S \) with

\[
t_1(r_1s_2 - r_2s_1) = 0 \text{ and } t_2(r_2s_3 - r_3s_2) = 0.
\]

Multiply the first equation with \( t_2s_3 \) and the second one with \( t_1s_1 \). Then both equation contain the term \( t_1t_2r_2s_1s_3 \) but with opposite sign. So adding the two resulting equations we see:

\[
0 = t_2s_3t_1r_1s_4 - t_1s_1t_2r_3s_2 = t_1t_2s_2(r_1s_3 - r_3s_1)
\]
Thus \((r_1, s_1) \sim (r_3, s_3)\). \(\Box\)

Let \(S, R\) and \(\sim\) as in the previous lemma. Then \(S^{-1}R\) denotes the set of equivalence classes of \(\sim\). \(\frac{r}{s}\) stands for the equivalence class containing \((r, s)\). Note that if \(0 \in S\), \(\sim\) has exactly one equivalence class. If \(R\) has no zero divisors and \(0 \notin S\) then \(\frac{r_1}{s_1} = \frac{r_2}{s_2}\) if and only if \(r_1s_2 = r_2s_1\).

**Proposition 3.4.3** \(\text{ringfrac}\) Let \(S\) be a multiplicative subset of the commutative ring \(R\) and \(s \in S\)

(a) The binary operations

\[
\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \quad \text{and} \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}
\]

on \(S^{-1}R\) are well-defined.

(b) \((S^{-1}R, +, \cdot)\) is an ring.

(c) \(\frac{r}{s}\) is an identity.

(d) The map

\[
\phi_S : R \to S^{-1}R, \quad r \mapsto \frac{rs}{s}
\]

is a ring homomorphism and independent from the choice of \(s\).

(e) \(\phi_S(s)\) is invertible.

**Proof:**  (a) By symmetry it suffices to check that the definition of \(+\) and \(\cdot\) does not depend on the choice of \((r, s)\) in \(\frac{r}{s}\). Let \(\frac{r}{s_1} = \frac{r}{s}\) so \(t(rs_1 - r_1s) = 0\) for some \(t \in S\).

Then

\[
t[(rs' + r's)s_1s' - (r_1s' + r's_1)ss'] = t(rs_1 - r_1s)s's' = 0
\]

and so \(+\) is well defined. Also

\[
t(rr's_1s' - r_1r'ss') = t(rs_1 - r_1s)r's' = 0
\]

and so \(\cdot\) is well defined.

(b) It is a routine exercise to check the various rules for a ring. Maybe the least obvious one is the associativity of the addition:

\[
\frac{r_1}{s_1} + \frac{r_2}{s_2} + \frac{r_3}{s_3} = \frac{r_1s_2 + r_2s_1 + r_3}{s_1s_2s_3} = \frac{r_1s_2s_3 + r_2s_1s_3 + r_3s_1s_2}{s_1s_2s_3} = \frac{r_1}{s_1} + \frac{r_2s_3 + r_3s_2}{s_2s_3} = \frac{r_1}{s_1} + \left(\frac{r_2}{s_2} + \frac{r_3}{s_3}\right)
\]

We leave it to the reader to check the remaining rules.

(c) and (d) are obvious. For (e) note that \(\phi_S(s) = \frac{s^2}{s}\) has \(\frac{s}{s^2}\) as its inverse. \(\Box\)

The ring \(S^{-1}R\) is called the ring if fraction of \(R\) by \(S\). It has the following universal property:
Proposition 3.4.4 Let $R$ be a commutative ring, $S_0$ a non-empty subset and $S$ the multiplicative subset of $R$ generated by $S$. Suppose that $R'$ is a commutative ring with identity and $\alpha(R) \to R'$ is a ring isomorphism so that $\alpha(s_0)$ is a unit for all $s_0 \in S_0$. Then there exists a unique homomorphism $\alpha^*: S^{-1}R \to R'$ with $\phi_S(r) \to \alpha(r)$.

Moreover, $\alpha^*(\frac{r}{s}) = \alpha(r)\alpha(s)^{-1}$.

**Proof:** Note that as $\alpha(S_0)$ consists of units so does $\alpha(S)$. So once we verify that $\alpha^*(\frac{r}{s}) = \alpha(r)\alpha(s)^{-1}$ is well defined, the remaining assertion are readily verified. 

So suppose that $\frac{r_1}{s_1} = \frac{r_2}{s_2}$. Then $t(r_1s_2 - r_2s_1) = 0$

for some $t \in S$. Applying $\alpha$ we conclude

$\alpha(t)(\alpha(r_1)\alpha(s_2) - \alpha(r_2)\alpha(s_1)) = 0$.

As $\alpha(t), \alpha(s_1)$ and $\alpha(s_2)$ are units, we get

$\alpha(r_1)\alpha(s_1)^{-1} = \alpha(r_2)\alpha(s_2)^{-1}$

Hence $\alpha^*$ is indeed well-defined. 

When is $\frac{r}{s} = 0$? The zero element in $S^{-1}R$ is $\frac{0}{1}$. Hence $\frac{r}{s} = 0$ if and only if there exists $t \in S$ with $0 = t(rs - 0s) = trs$ for some $t \in S$. This is true if and only if $tr = 0$ for some $t \in S$. Put $R_S = \{r \in R \mid tr = 0 \text{ for some } t \in S\}$.

So $\frac{r}{s} = 0$ if and only $r \in R_S$.

What is the kernel of $\phi = \phi_S$? $\phi(r) = \frac{rs}{s}$. Hence $r \in \ker \phi$ if and only if $rs \in R_S$ and so if and only if $r \in R_S$. Thus $\ker \phi = R_S$. So $\phi$ is one to one if and only if $R_S = 0$. This in turn just means that $S$ contains no zero divisors. In this is the case we will identify $R$ with its image in $S^{-1}R$.

Let $\hat{R}$ be the set of all non-zero, non zero divisors. and assume $\hat{R} \neq \emptyset$. We claim that $\hat{R}$ is a multiplicative set. Indeed let $s, t \in \hat{R}$. Suppose that $rst = 0$ for some $r \in R$. Then as $t \in \hat{R}$, $rs = 0$ and as $s \in \hat{R}$, $r = 0$ so $st \in \hat{R}$. The $\hat{R}^{-1}R$ is called the complete ring of fraction of $R$.

If $R$ has no zero divisors, then $\hat{R} = R^\#$ and the complete ring of fraction is a field. This field is called the field of fraction of $R$ and denoted by $\mathbb{F}_R$. 

The standard example is $R = \mathbb{Z}$. Then $\mathbb{F}_\mathbb{Z} = \mathbb{Q}$.

If $K$ is a field then $\mathbb{F}_K[x] = K(x)$, the field of rational functions over $K$. Slightly more general if $R$ has no-zero divisors then $\mathbb{F}_{R[x]} = \mathbb{F}_R(x)$, the field of rational function over the field of fractions of $R$.

We will now spend a little but of time to investigate the situation where $S$ does contain some zero divisors.

Define

$$\phi^* : S^{-1}R \to \phi(S)^{-1}\phi(R), \quad \frac{r}{s} \to \frac{\phi(r)}{\phi(s)}$$

We claim that $\phi^*$ is a well defined isomorphism. For this we prove the following lemma.

**Lemma 3.4.5** \[\text{alp}\] Let $\alpha : R \to R'$ be a homomorphism of commutative rings and $S$ and $S'$ multiplicative subsets of $R$ and $R'$ respectively. Suppose that $\alpha(S) \subseteq S'$.

(a) $\alpha(S)$ is a multiplicative subset of $R'$.

(b)

$$\alpha^* : S^{-1}R \to S'^{-1}R', \quad \frac{r}{s} \to \frac{\alpha(r)}{\alpha(s)}$$

is a well defined homomorphism.

(c) Suppose that $S' = \alpha(S)$. Then

$$\ker \alpha^* = \left\{ \frac{r}{s} \mid r \in R, s \in S, Sr \cap \ker \alpha \neq \emptyset \right\} \text{ and } \alpha^*(S^{-1}R) = \alpha(S)^{-1}\alpha(R)$$

**Proof:**

(a) Just note that $\alpha(s)\alpha(t) = \alpha(st)$ for all $s, t \in S$.

(b) Note that $\phi_{S'}(\alpha(s))$ is invertible. Hence $\alpha^*$ is nothing else as the homomorphism given by 3.4.4 applied to the homomorphism:

$$\phi_{S'} \circ \alpha : R \to S'^{-1}R'$$

(c) Let $\frac{r}{s} \in \ker \alpha^*$. As seen above this means $t'\alpha(r) = 0$ for some $t' \in S'$. By assumption $t' = \alpha(t)$ for some $t \in T$. Thus $\frac{r}{s} = 0$ if and only if $tr \in \ker \alpha$ for some $t \in S$.

That $\alpha^*(S^{-1}R) = \alpha(S)^{-1}\alpha(R)$ is obvious.

Back to the map $\phi^*$. By the previous lemma $\phi^*$ is a well defined homomorphism and onto. Let $\frac{r}{s} \in \ker \phi^*$. Then $tr \in \ker \phi$ for some $t \in S$. As $\ker \phi = R_S$, $itr = 0$ for some $\tilde{t} \in S$. Hence $r \in R_S$ and $\frac{r}{s} = 0$. Therefore $\phi^*$ is one to one and so an isomorphism.

Note also that $\phi(R) \cong R/R_S$. Let $\bar{R} = R/R_S$ and $\bar{S} = S + R_S/R_S$. As $\phi^*$ is an isomorphism we get

$$S^{-1}R \cong \bar{S}^{-1}\bar{R}$$

We have $\bar{R}_S = 0$. So in some sense we can always reduce to the case where $S$ has no zero divisors.
In the next lemma we study the ideals in $S^{-1}R$. For $A \subset R$ and $T \subseteq S$ put

$$T^{-1}A = \{ \frac{a}{t} \mid a \in A, t \in T \}$$

**Proposition 3.4.6 [idealfrac]** Let $S$ be a multiplicative subset of the commutative ring $R$.

(a) If $I$ is an ideal in $R$ then $S^{-1}I$ is an ideal in $S^{-1}R$

(b) If $J$ is an ideal in $R$ then $I = \phi_S^{-1}(J)$ is an ideal in $R$ with $J = S^{-1}I$.

(c) The map $I \to S^{-1}I$ is a surjection from the set of ideals in $I$ to the set of ideals to $S^{-1}R$.

**Proof:** Put $\phi = \phi_S$.

(a) is readily verified.

(b) Inverse images of ideals are always ideals. To establish the second statement in (b) let $j = \frac{r}{s} \in J$. As $J$ is an ideal

$$\frac{s^2 r}{s^2} = \frac{rs^2}{s^2} = \frac{rs}{s} \in J$$

Thus $\phi(r) \in J$ and $r \in I$. So $j = \frac{r}{s} \in S^{-1}I$.

Conversely, if $r \in I$ and $s \in S$ then since $\phi(r) \in J$ an $dJ$ is an ideal:

$$\frac{r}{s} = \frac{rs^2}{s^3} = \frac{s}{s^2} \frac{rs}{s} = \frac{s}{s^2} \phi(r) \in \frac{s}{s^2} J \subseteq J$$

So (b) holds.

(c) follows from (a) and (b). \qed

If $R$ has an identity the previous proposition can be improved:

**Proposition 3.4.7 [idfraid]** Let $R$ be a commutative ring with identity and $S$ a multiplicative subset $R$.

(a) Suppose $R$ has an identity. Let $I$ be an ideal in $R$. Then

$$\phi_S^{-1}(S^{-1}I) = \{ r \in R \mid Sr \cap I \neq \emptyset \}.$$

(b) Define an ideal $I$ in $R$ to be $S^{-1}$-closed if $r \in I$ for all $r \in R$ with $rS \cap I \neq \emptyset$. Then

$$\tau : I \to S^{-1}I$$

is a bijection between the $S^{-1}$-closed ideals and the ideals in $S^{-1}R$. The inverse map is given by

$$\tau^{-1} : J \to \phi_S^{-1}J.$$
3.4. LOCALIZATION

(c) \( I \cap S = \emptyset \) for all \( S^{-1} \) closed ideals with \( I \neq R \).

(d) A prime ideal \( P \) in \( R \) is \( S^{-1} \) closed if and only if \( P \cap S = \emptyset \).

(e) \( \tau \) induces a bijection between the \( S^{-1} \) closed prime ideals in \( R \) and the prime ideals in \( S^{-1}R \).

Proof: (a) Let \( r \in R \) then the following are equivalent:
\[ \phi(r) \in S^{-1}I. \]
\[ \phi(r) = \frac{1}{s} \text{ for some } i \in I, s \in S \]
\[ \frac{r}{1} = \frac{i}{s} \text{ for some } i \in I, s \in S \]
\[ t(rs - i) = 0 \text{ for some } i \in I, s, t \in S \]
\[ tsr = ti \text{ for some } i \in I, s, t \in S \]
\[ sr \in I \text{ for some } s \in S \]
\[ Sr \cap I \neq \emptyset. \]

So (a) holds.
We write \( \phi \) for \( \phi_S \) and say "closed" for \( S^{-1} \) closed.
(b) follows from (a) and 3.4.6b,c.
(c) Suppose \( I \) is closed and \( s \in S \cap I \). Then \( S^{-1}I \) contains the unit \( \phi(s) \) and so \( S^{-1}I = S^{-1}R \). Thus \( I = S^{-1}R \) and \( I = R \).
(d) Let \( P \) be a prime ideal in \( R \). Suppose that \( S \cap P = \emptyset \) and let \( r \in R \) and \( s \in S \) with \( rs \in P \). Then by 3.2.6b, \( r \in P \) or \( s \in P \). By assumption \( s \notin P \) and so \( r \in P \). Thus \( P \) is closed. Conversely, if \( P \) is closed, (c) implies \( P \cap S = \emptyset \).
(e) Let \( P \) be a closed prime ideal. We claim the \( S^{-1}R \) is a prime ideal in \( R \). First since \( \tau \) is an bijection, \( S^{-1}P \neq R \). Suppose that \( \frac{r}{s}, \frac{r'}{s'} \in S^{-1}P \). Then also \( \phi(rr') \in S^{-1}P \). As \( P \) is closed, \( rr' \in P \). As \( P \) is prime we may assume \( r \in P \). But then \( \frac{r}{s} \in S^{-1}P \) and so \( S^{-1}P \) is a prime.

Suppose next that \( I \) is closed and \( S^{-1}I \) is a prime. If \( rr' \in I \), then \( \phi(r)\phi(r') \in S^{-1}I \). As \( S^{-1}I \) is prime we may assume that \( \phi(r) \in S^{-1}I \). As \( I \) is closed this implies \( r \in I \) and so \( I \) is a prime ideal. \( \square \)

Let \( R \) be a commutative ring with identity. By 3.2.6 an ideal \( P \) in \( R \) is a prime ideal if and only if \( R \setminus P \) is a multiplicative subset of \( R \). Let \( P \) be the prime ideal. The ring
\[ R_P := (R \setminus p)^{-1}R \]
is called the localization of \( R \) at the prime \( P \). For \( A \subseteq R \) write \( A_P \) for \( (R \setminus p)^{-1}A \).

Theorem 3.4.8 [localprimes] Let \( P \) be a prime ideal in the commutative ring with identity \( R \).

(a) The map \( Q \to Q_P \) is a bijection between the prime ideals of \( R \) contained in \( P \) and the prime ideals in \( R_P \).

(b) \( P_P \) is the unique maximal ideal in \( R_P \). \( r \in R \) is a unit if and only if \( r \notin P_P \).
Proof: (a) Put $S = R \setminus P$ and let $Q$ a prime ideal in $R$. Then $Q \cap S = \emptyset$ if and only if $Q \subseteq P$. Thus (a) follows from ??.

(b) Let $I$ be a maximal ideal in $R_P$. Then by 3.2.9 $I$ is prime ideal. Thus by (a) $I = Q_P$ for some $Q \subseteq P$. Thus $I \subseteq P_P$ and $I = P_P$. The statement about the units now follows from 3.3.2.

Actually we could also have argued as follows: all elements in $R_P \setminus P_P$ are of the form $\frac{s}{x^r}$ and so invertible. Hence by 3.3.2 $P_P$ is the unique maximal ideal in $R$.

Definition 3.4.9 A local ring is a commutative ring with identity which as a unique maximal ideal.

Using 3.3.2 we see

Lemma 3.4.10 [chlocal] Let $R$ be a commutative ring with identity. The the following are equivalent:

(a) $R$ is a local ring.

(b) All the non-units are contained in an ideal $M \leq R$.

(c) All the non-units form an ideal.

We finish this section with some examples.

Let $p$ be an prime integer. Then $\mathbb{Z}_{(p)} = \{ \frac{n}{m} \in \mathbb{Q} \mid p \nmid m \}$. Since 0 and $(p)$ are the only prime ideals of $\mathbb{Z}$ contained in $(p)$, $O$ and $\frac{n}{m} \in \mathbb{Q} \mid p \nmid m, p \mid n$ are the only prime ideal in $\mathbb{Z}_{(p)}$. What are the ideals? Every non zero ideal of $\mathbb{Z}$ is of the form $(t)$ for some $t \in \mathbb{Z}^+$. Write $t = ap^k$ with $p \nmid a$. Suppose $(t)$ is closed. As $a \in S = \mathbb{Z} \setminus (p)$ and $ap^k \in (t)$ we conclude that $p^k \in (t)$. Thus $a = 1$ and $t = p^k$. It is easy to see that $(p^k)$ is indeed closed.

So we conclude that the ideals in $\mathbb{Z}_{(p)}$ are

$$p^k \mathbb{Z}_{(p)} = \{ \frac{n}{m} \in \mathbb{Q} \mid p \nmid m, p^k \mid n \}$$

In particular $\mathbb{Z}_{(p)}$ is a PID.

We reader might have notice that in the above discussion $\mathbb{Z}$ can be replaced by any PID $R$, p by any prime in $R$ and $\mathbb{Q}$ by $F_R$.

3.5 Polynomials rings, power series and free rings

Let $R$ be a ring and $(A, +)$ a group written additively. Since $(A, +)$ is a subgroup of the multiplicative group of $R$ it is convenient to the following "exponential notation. Denote $a \in A$ be $x^a$ and define $x^a x^b = x^{a+b}$. The the elements in $R[A]$ can be uniquely written as $f = \sum_{a \in A} f_a x^a$ where $f_a \in R$, almost all $f_a = 0$. Also
Let $R$ be a ring and $I$ a set. Put $\mathbb{I} = \bigoplus_{i \in I} \mathbb{N}$, the free abelian monoid on $I$. The semigroup ring

$$R[\mathbb{I}]$$

is called the polynomial ring over $R$ in the variables $I$ and is denoted by $R[I]$. We will use the above exponential notation. Let $i \in I$. Recall that $\phi_i(1) \in \mathbb{I}$ is defined as

$$(\phi_i(1))_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

We write $x_i$ for $x^{\phi_i(1)}$. Let $\alpha \in \mathbb{I}$, then $\alpha$ is a tuple $(\alpha_i)_{i \in I}$, $\alpha_i \in \mathbb{N}$, where almost all $\alpha_i$ are zero. So

$$x^\alpha = \prod_{i \in I} x_i^{\alpha_i}.$$

Every element $f \in R[I]$ now can be uniquely written as

$$f = \sum_{\alpha \in \mathbb{I}} f_\alpha x^\alpha$$

where $f_\alpha \in R$ and almost all $f_\alpha$ are zero. The element of $R[I]$ are called polynomials. Polynomials of the form $rx^\alpha$, with $r \neq 0$, are called monomials. As almost all $\alpha_i$ are zero

$$rx^\alpha = r x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} \cdots x_{i_n}^{\alpha_{i_n}}$$

for some $i_k \in I$.

The $f_\alpha x^\alpha$ with $f_\alpha \neq 0$ are called the monomials of $f$. So every polynomial is the sum of its monomials.

Note that the map $r \rightarrow rx^0$ is monomorphism. So we can and do identify $r$ with $rx^0$.

If $I = \{1, 2, \ldots, m\}$ we also write $R[x_1, \ldots, x_m]$ for $R[I]$. Then every element in $R[x_1, \ldots, x_m]$ can be uniquely written as

$$\sum_{n_1=0}^{\infty} \sum_{n_2=0}^{\infty} \cdots \sum_{n_m=0}^{\infty} r_{n_1,\ldots,n_m} x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}$$

If $I$ has a unique element $i$ we write $x$ for $x_i$ and $R[x]$ for $R[I]$. Then each $f \in R[x]$ has the form $f = r_0 + r_1 x + r_2 x^2 + \ldots + r_n x^n$, where $n$ is maximal with respect to $r_n \neq 0$. $r_n$ is called the leading coefficient of $f$ and $n$ the degree of $f$.

Note that if $I$ happens to have the structure of a semigroup, the symbol $R[I]$ has a double meaning, the polynomial ring or the semigroup ring. But this should not lead to any confusions.
If \( y = (y_i, i \in I) \) is a family of pairwise commuting elements is some semigroup, and \( \alpha \in \mathbb{I} \) we define
\[
y^\alpha = \prod_{i \in I} y_i^{\alpha_i}
\]
Note that as almost all \( \alpha_i \) are zero and the \( y_i \) pairwise commute, this is well-defined. Also if we view the symbol \( x \) as the family (\( x_i, i \in I \)), this is consistent with the \( x^\alpha \) notation.

The polynomial ring has the following universal property:

**Proposition 3.5.1 [polev]** Let \( \Phi : R \to S \) be a ring homomorphism and \( y = (y_i)_{i \in I} \) a family of elements in \( S \) such that

(a) For all \( r \in R \) and all \( i \in I \)
\[
\Phi(r)y_i = y_i\Phi(r)
\]

(b) for all \( i, j \in I \)
\[
y_iy_j = y_jy_i
\]

Then there exists a unique homomorphism
\[
\Phi_y : R[I] \to S; \text{ with } rx_i \to \Phi(r)y_i \text{ for all } r \in R, i \in I.
\]

Moreover,
\[
\Phi_y : \sum_{\alpha \in \mathbb{I}} f_\alpha x^\alpha \to \sum_{\alpha \in \mathbb{I}} \Phi(f_\alpha)y^\alpha.
\]

**Proof:** As \( \mathbb{I} \) is the free abelian monoid on \( I \), (b) implies that there exists a unique homomorphism \( \beta : \mathbb{I} \to (S, \cdot) \) with \( \alpha(x_i) = y_i \). The existence of \( \Phi_y \) now follows from 3.1.6. The uniqueness is obvious. \( \square \)

The reader should notice that the assumption in the previous proposition are automatically fulfilled if \( S \) is commutative. So each \( f \in R[I] \) gives rise to a function \( f^\Phi : S^I \to S \) with \( f^\Phi(y) = \Phi_y(f) \).

**Example:** Suppose \( I = \{1, 2, \ldots, m\} \), \( R = S \) is commutative and \( \alpha = \text{id} = id_R \) and
\[
f = \sum r_{n_1, \ldots, n_m} x_1^{n_1} \cdots x_m^{n_m}
\]
Then
\[
f^\text{id}(y_1, \ldots, y_n) = \sum r_{n_1, \ldots, n_m} y_1^{n_1} \cdots y_m^{n_m}.
\]
The reader should be careful not to confuse the polynomial \( f \) with the function \( f^\text{id} \). Indeed the following example shows that \( f^\text{id} \) can be the zero function without \( f \) being zero.

Let \( R = \mathbb{Z}/p\mathbb{Z}, I = 1, p \) a prime integer, and
\[
f = x(x - 1)(x - 1) \cdots (x - (p - 1))
\]
Then \( f \) is a polynomial of degree \( p \) in \( (\mathbb{Z}/p\mathbb{Z})[x] \). But \( f^\text{id}(y) = 0 \) for all \( y \in \mathbb{Z}/p\mathbb{Z} \).
Lemma 3.5.2 [RIJ] Let $R$ be a ring and $I$ and $J$ disjoint sets. Then there exists a unique isomorphism

$$R[I][J] \rightarrow R[I \cup J]$$

with $rx_i \rightarrow rx_i$ and $rx_j \rightarrow rx_j$

for all $r \in R, i \in I, j \in J$.

**Proof:** Use 3.5.1 to show the existence of such a homomorphism and its inverse. We leave the details to the reader. \qed

Let $R$ be a ring and $G$ a semigroup. In the definition of the semigroup ring $R[G]$ we had to use the direct sum rather than the direct product since otherwise the definition of the products of two elements would involve infinite sums. But suppose $G$ has the following property

$$(FP) \quad |\{(a, b) \in G \times G \mid ab = g\}| \text{ is finite for all } g \in G.$$

Then we can define the **power semigroup ring** of $G$ over $R$, $R[[G]]$ by

$$(R[[G]], +) = (\prod_{g \in G} R, +)$$

and

$$(rg)_g \in G \cdot (sg)_g \in G = (\sum_{(h, k) \in G \times G | hk = g} rh s_k)_g \in G$$

If $G$ is a group then it fulfills $(FP)$ if and only if $G$ is finite. So we do not get anything new. But there are lots of infinite semigroups with $(FP)$. For example $G = \mathbb{N}$. $R[[\mathbb{N}]]$ is isomorphic to $R[[x]]$ the ring of formal power series. Other semigroups with $(FP)$ are the free (abelian) monoids (or semigroups) over a set

Let $I$ be a set. Then the power semigroup ring

$$R[\bigoplus_{i \in I} \mathbb{N}]$$

is called the ring of **formal power series** over $R$ in the variables $I$ and is denoted by $R[[I]]$. The elements of $R[[I]]$ are called formal power series. We use the same exponential notation as for the ring of polynomials. Every formal power series can be uniquely written as a formal sum

$$f = \sum_{\alpha \in I} f_{\alpha} x^\alpha$$

Here $f_{\alpha} \in R$. But in contrast to the polynomials we do not require that almost all $f_{\alpha}$ are zero.

If $I = \{1\}$ the formal power series have the form:

$$f = \sum_{n=0}^{\infty} f_n x^n = f_0 + f_1 x + f_2 x^2 \ldots f_n x^n \ldots$$

with $f_n \in R$. Note that there does not exist an analog for 3.5.1 for formal power series, since the definition of $\Phi_y(f)$ involves an infinite sum.
Lemma 3.5.3 [invpower] Let $R$ be ring with identity and $f \in R[[x]]$.

(a) $f$ is a unit if and only if $f_0$ is.

(b) If $R$ is commutative and $f_0$ is irreducible, then $f$ is irreducible.

Proof: (a) Note that $(fg)_0 = f_0g_0$ and $1_0 = 1$ so if $f$ is a unit so is $f_0$. Suppose now that $f_0$ is a unit. We define $g \in R[[x]]$ by defining its coefficients inductively as follows $g_0 = f_0^{-1}$ and for $n > 0$,

$$g_n = -f_0^{-1}\sum_{i=0}^{n-1} f_{n-i}g_i$$

Note that this just says $\sum_{i=0}^{n-1} f_{n-i}g_i = 0$ for all $n > 0$. Hence $fg = 1$. Similarly $f$ has a left inverse $h$ by 2.2.2 $g = h$ is a left inverses.

(b) Suppose that $f = gh$. Then $f_0 = g_0h_0$. So as $f_0$ is irreducible, one of $g_0, f_0$ is a unit. Hence by (a) $g$ or $h$ is a unit. \qed

As an example we see that $1 - x$ is a unit in $R[[x]]$. Indeed

$$(1 - x)^{-1} = 1 + x + x^2 + x^3 + \ldots .$$

Lemma 3.5.4 [fdpow] Let $\mathbb{D}$ be a division ring.

(a) $(x) = \{ f \in \mathbb{D}[[x]] \mid f_0 = 0 \}$

(b) The elements of $(x)$ are exactly the non-units of $\mathbb{D}[[x]]$.

(c) Let $I$ be a left ideal in $\mathbb{D}[[x]]$. Then $I = x^n\mathbb{D}[[x]] = (x^k)$ for some $k \in \mathbb{N}$.

(d) Every left ideal in $\mathbb{D}[[x]]$ is a right ideal and $\mathbb{D}[[x]]$ is a principal ideal ring.

(e) $(x)$ is the unique maximal ideal in $\mathbb{D}[[x]]$.

(f) If $\mathbb{D}$ is a field, $\mathbb{D}[[x]]$ is a PID and a local ring.

Proof: (a) is obvious and (b) follows from 3.5.3.

(c) Let $k \in \mathbb{N}$ be minimal with $x^k \in I$. Let $f \in I$ and let $n$ be minimal with $f_n \neq 0$. Then $f = x^ng$ for some $g \in \mathbb{D}[[x]]$ with $g_0 \neq 0$. Hence $g$ is unit and $x^n = g^{-1}f \in I$. So $k \leq n$ and $f = (x^{n-k}g)x^k \in \mathbb{D}[[x]]x^k = (x^k)$. Thus $I = (x^k)$.

(d), (e) and (f) follow immediately from (c).
3.6 Factorizations in polynomial rings

Let $R$ be a ring and $I$ a set and $f \in R[I]$. We define the degree function

$$\deg : R[I] \to \mathbb{N} \cup \{-\infty\}$$

as follows:

(a) if $f$ is a monomial $rx^\alpha$, then $\deg f = \sum_{i \in I} \alpha_i$,

(b) if $f \neq 0$ then $\deg f$ is the maximum of the degrees of its monomials.

(c) if $f = 0$ then $\deg f = -\infty$

Sometimes it will be convenient to talk about the degree $\deg_J f$ with respect to subset $J$ of $I$. This is defined as above, only that

$$\deg_J (rx^\alpha) = \sum_{j \in J} \alpha_j$$

Alternatively, $\deg_J f$ is the degree of $f$ as a polynomial in $R'[J]$, where $R' = R[I \setminus J]$.

A polynomial is called homogeneous if all its monomials have the same degree. Let $f \in R[\langle X \rangle]$ then $f$ can be uniquely written as

$$f = \sum_{i=0}^{\infty} h(f,i)$$

where $h(f,i)$ is zero or a homogenous polynomial of degree $i$. Note here that almost all $h(f,i)$ are zero. Let $h(f) = h(f, \deg f)$.

**Lemma 3.6.1 [basdeg]** Let $R$ be a ring, $I$ a set and $f, g \in R[I]$.

(a) $\deg(f + g) \leq \max(\deg f, \deg g)$ with equality unless $h(g) = -h(f)$.

(b) If $f$ and $g$ are homogeneous, then $fg$ is homogeneous. Also either $\deg(fg) = \deg(f) + \deg(g)$ or $fg = 0$.

(c) $h(fg) = h(f)h(g)$ unless $h(f)h(g) = 0$.

(d) $R[I]$ has no zero divisors if and only if $R$ has no zero divisors.

(e) $\deg fg \leq \deg f + \deg g$ with equality if $R$ has no zero divisors.

**Proof:** (a),(b) and (c) are readily verified.

(d) If $R$ has zero divisors, then as $R$ is embedded in $R[I]$, $R[I]$ has zero divisors.

Suppose next that $R$ has no zero divisors. Let $f, g \in R[I]^\#$. We need to show that $fg \neq 0$. By (c) we may assume that $f$ and $g$ are homogeneous.
Consider first the case that $|I| = 1$. Then $f = ax^n$, $g = bx^m$ and $fg = (ab)x^{n+m}$. Here $a, b \in R^\#$ and so $ab \neq 0$. Thus also $fg \neq 0$. If $I$ is finite, $R[I] = R[I \setminus \{i\}]$ and so by induction $R[I]$ has no zero divisors.

For the general case just observe that $f, g \in R[J]$ for some finite subset $J$ of $I$.

(e) If $R$ has no zero divisors, (d) implies $h(f)h(g) \neq 0$. Thus by (b) and (c),

$$\deg f = \deg h(fg) = \deg h(f)h(g) = \deg h(f) + \deg h(g) = \deg f + \deg g.$$ 

\[\square\]

**Lemma 3.6.2 [RP]** Let $R$ be a ring, $P$ an ideal in $R$ and $I$ a set.

(a) Let $P[I] = \{ f \in R[I] | f \alpha \in P \text{ for all } \alpha \in I \}$. Then $P[I]$ is an ideal in $R[I]$ and

$$R[I]/P[I] \cong (R/P)[I]$$

(b) If $R$ has an identity, $P[I] = P \cdot R[I]$ is the ideal in $R[I]$ generated by $P$.

**Proof:** (a) Define $\phi : R[I] \to (R/P)[I], \sum_{\alpha \in I} f \alpha x^{\alpha} \to \sum_{\alpha \in I} (f \alpha + P)x^{\alpha}$. By 3.5.1 $\phi$ is a ring homomorphism. Clearly $\phi$ is onto and $\ker \phi = P[I]$ so (a) holds.

(b) Let $p \in P$ then $px^{\alpha} \in P \cdot R[I]$. Thus $P[I] \leq P \cdot R[I]$. The other inclusion is obvious. \[\square\]

**Corollary 3.6.3 [pstay]** Let $R$ be a commutative ring with identity, $I$ a set and $p \in R$. Then $p$ is a prime in $R$ if and only if $p$ is a prime in $R[I]$.

**Proof:** $R$ is a prime if and only if $R/pR$ is an integral domain. So by 3.6.1d if and only if $(R/pR)[I]$ is an integral domain. So by 3.6.2 if and only if $R[I]/pR[I]$ is a prime ideal and so if and only if $p$ is a prime in $R[I]$. \[\square\]

**Theorem 3.6.4 (Long Division) [lngdiv]** Let $R$ be a ring and $f, g \in R[x]$. Suppose that the leading coefficient of $g$ is a unit in $R$. Then there exist uniquely determined $q, r \in R$ with

$$f = qg + r \text{ and } \deg r < \deg g$$

**Proof:** Let $h(f) = ax^n$ and $h(g) = bx^m$. If $n < m$, we conclude that $q = 0$ and $r = f$ is the unique solution.

So suppose that $m \leq n$. Then any solution necessarily has $h(f) = h(q)h(g)$ and so $s(q) = ab^{-1}x^{n-m}$. Now $f = qg - r$ if and only if

$$f - ab^{-1}x^{n-m}g = (q - ab^{-1}x^{n-m})g + r$$

So uniqueness and existence follows by induction on $\deg f$. \[\square\]
Let $R$ be a ring and $f \in R[x]$. Define the function

$$f^r : R \rightarrow R, c \mapsto \sum_{\alpha \in \mathbb{N}} f_{\alpha}c^{\alpha}$$

The function $f^r$ is called the right evaluation of $f$. Note here that as $R$ is not necessarily commutative, $f_{\alpha}c^{\alpha}$ might differ from $c^{\alpha}f_{\alpha}$. If $R$ is commutative $f^r = f^{id}$.

The map $f \mapsto f^r$ is an additive homomorphism but not necessarily a multiplicative homomorphism. That is we might have $(fg)^r(c) \neq f^r(c)g^r(c)$. Indeed let $f = rx$ and $g = sx$. Then $fg = (rs)x^2$, $(fg)^r(c) = rsc^2$ and $f^r(c)g^r(c) = rsc$.

**Lemma 3.6.5** $[fgfg]$ Let $R$ be a ring, $f, g \in R[x]$ and $c \in R$. If $g^r(c)c = cg^r(c)$ then

$$(fg)^r(c) = f^r(c)g^r(c).$$

**Proof:** As $f \mapsto f^r$ is a additive homomorphism we may assume that $f = rx^m$ for some $r \in R, m \in \mathbb{N}$. Thus

$$fg = \sum_{\alpha \in \mathbb{N}} rg_{\alpha}x^{\alpha+m}$$

and so

$$(fg)^r(c) = \sum_{\alpha \in \mathbb{N}} rg_{\alpha}c^{\alpha+m} =$$

$$= r(\sum_{\alpha \in \mathbb{N}} g_{\alpha}c^\alpha)c^m = rg^r(c)c^m = rc^m g^r(c) = f^r(c)g^r(c)$$


**Corollary 3.6.6** $[xmc]$ Let $R$ be a ring with identity, $c \in R$ and $f \in R[x]$.

(a) Then there exists a unique $q \in R[x]$ with

$$f = q(x - c) + f^r(c).$$

(b) $f^r(c) = 0$ if and only if $f = q(x - c)$ for some $q \in R[x]$.

**Proof:** (a) By 3.6.4 $f = q \cdot (x - c) + r$ with $\deg r < \deg(x - c) = 1$. Thus $r \in R$. By 3.6.5

$$f^r(c) = q^r(c)(c - c) + r = r$$

Hence $r = f^r(c)$. The uniqueness follows from 3.6.4

(b) follows from (a).
Corollary 3.6.7 \[\text{xmcp}\] Let \( R \) be a commutative ring with identity and \( c \in R \).

(a) \( R[x]/(x - c) \cong R \).

(b) \( x - c \) is a prime if and only if \( R \) is an integral domain.

Proof:
(a) Consider the ring homomorphism \( \text{id}_c : R[x] \to R, f \to f(c) \) (see 3.5.1 Clearly \( \text{id}_c \) is onto. By 3.6.6b \( \ker \text{id}_c = (x - c) \) so (b) follows from the Isomorphism Theorem for rings.

(b) Note that \( x - c \) is a prime if and only if \( R[x]/(x - c) \) has non-zero divisors. Thus (b) follows from (a).

Corollary 3.6.8 Let \( \mathbb{F} \) be a field. Then \( \mathbb{F}[x] \) is an Euclidean domain. In particular, \( \mathbb{F}[x] \) is a PID and a UFD. The units in \( \mathbb{F}[x] \) are precisely the nonzero elements in \( \mathbb{F} \).

Proof: Just note that by 3.6.4 \( \mathbb{K}[x] \) is a Euclidean domain.

Let \( R \) be a subring of the commutative ring \( S \). Write \( R \to S \) for the inclusion map from \( R \) to \( S \). Let \( I \) be a set, \( f \in R[I] \) and \( c \in S^I \). We say that \( c \) is a root of \( f \) if

\[ f^{R \to S}(c) = 0. \]

Let \( R \) be any ring, \( f \in R[x] \) and \( c \in R \). We say that \( c \) is a root of \( f \) if \( f^r(c) = 0 \). Note that for \( R \) commutative this agrees with previous definition of a root for \( f \) in \( R \).

Theorem 3.6.9 \[\text{sroots}\] Let \( D \) be an integral domain contained in the integral domain \( E \). Let \( 0 \neq f \in D[x] \). Let \( m \in \mathbb{N} \) be maximal so that there exists \( c_1, \ldots, c_m \in E \) with

\[ \prod_{i=1}^{m} x - c_i \mid f \]

in \( E[x] \). Let \( c \) be any root of \( f \) in \( E \). Then \( c = c_i \) for some \( i \). In particular, \( f \) has at most \( \deg f \) distinct roots in \( E \).

Proof: Let \( f = g \prod_{i=1}^{m} x - c_i \) with \( g \in E[x] \). By maximality of \( m \), \( x - c \nmid g \). By ?? \( x - c \) is a prime in \( E[x] \) and so

\[ x - c \mid \prod_{i=1}^{m} x - c_i \]

By 3.3.7, \( x - c \sim x - c_i \) for some \( i \). Thus \( x - c = x - c_i \) and \( c = c_i \).

We remark that the previous theorem can be false for non-commutative division rings. For example the polynomial \( x^2 + 1 = 0 \) has six roots in the division ring \( \mathbb{H} \) of quaternions, namely \( \pm i, \pm j, \pm k \).
Let $R$ be a ring, $f \in R[x]$ and $c$ a root of $f$ in $D$. Then by 3.6.9 we can write $f = g(x - c)^m$ with $m \in \mathbb{Z}^+$, $g \in R[x]$ and so that $c$ is not a root of $g$. $m$ is called the multiplicity of the root $g$. If $m \geq 2$ we say that $c$ is a multiple root.

As a tool to detect multiple roots we introduce the formal derivative $f'$ of a polynomial $f \in R[x]$.

$$f' := \sum_{\alpha \in \mathbb{Z}^+} n f_\alpha x^{\alpha - 1}$$

Put $f^{[0]} = f$ and inductively, $f^{[k+1]} = (f^{[k]}')$ for all $k \in \mathbb{N}$.

**Lemma 3.6.10 [diru]** Let $R$ be a ring, $f, g \in R[x]$ and $c \in R$. Then

(a) $(cf)' = cf'$

(b) $(f + g)' = f' + g'$.

(c) $(fg)' = f'g + fg'$.

(d) If $ff' = f'f$, $(f^n)' = nf^{n-1}f'$.

**Proof:** (a) and (b) are obvious.

(c) By (b) we may assume that $f = rx^m$ and $g = sx^n$ are monomials. We compute

$$(fg)' = (rsx^{n+m})' = (n + m)rsx^{n+m-1}$$

$$f'g + fg' = mrx^{m-1}sx^n + rx^m nsx^{n-1} = (n + m)rsx^{m+n-1}$$

Thus (c) holds.

(d) follows from (c) and induction on $n$. \qed

**Lemma 3.6.11 [mroots]** Let $R$ be a ring with identity, $f \in R[x]$ and $c \in R$ a root of $f$.

(a) Suppose that $f = g(x - c)^n$ for some $n \in \mathbb{N}$ and $g \in R[x]$. Then

$$f^{[n]}(c) = n! g(c).$$

(b) $c$ is a multiple root of $f$ if and only if $f'(c) = 0$.

(c) Suppose that $(\deg f)!$ is neither zero nor a zero divisor in $R$. Then the multiplicity of the root $c$ is smallest number $m \in \mathbb{N}$ with $f^{[m]}(c) \neq 0$.

**Proof:** (a) We will show that for all $0 \leq i \leq n$, there exists $h_i \in R[x]$ with

$$f^{[i]} = \frac{n!}{(n-i)!} g(x - c)^{n-i} + h_i(x - c)^{n-i+1}$$

For $i = 0$ this is true with $h_0 = 0$. So suppose its true for $i$. Then using 3.6.10
f^{[i+1]} = (f^i)' = \frac{n!}{(n-i)!} (g'(x-c)^{n-i}+g(n-i)(x-c)^{n-1-i})+h'_i(x-c)^{n-i+1}+h_i(n-i+1)x^{n-i}

This is of the form \( \frac{n!}{(n-i-1)!} g(x-c)^{n-i-1} \) plus a left multiple of \((x-c)^{n-i}\). So the statements holds for \( i+1 \).

For \( i = n \) we conclude \( f^{[n]} = n!g + h_n(x-a) \) Thus (a) holds.

(b) Since \( c \) is a root, \( f = g(x-a) \) for some \( g \in R[x] \). So by (a) applied to \( n = 1 \), \( f'(c) = g(c) \). Thus (b) holds.

(c) Let \( m \) the multiplicity of \( c \) has a root of \( f \). So \( f = g(x-c)_m \) for some \( g \in R[x] \) with \( g(c) \neq 0 \). Let \( n < m \). Then \( f = (g(x-c)^{m-n})(x-c)^n \) and (a) implies \( f^{[n]}(c) = 0 \). Suppose that \( f^{[m]}(c) = 0 \). Then by (a), \( m!g(c) = 0 \). As \( m \leq \deg f \) we get \( (\deg f)!g(c) = 0 \). Thus by assumption \( g(c) = 0 \), a contradiction. This \( f^{[m]}(c) \neq 0 \) and (c) holds.

Consider the polynomial \( x^p \) in \( \mathbb{Z}/p\mathbb{Z}[x] \). Then \( (x^p)' = px^{p-1} = 0 \). This shows that the condition on \((\deg f)! \) in part (c) of the previous theorem is necessary.

Let \( D \) be an UFD, \( I \) a set and \( f \in D[I] \). We say that \( f \) is primitive if 1 is a greatest common divisor of the coefficients of \( f \).

**Lemma 3.6.12 (cont)** Let \( D \) be a UFD, \( \mathbb{F} \) its field of fractions and \( I \) a set. Let \( f \in \mathbb{F}[I] \). Then there exists \( a_f, b_f \in D \) and \( f^* \in D[I] \) so that

(a) \( f^* \) is primitive in \( D[I] \).

(b) \( a_f \) and \( b_f \) are relatively prime.

(c) \( f = \frac{a_f}{b_f} f^* \).

Moreover \( a_f, b_f \) and \( f^* \) are unique up to associates in \( D \).

**Proof:** We will first show the existence. Let \( f = \sum_{\alpha \in I} f_\alpha x^\alpha \) with \( f_\alpha \in \mathbb{F} \). Then \( f_\alpha = \frac{r_\alpha}{s_\alpha} \) with \( r_\alpha, s_\alpha \in D \). Here we choose \( s_\alpha = 1 \) if \( f_\alpha = 0 \). Let \( s = \prod_{\alpha \in I} s_\alpha \). Then \( sf \in D[I] \). Let \( r = \gcd_{\alpha \in I} s_\alpha \) and \( f^* = r^{-1}sf \). Then \( f^* \in D[I], f^* \) is primitive and \( f = \frac{r}{s}f^* \). Let \( e \) the a greatest common divisor of \( r \) and \( s \) and put \( a_f = \frac{r}{e} \) and \( b_f = \frac{s}{e} \). Then (a),(b) and (c) hold.

To show uniqueness suppose that \( f = \frac{a}{b}f \) with \( a, b \in D \) relative prime and \( f \in D[I] \) primitive. Then

\[ ba^*_f = bfa \]

Taking the greatest common divisor of the coefficients on each side of this equation we see that \( ba_f \) and \( bfa \) are associate in \( D \). In particular, \( a \) divides \( ba_f \) and as \( b \) is relatively prime to \( a, a \) divides \( a_f \). By symmetry \( a_f \) divides \( a \) and so \( a = ua_f \) for some unit \( u \) in \( D \). Similarly \( b = vb_f \) for some unit \( v \in D \). Thus \( vb_fa_f f^* = ub_fa_f f^* \). As \( D \) is an integral domain we conclude \( f = u^{-1}vf^* \). \( \square \)

Let \( f \) be as in the previous theorem. The fraction \( c_f = \frac{a_f}{b_f} \) is called the content of \( f \). Note that \( c_f \in \mathbb{F} \) and \( f = c_ff^* \).
Lemma 3.6.13 [cont] Let $D$ be a UFD, $\mathbb{F}$ its field of fraction, $I$ a set and $f, g \in \mathbb{F}[I]$.  
(a) $c_f g = uc_f c_g$ for some unit $u \in D$.  
(b) $(fg)^* = u^{-1}f^* g^*$  
(c) The product of primitive polynomials is primitive.  
(d) If $f \mid g$ in $\mathbb{F}[I]$, then $f^* \mid g^*$ in $D[I]$.  
(e) Suppose $f$ is primitive. Then $f$ is irreducible in $D[I]$ if and only if its irreducible in $\mathbb{F}[I]$.  
(f) Suppose $f$ is primitive. Then $f$ is a prime in $D[I]$ if and only if it is a prime in $\mathbb{F}[I]$.  

Proof: Note that $fg = c_f c_g f^* g^*$. So (a), (b) and (c) will follow once the show that the product of two primitive polynomials is primitive. Suppose not. Then there exist primitive $f, g \in D[I]$ and a prime $p$ in $D$ dividing all the coefficients of $fg$. But then $p \mid fg$ in $D[I]$. By 3.6.3 $p$ is prime in $D[I]$ and so $p$ divides $f$ or $g$ in $D[I]$. A contradiction as $f$ and $g$ are primitive.  
(d) Suppose that $f \mid g$. Then $g = fh$ for some $h \in \mathbb{F}[I]$. By (b) $g^* = f^* h^*$ and so (d) holds.  
(e) Suppose that $f$ is irreducible in $\mathbb{F}[I]$ and $f = gh$ with $g, h \in D[x]$ Then by (a) both $g$ and $h$ are primitive. On the other hand since $f$ is irreducible in $\mathbb{F}[I]$, one of $g$ or $h$ is a unit in $F[I]$ and so in $\mathbb{F}$. It follows that one of $g$ and $h$ is a unit in $D$. So $f$ is also irreducible in $D[I]$.  
Suppose that $f$ is irreducible in $D[I]$ and $f = gh$ for some $g, h \in D[x]$. Then $f = f^* \sim g^* h^*$ and as $f$ is irreducible in $D[I]$, one of $g^*, h^*$ is a unit in $D$. But then one of $g$ and $h$ is in $\mathbb{F}$ and so a unit in $\mathbb{F}[I]$.  
(f) Suppose that $f$ is prime in $D[I]$ and that $f \mid gh$ in $\mathbb{F}[I]$. By (d) $f = f^* \mid g^* h^*$ and as $f$ is a prime in $D[I]$ we may assume $f \mid g^*$. As $g^*$ divides $g$ in $F[I]$ $f$ does too. So $f$ is a prime in $F[I]$.  
Suppose that $f$ is a prime in $F[I]$ and $f \mid gh$ in $D[I]$ for some $g, h \in D[I]$. Then as $f$ is a prime in $F[I]$ we may assume $f \mid g$ in $F[I]$. But (d) $f = f^* \mid g^*$ in $D[I]$. As $g^*$ divides $g$ in $D[I]$, $f$ does too. So $f$ is a prime in $D[I]$.  

\[ \square \]

Theorem 3.6.14 [DXUFD] Let $D$ be a UFD and $I$ a set, then $D[I]$ is a UFD.  

Proof:  
Let $f$ be in $D[I]$. We need to show that $f$ is the product of primes. Now $f \in D[J]$ for some finite $f$ and by 3.6.3 a prime factorization in $D[J]$ is a prime factorization in $D[I]$. So we may assume that $J$ is finite and then by induction that $|I| = 1$.  
Note that $f = c_f f^*$ with $f^* \in D[x]$ primitive and $c_f \in D$. As $D$ is a UFD, $c_f$ is a product of primes in $D$ and by 3.6.3 also a product of primes in $D[x]$. So we may assume...
that $f$ is primitive. Suppose that $f = gh$ with $g, h \in D[x]$ with neither $g$ nor $h$ a unit. As $f$ is primitive, $g$ and $h$ both have positive degree smaller than $f$. So by induction on $\deg f$ both $g$ and $h$ are a product of primes. So we may assume that $f$ is irreducible. Let $\mathbb{F} = \mathbb{F}_D$. By 3.6.13 $f$ is irreducible in $\mathbb{F}[x]$. As $\mathbb{F}[x]$ is Euclidean, $f$ is a prime in $\mathbb{F}[x]$. Hence by 3.6.13 $f$ is a prime in $D[x]$. \hfill \Box
Chapter 4

Modules

4.1 Modules and Homomorphism

In this section we introduce modules over a ring. It corresponds to the concept of group action in the theory of groups.

Definition 4.1.1 Let $R$ be a ring. A (left) $R$-modules is an abelian group $M$ together with a function

$$ R \times M \to M, \quad (r, m) \to rm $$

such that for all $r, s \in R$ and $a, b \in M$:

(Ma) $r(a + b) = ra + rb$.  
(Mb) $(r + s)a = ra + sa$.  
(Mc) $r(sa) = (rs)a$.

Given a ring $R$ and an abelian group $M$. $M$ is an $R$-modules if and only if there exists a ring homomorphism $\Phi : R \to \text{End}(M)$.

Indeed if $M$ is an $R$-modules define $\Phi : R \to \text{End}(M)$ by

$$ \Phi(r)(m) = rm $$

By (Ma), $\Phi(r)$ is indeed an homomorphism. And (Mb) and (Mc) imply that $\Phi$ is a ring homomorphism.

Conversely, given a ring homomorphism $\Phi : R \to \text{End}(M)$, define $rm = \Phi(r)m$. Then $M$ is a $R$-module.

Analogue to a module we can define a right $R$-module via a function $M \times R \to R$ fulfilling the appropriate conditions. It is then easy to verify that a right modules for $R$ is nothing else as a left modules for $R^{\text{op}}$. In particular, for commutative ring left and right modules are the same.

Every abelian group $M$ is a $\mathbb{Z}$-module via $(n, m) \to nm$. Indeed this is the only way $M$ becomes a $\mathbb{Z}$ module under the additional assumption that $1m = m$.  

93
Definition 4.1.2 Let \( R \) be a ring with identity and \( M \) a \( R \)-modules.

(a) \( M \) is a unitary \( R \)-module provide that

\[ 1m = m \]

for all \( m \in M \).

(b) If \( R \) is a division ring and \( M \) is unitary then \( M \) is called a vector space over \( R \).

Examples:
If \( M \) is an abelian group then \( M \) is a module for \( \text{End}(M) \) via \( \phi m = \phi(m) \).

If \( R \) is a ring and \( I \) is an left ideal then \( I \) and \( R/I \) are \( R \)-modules by left multiplication.

If \( S \) is a subring of \( R \) then \( R \) is an \( S \)-module via left multiplication.

Direct sums and direct products of \( R \)-modules are \( R \) modules. In particular, if \( \Omega \) is a set, then \( R^\Omega \) is a \( R \)-module via \( (rf)(\omega) = rf(\omega) \). Or \( r(s\omega) = (rs)\omega \).

Let \( R \) is a ring and \( G \) a semigroup. Suppose that \( G \) act on a set \( \Omega \). Then \( R^\omega \) is an \( R[G] \) modules. To see this we first define an action of \( G \) on \( R^\Omega \) by

\[ (gf)(\omega) = f(g^{-1}\omega) \]

Then extend this to \( R[G] \) by

\[ (\sum_{g \in G} r_g g) f = \sum_{g \in G} r_g g f \]

Definition 4.1.3 Let \( V \) and \( W \) be \( R \)-modules. An \( R \)-module homomorphism from \( V \) to \( W \) is a function:

\[ f : V \to W \]

such that

\[ f(a + c) = f(a) + f(c) \text{ and } f(ra) = rf(a) \]

for all \( a, c \in R, r \in R \).

We often will say that \( f : V \to W \) is \( R \)-linear instead of \( f : V \to W \) is a \( R \)-modules homomorphism. Terms like \( R \)-module monomorphism, \( R \)-module isomorphism, \( \text{ker} f \) and so on are defined in the usual way. If \( V \) and \( W \) are \( R \)-modules, \( \text{Hom}(V, W) \) denotes the set of \( R \)-linear maps from \( V \) to \( W \). Since sums of \( R \)-linear maps are \( R \)-linear, \( \text{End}(V, W) \) is an abelian group. \( \text{End}(V) \) denotes set of \( R \)-linear endomorphisms of \( V \). Since compositions of \( R \)-linear maps are \( R \)-linear, \( \text{End}(V) \) is a ring. Note that \( V \) is also a module for \( \text{End}(V) \) via \( \phi v = \phi(v) \).

Definition 4.1.4 Let \( R \) be a ring and \( M \) a \( R \)-module. An \( R \)-submodule \( A \) of \( M \) is an additive subgroup \( A \) of \( M \) such that \( ra \in A \) for all \( r \in R, a \in A \).
4.1. MODULES AND HOMOMORPHISM

Note that submodules of modules are modules. If the modules is unitary so is the submodule. If $V$ is a submodules of $M$, then $M/V$ is a $R$-module by

$$r(m + V) = rm + V$$

It is easy to verify that this gives a well-defined module structure. Also the map

$$M \rightarrow M/V, m \rightarrow m + V$$

is $R$-linear, is onto and has kernel $V$.

If $f : V \rightarrow W$ is $R$-linear, then $\ker f$ is a submodule of $V$ and $f(V)$ is a submodules of $W$.

**Theorem 4.1.5 (Isomorphism Theorem for Modules) [IMT]** Let $R$ be a ring and $f : V \rightarrow W$ and $R$-linear map. Then

$$\bar{f} : V/W \rightarrow f(W), v + W \rightarrow f(v)$$

is a well-defined $R$-linear isomorphism.

**Proof:** By the isomorphism theorem for groups 2.5.5, this is a well defined isomorphism of (additive) groups. We just need to check that it is $R$-linear. So let $r$ and $v \in V$. Then

$$\bar{f}(r(v + W)) = \bar{f}(rv + W) = f(rv) = rf(v) = r\bar{f}(v + W)$$

Let $M$ an $R$-module and $S \subseteq R$ and $X \subset M$.

$$SX = \langle sx \mid s \in S, x \in X \rangle$$

that is the additive subgroup of $M$ generated by the $sx, s \in S, x \in X$. Note that for all $X \subseteq M$, $RM$ is a submodule of $M$.

Let $T \subseteq R$. Recall that $ST = \langle st \mid s \in S, t \in T \rangle$. Note that this agrees with the above definition of $SX$, when we view $T$ is a subset of the $R$-module $R$. It is easy to verify that

$$(ST)X = S(TX) = \langle stx \mid s \in S, t \in T, x \in X \rangle$$

Here we wrote $stx$ for $(st)x = s(tx)$.

Define the submodule $(X)$ of $M$ generated by $R$ as the intersection of all the $R$-submodules of $M$ containing $X$. Note $(X) = M + RM$ and if $M$ is unitary $(X) = RM$.

For $X \subset M$ define the **annihilator of $R$ in $X$** as

$$\text{Ann}_R(X) = \{ r \in R \mid rX = \{0\} \}$$

For $S \subseteq R$ define

$$\text{Ann}_M(S) = \{ m \in M \mid Sm = \{0\} \}$$
Lemma 4.1.6 [bann] Let $R$ be ring, $M$ a $R$-module and $X \subseteq M$. Then

(a) $\text{Ann}_R(X)$ is a left ideal in $R$.

(b) Let $I$ be a right ideal in $R$. Then $\text{Ann}_M(I)$ is $R$-submodule in $M$.

(c) Suppose that one of the following holds:

1. $R$ is commutative.
2. All left ideals in $R$ are also right ideals.
3. $\text{Ann}_R(X)$ is a right ideal.

Then $\text{Ann}_R(X) = \text{Ann}_R((X))$.

(d) Let $m \in M$. Then the map

$$R/\text{Ann}_R(m) \to Rm, r \to rm$$

is a well defined $R$-isomorphism.

(a) Let $r, s \in \text{Ann}_R(X)$, $t \in R$ and $x \in X$. Then

$$(r + s)x = rx + sx = 0 \text{ and } (ts)x = t(sx) = 0$$

So $\text{Ann}_R(X)$ is a left ideal in $R$.

(b) $I(R\text{Ann}_M(I)) = (IR) \text{Ann}_M(I) \subseteq I\text{Ann}_M(I) = \{0\}$.

Thus $R\text{Ann}_M(I) \leq \text{Ann}_M(I)$ and (b) holds.

(c) Note that 1. implies 2. and by (a) 2. implies 3. So in any case $\text{Ann}_R(X)$ is a right ideal in $R$. Hence by (b)

$$W := \text{Ann}_M(\text{Ann}_R(X))$$

is an $R$-submodule. Since $X \subseteq W$ we get $(X) \leq W$. Thus $\text{Ann}_R(X)$ annihilates $(X)$. So

$$\text{Ann}_R(X) \leq \text{Ann}_R((X)).$$

The other inclusion is obvious.

(d) Consider the map

$$f : R \to M, \quad r \to rm.$$  

Clearly $f$ is $\mathbb{Z}$-linear. Also for $r, s \in R$

$$f(rs) = (rs)m = r(sm) = rf(s)$$

So $f$ is $R$-linear. Since $\text{Ann}_R(m) = \ker f$, (d) follows from the isomorphism theorem. \qed

**Example** Let $\mathbb{K}$ be a field. Let $R = M_{\mathbb{K}}(n)$ be the ring of $n \times n$ matrices over $\mathbb{K}$. Then $\mathbb{K}^n$ is a module for $R$ via $(m_{ij}(k_i) = (\sum_{j=1}^n m_{ij}k_j)$. Let $e_1 = (e_{1i}) \in K^n$ be defined
by $e_{11} = 1$ and $e_{1i} = 0$ for all $2 \leq i \leq n$. Then $\text{Ann}_R(e_1)$ consists of all matrices whose first column is zero. Note that $(e_1) = Re_1 = K^n$, indeed if $k \in K^n$ and $M$ is any matrix with $k$ as it first column, then $Me_1 = k$ and so $k \in Re_1$. Hence $\text{Ann}_R((e_1)) = 0$ and $\text{Ann}_R(e_1) \neq \text{Ann}_R((e_1))$. So the conclusion in part (c) of the previous lemma does not hold in general.

4.2 Exact Sequences

**Definition 4.2.1** [dexact] A (finite or infinite) sequence of $R$-linear maps

$$\cdots \xrightarrow{f_{i-2}} A_{i-2} \xrightarrow{f_{i-1}} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots$$

is called exact if for all suitable $j \in \mathbb{Z}$

$$\text{Im } f_j = \ker f_{j+1}$$

We denote the zero $R$-module with 0. Then for all $R$-modules $M$ there exists unique $R$-linear maps, $0 \to M$ and $M \to 0$.

The sequence

$$0 \to A \xrightarrow{f} B$$

is and only if $f$ is one to one.

$$A \xrightarrow{f} B \to 0$$

is exact if and only if $f$ is onto.

$$0 \to A \xrightarrow{f} B \to 0$$

is exact if and only if $f$ is an isomorphism.

A sequence of the form

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is called a short sequence. If it is exact we have that $f$ is one to one, $\ker g = \text{Im } f$ and $g$ is onto. Since $f$ is one to one we have $\text{Im } f \cong A$ and so $\ker g \cong A$. Since $g$ is onto the isomorphisms theorem says $B/\ker g \cong C$. So the short exact sequence tells us that $B$ has a submodule which isomorphic to $A$ and whose quotient is isomorphic to $C$.

Given two exact sequences

$$A : f_{i-1} \xrightarrow{f_i} A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1} \xrightarrow{f_{i+2}} \cdots$$

and $B : g_{i-1} \xrightarrow{g_i} B_{i-1} \xrightarrow{g_i} B_i \xrightarrow{g_{i+1}} B_{i+1} \xrightarrow{g_{i+2}} \cdots$

A homomorphism of exact sequences $\varphi : A \to B$ is a tuple of $R$-linear maps $(h_i : A_i \to B_i)$ so that the diagram

$$\begin{array}{ccccccc}
A_{i-1} & \xrightarrow{f_{i-1}} & A_{i-1} & \xrightarrow{f_i} & A_i & \xrightarrow{f_{i+1}} & A_{i+1} & \xrightarrow{f_{i+2}} \\
\downarrow h_{i-1} & & \downarrow h_i & & \downarrow h_{i+1} & & \\
B_{i-1} & \xrightarrow{g_{i-1}} & B_i & \xrightarrow{g_i} & B_i & \xrightarrow{f_{i+1}} & B_{i+1} & \xrightarrow{g_{i+2}}
\end{array}$$
commutes. \( \text{id}_A : A \to A \) is defined as \( \text{id}_A \). \( \varphi \) is called as isomorphism if there exists \( \vartheta : B \to A \) with \( \vartheta \varphi = \text{id}_A \) and \( \varphi \vartheta = \text{id}_B \). It is an easy exercise to show that \( \varphi \) is an isomorphism and if and only if each \( h_i \) is.

**Theorem 4.2.2 (Short Five Lemma) [five]** Given a homomorphism of short exact sequences:

\[
\begin{array}{cccccc}
0 & \longrightarrow & A & \overset{f}{\longrightarrow} & B & \overset{g}{\longrightarrow} & C & \longrightarrow & 0 \\
& & \downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} & & \\
0 & \longrightarrow & A' & \overset{f'}{\longrightarrow} & B' & \overset{g'}{\longrightarrow} & C' & \longrightarrow & 0
\end{array}
\]

Then

(a) If \( \alpha \) and \( \gamma \) are one to one, so is \( \beta \).

(b) If \( \alpha \) and \( \gamma \) are onto, so is \( \beta \).

(c) If \( \alpha \) and \( \gamma \) are isomorphisms, so is \( \beta \).

**Proof:** (a) Let \( b \in B \) with \( \beta(b) = 0 \). Then also \( g'(\beta(b)) = 0 \) and as the diagram commutes \( \gamma(g(b)) = 0 \). As \( \gamma \) is one to one \( g(b) = 0 \). As \( \ker g = \text{Im} f \), \( b = f(a) \) for some \( a \in A \). Thus \( \beta(f(a)) = 0 \) and so \( f'(\alpha(a)) = 0 \). As \( f' \) is one to one, \( \alpha(a) = 0 \). As \( \alpha \) is one to one, \( a = 0 \). So \( b = f(a) = 0 \) and \( \beta \) is one to one.

(b) Let \( b' \in B' \). As \( \gamma \) and \( g \) are onto, so is \( \gamma \circ g \). So there exists \( b \in B \) with \( g'(b') = \gamma(g(b)) \). As the diagram commutes \( \gamma(g(b)) = g'(\beta(b)) \). Thus \( d := b' - \beta(b) \in \ker g' \). As \( \ker g' = \text{Im} f' \) and \( \alpha \) is onto, \( \ker g' = \text{Im}(f' \circ \alpha) \). So \( d = f'(\alpha(a)) \) for some \( a \in A \). As the diagram commutes, \( d = \beta(f(a)) \). So

\[
b' - \beta(b) = d = \beta(f(a))
\]

Hence \( b' = \beta(b + f(a)) \) and \( \beta \) is onto.

(c) follows directly from (a) and (b).

**Theorem 4.2.3 [split]** Given a short exact sequence \( 0 \to A \overset{f}{\longrightarrow} B \overset{g}{\longrightarrow} C \to 0 \). Then the following three statements are equivalent:

(a) There exists a \( R \)-linear map \( \gamma : C \to B \) with \( g \circ \gamma = \text{id}_C \).

(b) There exists a \( R \)-linear map \( \eta : B \to A \) with \( \eta \circ f = \text{id}_A \).

(c) There exists \( \tau : B \to A \oplus C \) so that

\[
\begin{array}{cccccc}
0 & \longrightarrow & A & \overset{f}{\longrightarrow} & B & \overset{g}{\longrightarrow} & C & \longrightarrow & 0 \\
& & & \downarrow{\tau} & & & & \\
0 & \longrightarrow & A & \overset{\rho_1}{\longrightarrow} & A \oplus C & \overset{\pi_2}{\longrightarrow} & C & \longrightarrow & 0
\end{array}
\]

is an isomorphism of short exact sequences.
4.2. EXACT SEQUENCES

Proof: (a) ⇒ (c) Consider

\[
\begin{array}{c}
0 \longrightarrow A \overset{\rho_1}{\longrightarrow} A \oplus C \overset{\pi_2}{\longrightarrow} C \longrightarrow 0 \\
\end{array}
\]

Here \((f, \gamma) : A \oplus C \rightarrow B, (a, c) \rightarrow f(a) + \gamma(c)\). It is readily verified that this is a homomorphism. The Short Five Lemma 4.2.2 implies that is an isomorphism.

(b) ⇒ (c) This time consider

\[
\begin{array}{c}
0 \longrightarrow A \overset{f}{\longrightarrow} B \overset{g}{\longrightarrow} C \longrightarrow 0 \\
\end{array}
\]

(c) ⇒ (a) & (b) Define \(\eta = \pi_1 \circ \tau\) and \(\gamma = \tau^{-1} \rho_2\). Then

\[
\eta \circ f = \pi_1 \circ (\tau \circ f) = \pi_1 \circ \rho_1 = \text{id}_A
\]

and

\[
g \circ \gamma = (g \circ \tau^{-1}) \circ \rho_2 = \pi_1 \circ \rho_2 = \text{id}_C
\]

An exact sequence which fulfills the three equivalent conditions in the previous theorem is called split.

To make the last two theorems a little more transparent we will restate them in an alternative way. First note that any short exact sequence can be viewed as pair of \(R\) modules \(D \leq M\). Indeed, given \(D \leq M\) we obtain a short exact sequence

\[
\begin{array}{c}
0 \longrightarrow D \longrightarrow M \longrightarrow M/D \longrightarrow 0 \\
\end{array}
\]

Here \(D \rightarrow M\) is the inclusion map and \(M \rightarrow M/D\) is the canonical epimorphism. Conversely, every short exact sequence is isomorphic to one of this kind:

\[
\begin{array}{c}
0 \longrightarrow A \overset{f}{\longrightarrow} B \overset{g}{\longrightarrow} C \longrightarrow 0 \\
\end{array}
\]

Secondly define a homomorphism \(\Phi : (A \leq B) \rightarrow (A' \leq B')\) to be a homomorphism \(\Phi : B \rightarrow B'\) with \(\Phi(A) \leq A'\)

Such a \(\Phi\) corresponds to the following homomorphism of short exact sequences:
Here $\Phi_A : A \to A' : a \to \Phi(a)$ and $\Phi_{B/A} : B/A \to B'/A' : b + A \to \Phi(b) + A'$. Since $\Phi(A) \leq A'$ both of these maps are well defined.

Let's translate the Five Lemma into this language:

**Lemma 4.2.4** \textbf{[five”]} Let $\Phi : (A \leq B) \to (A' \leq B')$ be a homomorphism.

(a) If $\Phi_A$ and $\Phi_{B/A}$ are one to one, so is $\Phi$.

(b) If $\Phi_A$ and $\Phi_{B/A}$ are onto so is $\Phi$.

(c) If $\Phi_A$ and $\Phi_{B/A}$ are isomorphism, so is $\Phi$.

**Proof:** This follows from the five lemma, but we provide a second proof:

(a) As $\ker \Phi_{B/A} = 0$, $\ker \Phi \leq A$. So $\ker \Phi = \ker \Phi_A = 0$.

(b) As $\Phi_{B/A}$ is onto, $B' = \Phi(B) + A'$. As $\Phi(A) = A'$ we conclude $B' = \Phi(B)$.

(c) Follows from (a) and (b).

The three conditions on split exact sequences translate into:

**Lemma 4.2.5** \textbf{[split”]} Given a pair of $R$-modules $A \leq B$. The following three conditions are equivalent.

(a) There exists a homomorphism $\gamma : B/A \to B$ with $\bar{b} = \gamma(\bar{b}) + A$ for all $\bar{b} \in B$.

(b) There exists a homomorphism $\eta : B \to A$ with $\eta(a) = a$ for all $a \in A$.

(c) There exists a $R$-submodule $K$ of $B$ with $B = A \oplus K$.

**Proof:** Again this follows from 4.2.3 but we give a second proof:

(a)$\Rightarrow$(c): Put $K = \gamma(B/A)$. Then clearly $K + A = B$. Also if $\gamma(b + A) \in A$ we get $b + A = A = 0_{B/A}$. Thus $\gamma(b + A) = 0$ and $K \cap A = 0$.

(b)$\Rightarrow$(c): Put $K = \ker \eta$. The clearly $K \cap A = 0$. Also if $b \in B$. Then $\eta(b) \in A$ and $\eta(b - \eta(b)) = \eta(b) - \eta(b) = 0$. Thus $b = \eta(b) + (b - \eta(b)) \in A + B$. Thus $B = A + K$.

(c)$\Rightarrow$(a): Define $\gamma(k + A) = k$ for all $k \in K$.

(c)$\Rightarrow$(b): Define $\eta(a + k) = a$ for all $a \in A, k \in K$.

Finally if $A$ is a $R$-submodule of $B$ we say that $B$ splits over $A$ if the equivalent conditions in the previous lemma hold.
4.3 Projective and injective modules

In this section all rings are assumed to have an identity and all \( R \)-modules are assumed to be unitary.

We write \( \phi : A \to B \) if \( \phi : A \to B \) is onto. And \( \phi : A \to B \) if \( \phi \) is one to one.

**Definition 4.3.1** Let \( P \) be a module over the ring \( R \). We say that \( P \) is projective provided that

\[
\begin{array}{ccc}
    P & \to & A \\
    \downarrow \beta & & \downarrow \alpha \\
    B & \leftarrow & A
\end{array}
\Rightarrow
\begin{array}{ccc}
    P & \to & A \\
    \downarrow \beta & & \downarrow \alpha \\
    B & \leftarrow & A
\end{array}
\]

where both diagrams are commutative.

Let \( I \) be a set and \( R \) a ring. Then the free module \( F_R(I) \) on \( I \) over is the module \( \bigoplus_{i \in I} R \). We will usually write \( F(I) \) for \( F_R(I) \). We identify \( i \) with \( \rho_i(1) \). Hence \( F_R(I) = \bigoplus_{i \in I} Ri \).

**Lemma 4.3.2** \([\text{universal free}]\) Let \( M \) be an \( R \)-module and \(( m_i, i \in I)\) a family of elements in \( M \). Then there exists a unique homomorphism

\[
\alpha : F_R(I) \to M \text{ with } i \to m_i.
\]

\(\alpha\) is given by \( \alpha(\sum_{i \in I} r_i i) = \sum_{i \in I} r_i m_i \).

**Proof:** Obvious.

**Lemma 4.3.3** \([\text{free proj}]\) Any free module is projective.

**Proof:** Given \( \alpha : A \to B \) and \( \beta : F_R(I) \to B \). Let \( i \in I \). Since \( \alpha \) is onto, \( \beta(i) = \alpha(a_i) \) for some \( a_i \in A \). By 4.3.2 there exists \( \gamma : F_R(I) \to A \) with \( \gamma(i) = a_i \). Then

\[
\alpha(\gamma(i)) = \alpha(a_i) = \beta(i).
\]

So by the uniqueness assertion in 4.3.2, \( \alpha \circ \gamma = \beta \).

Let \( A \) and \( B \) be \( R \)-modules. We say that \( A \) is a *direct summand* of \( B \) if \( A \leq B \) and \( B = A \oplus C \) for some \( C \leq B \).

Note that if \( A \) is a direct summand of \( B \) and \( B \) is direct summand of \( C \) then \( A \) is a direct summand of \( C \). Also if \( A_i \) is a direct summand of \( B_i \), then \( \bigoplus_{i \in I} A_i \) is a direct summand of \( \bigoplus_{i \in I} B_i \).

**Lemma 4.3.4** \([\text{dsum proj}]\) Any direct summand of a projective module is projective.
Proof:
Let $P$ be projective and $P = P_1 \oplus P_2$ for some submodules $P_i$ of $P$. We need to show that $P_i$ is projective. Given $\alpha : A \to B$ and $\beta : P_1 \to B$. Since $P$ is projective there exists $\tilde{\gamma} : P \to A$ with

$$\alpha \circ \tilde{\gamma} = \beta \circ \pi_1$$

Put $\gamma = \tilde{\gamma} \rho_1$. Then

$$\alpha \circ \gamma = \alpha \circ \tilde{\gamma} \circ \rho_1 = \beta \circ \pi_1 \circ \rho_1 = \beta$$

\[\square\]

**Theorem 4.3.5 [chproj]** Let $P$ be a module over the ring $R$. Then the following are equivalent:

(a) $P$ is projective.

(b) Every short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ splits.

(c) $P$ is (isomorphic to) a direct summand of a free module.

Proof: (a) $\Rightarrow$ (b): Since $P$ is projective we have

$$\begin{array}{ccc}
P & \xrightarrow{\gamma} & B \\
\downarrow{id_P} & & \downarrow{g} \\
P & \xrightarrow{\beta} & B
\end{array}$$

So the exact sequence is split by 4.2.3a.

(b) $\Rightarrow$ (c): Note that $P$ is the quotient of some free module $F$. But then by (b) and 4.2.3c, $P$ is isomorphic to a direct summand of $F$.

(c) $\Rightarrow$ (a): Follows from 4.3.3 and 4.3.4

\[\square\]

**Corollary 4.3.6** Direct sums of projective modules are projective.

Proof: Follows from 4.3.5c.

Next we will dualize the concept of projective modules.

**Definition 4.3.7** A module $J$ for the ring $R$ is called injective if

$$\begin{array}{ccc}
J & \xrightarrow{\alpha} & A \\
\downarrow{\beta} & & \downarrow{\beta} \\
B & \xrightarrow{\gamma} & A
\end{array}$$

where both diagrams are commutative.
Above we showed that free modules are projective and so every module is the quotient of a projective module. To dualize this our first goal is to find a class of injective $R$-modules so that every $R$-modules is embedded into a member of the class. We do this into step steps: First we find injective modules for $R = \mathbb{Z}$. Then we use those to define injective modules for an arbitrary ring (with identity).

To get started we prove the following lemma, which makes it easier to verify that a given module is injective.

**Lemma 4.3.8 [ezin]** Let $J$ be a module over the ring $R$. Then $J$ is injective if and only if for all left ideals $I$ in $R$:

\[
\begin{array}{ccc}
J & \xrightarrow{\beta} & R \\
\downarrow & & \downarrow \\
I & \xrightarrow{\gamma} & I \\
\end{array}
\]

where both diagrams are commutative.

**Proof:** Given $\alpha : B \rightarrow A$ and $\beta : B \rightarrow J$, we need to find $\gamma : B \rightarrow J$ with $\beta = \gamma \alpha$. Without loss, $B \leq A$ and $\alpha$ is the inclusion map. $\beta = \gamma \alpha$ now just means $\gamma |_B = \beta$.

That is we are trying to extend $\beta$ to $A$. We will use Zorn’s lemma find a maximal extension of $\beta$. Indeed let

\[ M = \{ \delta : D \rightarrow J \mid B \leq D \leq A, \delta |_B = \beta \} \]

Order $M$ by $\delta_1 \leq \delta_2$ if $D_1 \subseteq D_2$ and $\delta_2 |_{D_1} = \delta_1$

We claim that every chain $\{ \delta_i : D_i \rightarrow J \mid i \in I \}$ in $M$ has an upper bound. Let $D = \bigcup_{i \in I} D_i$ and define $\delta : D \rightarrow J$ by $\delta(d) = \delta_i(d)$ if $d \in D_i$ for some $i \in I$. It is easy to verify that $\delta$ is well defined, $\delta \in M$ and $\delta$ is an upper bound for $\{ \delta_i : D_i \rightarrow J \mid i \in I \}$.

Hence by Zorn’s lemma, $M$ has a maximal element $\delta : D \rightarrow J$.

The reader might have noticed that we did not use our assumptions on $J$ yet. Maximal extensions always exists.

Suppose that $D \neq B$ and pick $b \in B \setminus D$.

Consider the $R$-linear map:

\[ \mu : D \oplus R \rightarrow A, \quad (d, r) \rightarrow d + rb \]

Let $I$ be the projection of $\ker \mu$ onto $D$. Then as $\ker \mu$ is a submodule of $D \oplus R$, $I$ is a submodule of $R$, that is a left ideal. Moreover, $\ker \mu = \{(-ib, i) \mid i \in I \}$ and $I$ consists of all $r \in R$ with $rb \in D$. Consider the map $\xi : I \rightarrow J, i \rightarrow \delta(ib)$. By assumption $\xi$ can be extended to a map

\[ \xi : R \rightarrow J \text{ with } \xi(i) = \delta(ib). \]
Define $\Xi : D \oplus R \to J, (d, r) \to \delta(d) + \xi(r)$. Then $\Xi$ is $R$-linear. Also $\Xi(-ib, i) = -\delta(ib) + \xi(i) = -\delta(ib) + \delta(ib) = 0$. Hence $\ker \mu \leq \ker \Xi$ and we obtain a $R$-linear map

$$\tilde{\Xi} : (D \oplus R)/\ker \mu \to J.$$ 

So by the Isomorphism Theorem we conclude that

$$D + Rb \to J, \quad d + rb \to \delta(d) + \xi(r)$$

is a well defined $R$-linear map. Clearly its contained in $\mathcal{M}$, a contradiction to the maximal choice of $\delta$.

Thus $D = B$ and $J$ is injective. The other direction of the lemma is obvious. \hfill $\square$

**Lemma 4.3.9** [hrmr] Let $R$ be a ring and $M$ an $R$-module. Then

$$\Delta : \text{Hom}_R(R, M) \to M, \phi \to \phi(1)$$

is a $\mathbb{Z}$-isomorphism.

**Proof:** Clearly $\Delta$ is $\mathbb{Z}$-linear. To show that $\Delta$ is an bijective we will find an inverse. Let $m \in M$. Define

$$\Gamma(m) : R \to M, r \to rm$$

. The claim that $\Gamma(m)$ is $R$-linear. Indeed its $\mathbb{Z}$-linear and

$$\Gamma(m)(sr) = (sr)m = s(rm)$$

for all $s, t \in R$. So $\Gamma(m) \in \text{Hom}_R(R, M)$. Also

$$\Delta(\Gamma(m)) = \Gamma(m)(1) = 1m = m$$

and for $\phi \in \text{Hom}_R(R, M)$,

$$(\Gamma(\Delta(\phi))(r) = r\Delta(\phi) = r\phi(1) = \phi(r1) = \phi(r)$$

So $\Gamma(\Delta(\phi)) = \phi$ and $\Gamma$ is the inverse of $\Delta$. \hfill $\square$

Let $R$ be an integral domain. We say that the $R$-module $M$ is **divisible** if $rM = M$ for all $r \in R^\#$. Note that every quotient of a divisible module is divisible. Also direct sums and direct summand of divisible modules are divisible.

If $R$ is divisible as an $R$-modules if and only if $R$ is a field. The field of fraction, $\mathbb{F}_R$ is divisible as an $R$-module.

**Lemma 4.3.10** [divinj] Let $R$ be an integral domain and $M$ an $R$-module.

(a) If $M$ is injective, then $M$ is divisible.
4.3. PROJECTIVE AND INJECTIVE MODULES

(b) If $R$ is a PID, $M$ is injective if and only of $M$ is divisible.

Proof: (a) Let $0 \neq t \in R$ and $m \in M$ Consider the map

$$Rt \rightarrow M, rt \rightarrow rm$$

As $I$ is an integral domain this is well defined and $R$-linear. As $M$ is injective this homomorphism can be extended to a homomorphism $\gamma : R \rightarrow M$. Then $t\gamma(1) = \gamma(t1) = \gamma(t) = m$. Thus $m \in tR$ and $R = tR$ so $M$ is divisible.

(b) Suppose that $M$ is divisible. Let $I$ be a ideal in $R$ and $\beta : I \rightarrow M$ a $R$-linear map. As $R$ is a PID, $I = Rr$ for some $t \in R$. As $M$ is divisible, $\beta(t) = tm$ for some $m \in M$. Define

$$\gamma : R \rightarrow M, r \rightarrow rm$$

Then $\gamma$ is $R$-linear and $\gamma(rt) = rtm = \beta(rt)$. We showed that the condition of 4.3.8 are fulfilled. So $M$ is injective. $\Box$

Proposition 4.3.11 [exinj] Let $R$ be a integral domain.

(a) Every $R$ module can be embedded into an divisible $R$-module.

(b) If $R$ is a PID, then every $R$-module can be embedded into a injective module.

Proof: (a) Let $M$ a $R$ module. Then

$$M \cong A/B$$

where $A = \bigoplus_{i \in I} R$for some set $I$ and $B$ is a submodule of $A$. Let $D = \bigoplus_{i \in I} \mathbb{F}_R$. Then $D$ is divisible and $B \leq A \leq D$. Also $D/B$ is divisible and $A/B$ is a submodule of $D/B$ isomorphic to $M$.

(b) follows from (a) and 4.3.10. $\Box$

An abelian group $A$ is called divisible if it is divisible as $\mathbb{Z}$-module.

Let $R$ be a ring and $A, B$ and $T$ be $R$-modules. Let $\phi : A \rightarrow B$ be $R$-linear. Then the maps

$$\phi^* : \text{Hom}_R(B,T) \rightarrow \text{Hom}_R(A,T), f \rightarrow f \circ \phi$$

and

$$\tilde{\phi} : \text{Hom}_R(A,T) \rightarrow \text{Hom}_R(B,T), f \rightarrow \phi \circ f$$

are $\mathbb{Z}$ linear. Suppose that $\psi : B \rightarrow C$ is $R$-linear. Then

$$(\psi \circ \phi) = \tilde{\phi} \circ \tilde{\psi} \text{ and } (\phi \circ \psi)^* = \psi^* \circ \phi^*.$$

Lemma 4.3.12 [exinjR] Let $R$ be a ring, $M$ a $R$-module, $D$ a right $R$-module and $A$ an abelian group.
(a) $\text{Hom}_{\mathbb{Z}}(D, A)$ is an $R$-module via $r\phi(d) = \phi(dr)$.

(b) The map

$$
\Xi = \Xi(M, A) : \text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, A)) \to \text{Hom}_{\mathbb{Z}}(M, A), \quad \Xi(\Phi)(m) = \Phi(m)(1)
$$

is an $\mathbb{Z}$-isomorphism.

(c) $\Xi(M, A)$ depends naturally on $M$ and $A$. That is

(1) Let $\beta : A \to B$ be $\mathbb{Z}$-linear. Then the following diagram is commutative:

$$
\begin{array}{ccc}
\text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, A)) & \xrightarrow{\Xi(M, A)} & \text{Hom}_{\mathbb{Z}}(M, A) \\
\downarrow \beta & & \downarrow \beta \\
\text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, B)) & \xrightarrow{\Xi(M, B)} & \text{Hom}_{\mathbb{Z}}(M, B)
\end{array}
$$

That is $\Xi(\beta \circ \Phi) = \beta \circ \Xi(\Phi)$ for all $\Phi \in \text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, A))$.

(2) Let $\eta : M \to N$ be $R$-linear. Then the following diagram is commutative:

$$
\begin{array}{ccc}
\text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, A)) & \xrightarrow{\Xi(M, A)} & \text{Hom}_{\mathbb{Z}}(M, A) \\
\uparrow \eta^* & & \uparrow \eta^* \\
\text{Hom}_R(N, \text{Hom}_{\mathbb{Z}}(R, A)) & \xrightarrow{\Xi(N, A)} & \text{Hom}_{\mathbb{Z}}(N, A)
\end{array}
$$

That is $\Xi(\Psi) \circ \eta = \Xi(\Psi \circ \eta)$ for all $\Psi \in \text{Hom}_R(N, \text{Hom}_{\mathbb{Z}}(R, A))$.

(d) If $A$ is divisible, $\text{Hom}_{\mathbb{Z}}(R, A)$ is an injective $R$-module.

**Proof:**

(a) Let $r, s \in R$, $\phi, \psi \in \text{Hom}_{\mathbb{Z}}(D, A)$ and $d, e \in D$.

$$(r\phi + s\psi)(d + e) = \phi((d + e)r) = \phi(dr + er) = \phi(dr) + \phi(er) = (r\phi)(d) + (s\psi)(e)$$

Thus $r\phi \in \text{Hom}_{\mathbb{Z}}(D, A)$.

$$
(r\phi + s\psi)(d) = \phi(d) + \psi(dr) = \phi(dr) + \psi(dr) = (r\phi + s\psi)(d)
$$

$$
((r + s)\phi)(d) = \phi((d + s)r) = \phi(dr + s\phi) = (r\phi + s\phi)(d)
$$

$$
((rs)\phi)(d) = \phi((dr)s) = (s\phi)(dr) = (r(s\phi))(d)
$$

So $\text{Hom}_{\mathbb{Z}}(D, A)$ is indeed a $R$-module.

(b) Clearly $\Xi$ is $\mathbb{Z}$-linear. Suppose that $\Xi(\Phi) = 0$. Then $\Phi(m)(1) = 0$ for all $m \in M$. Let $r \in R$. Then

$$
0 = \Phi(rm)(1) = (r\Phi(m))(1) = (\Phi(m))(1r) = \Phi(m)(r)
$$
Thus $\Phi(m)(r) = 0$ for all $r$. So $\Phi(m) = 0$ for all $m$ and so $\Phi = 0$. So $\Xi$ is on to one.

To show that $\Xi$ is onto, let $\alpha \in \text{Hom}_R(M, A)$.

Define $\Phi \in \text{Hom}_R(M, \text{Hom}_R(A, A))$ by

$$\Phi(m)(r) = \alpha(rm)$$

Clearly $\Phi(m)$ is indeed in $\text{Hom}_R(A, A)$. We need to verify that $\Phi$ is $R$-linear. Let $s \in R$. Then $(\Phi(sm))(r) = \alpha(rsm)$ and $(s\Phi(m))(r) = \Phi(m)(rs) = \alpha(rsm)$. So $\Phi(sm) = s\Phi(m)$ and $\Phi$ is $R$-linear.

Also

$$(\Xi(\Phi))(m) = (\Phi(m))(1) = \alpha(1m) = \alpha(m)$$

and so $\Xi(\Phi) = \alpha$ and $\Xi$ is onto.

(ca) $$(\tilde{\beta} \circ \Xi)(\Phi)(m) = \beta(\Xi(\Phi)(m)) = \beta(\Phi(m)(1))$$

and

$$(\Xi \circ \tilde{\beta})(\Phi)(m) = \tilde{\beta}(\Phi)(m)(1) = (\tilde{\beta}(\Phi(m))(1) = \beta(\Phi(m)(1)).$$

(cb) Let $\Psi \in \text{Hom}_R(N, \text{Hom}_R(A, A))$. Then

$$(\eta^* \circ \Xi)(\Psi)(m) = \eta^*(\Xi(\Psi))(m) = \Xi(\Psi)(\eta(m)) = \Psi(\eta(m))(1)$$

and

$$(\Xi \circ \eta^*)(\Psi)(m) = \Xi(\eta^*(\Psi))(m) = (\eta^*(\Psi(m))(1) = \Psi(\eta(m))(1).$$

(d) Let $I$ be a left ideal in $R$ and $\beta : I \to \text{Hom}_R(R, A)$. By 4.3.8 we need to show that $\beta$ extends to $\gamma : R \to \text{Hom}_R(R, A)$. Let $\Xi = \Xi(I, A)$ be given by (b). Put $\beta = \Xi(\beta)$. Then

$$\tilde{\beta} : I \to A$$

is $\mathbb{Z}$-linear. Since $A$ is divisible, it is injective as an $\mathbb{Z}$-module. So $\tilde{\beta}$ extends a $\mathbb{Z}$-linear map $\tilde{\gamma} : R \to A$. That is $\tilde{\beta} = \tilde{\gamma} \circ \rho$, where $\rho : I \to M$ is the inclusion map. By (b) there exists an $R$-linear $\gamma : M \to \text{Hom}_R(R, A)$ with $\Xi(\gamma) = \tilde{\gamma}$. By (cb)

$$\Xi(\gamma \circ \rho) = \Xi(\gamma) \circ \rho = \tilde{\gamma} \circ \rho = \tilde{\beta} = \Xi(\beta)$$

As $\Xi$ is one to one, we conclude $\beta = \gamma \circ \rho$ and so $\gamma$ is the wanted extension of $\beta$. \qed

**Theorem 4.3.13** [eminj] *Let $R$ be a ring. Every $R$-module can be embedded into an injective $R$-module.*

**Proof:** Let $M$ be a $R$-module. By 4.3.11 $M$ is a subgroup of some divisible abelian group $A$. Let $\rho : M \to A$ be the inclusion map. Then $\rho : \text{Hom}_R(R, M) \to \text{Hom}_R(R, A)$, $\phi \to \rho \circ \phi$ is a $R$-momomorphism. By 4.3.9 $M \cong \text{Hom}_R(R, M)$ and so $M$ is isomorphic to an $R$-submodule of $\text{Hom}_R(R, A)$. By 4.3.12 $\text{Hom}_R(R, A)$ is injective. \qed
Lemma 4.3.14 [prodinj]

(a) Direct summands of injective modules are injective.

(b) Direct products of injective modules are injective.

Proof: (a) Let \( J = J_1 \oplus J_2 \) with \( J \) injective. Given \( \alpha : B \twoheadrightarrow A \) and \( \beta : B \rightarrow J_1 \). As \( J \) is injective there exists \( \tilde{\gamma} : A \rightarrow J \) with

\[
\tilde{\gamma} \circ \alpha = \rho_1 \circ \beta.
\]

Put \( \gamma = \pi_1 \circ \tilde{\gamma} \). Then

\[
\gamma \circ \alpha = \pi_1 \circ \tilde{\gamma} \circ \alpha = \pi_1 \circ \rho_1 \circ \alpha = \alpha.
\]

(b) Suppose that \( J_i, i \in I \) is a family of injective modules. Given \( \alpha : B \rightarrow A \) and \( \beta : B \rightarrow \prod_{i \in I} J_i \). Since \( J_i \) is injective there exists \( \gamma_i : A \rightarrow J_i \) with

\[
\gamma_i \circ \alpha = \pi_i \circ \beta.
\]

Put \( \gamma = (\gamma_i)_{i \in I} \).

Then

\[
\pi_i \circ \gamma \circ \alpha = \gamma_i \circ \alpha = \pi_i \circ \beta
\]

and so \( \gamma \circ \alpha = \beta \). Hence \( \prod_{i \in I} J_i \) is injective. \( \square \)

Theorem 4.3.15 [chrinj] Let \( M \) be an \( R \)-module. Then the following are equivalent:

(a) \( M \) is injective.

(b) If \( A \) is a \( R \)-module with \( M \leq A \), then \( A \) splits over \( M \).

Proof: (a)\( \Rightarrow \) (b) Since \( M \) is injective we obtain

\[
\begin{array}{ccc}
M & \xrightarrow{\gamma} & A \\
\downarrow{\text{id}_M} & & \downarrow{\text{id}_{M \rightarrow A}} \\
M & & \\
\end{array}
\]

Hence by ??, \( A \) splits over \( M \).

(b)\( \Rightarrow \) (a) By 4.3.13, \( M \) is a submodule of an injective module. So by assumption, \( M \) is a direct summand of this injective module. Thus by 4.3.14 \( M \) is injective. \( \square \)
4.4 The Functor Hom

If \(A \leq B\), \(\text{id}_{A \to B}\) denotes the inclusion map \(A \to B, a \to a\).

**Lemma 4.4.1** \(\text{[homex]}\) Let \(R\) be a ring. Given a sequence \(A \xrightarrow{f} B \xrightarrow{g} C\) of \(R\)-modules. Then the following two statements are equivalent:

(a) \(A \xrightarrow{f} B \xrightarrow{g} C\) is exact and \(A\) splits over \(\ker f\).

(b) For all \(R\)-modules \(D\),

\[
\text{Hom}_R(D, A) \xrightarrow{\hat{f}} \text{Hom}_R(D, B) \xrightarrow{\hat{g}} \text{Hom}_R(D, C)
\]

is exact.

**Proof:** We first compute \(\ker \hat{g}\) and \(\text{Im } \hat{f}\). Let \(\beta \in \text{Hom}_R(D, B)\). Then \(g \circ \beta = 0\) if and only if \(\text{Im } \beta \leq \ker g\). Thus

\[
\ker \hat{g} = \text{Hom}_R(D, \ker g).
\]

Also

\[
\text{Im } \hat{f} = f \circ \text{Hom}_R(D, A) := \{f \circ \alpha \mid \alpha \in \text{Hom}_R(D, A)\} \leq \text{Hom}_R(D, \text{Im } f).
\]

Suppose first that (a) holds. Then \(\ker g = \text{Im } f\) and \(A = \ker f \oplus K\) for some \(R\)-submodule \(K\) of \(A\). It follows that \(f \mid_K: K \to \text{Im } f\) is an isomorphisms. Let \(\phi \in \text{Hom}_R(D, \text{Im } f)\). Let

\[
\alpha = \text{id}_{K \to A} \circ (f \mid_K)^{-1} \circ \phi
\]

Then \(\alpha \in \text{Hom}_R(D, A)\) and \(f \circ \alpha = \phi\). So

\[
\text{Im } \hat{f} = \text{Hom}_R(D, \text{Im } f) = \text{Hom}_R(D, \ker g) = \ker \hat{g}.
\]

Suppose next that (b) holds. Let \(D = \ker g\). Then

\[
\text{id}_{\ker g \to B} \in \ker \hat{g} = \text{Im } \hat{g} \leq \text{Hom}_R(D, \text{Im } f)
\]

thus \(\ker g \leq \text{Im } f\). Next choose \(D = A\). Then

\[
f = f \circ \text{id}_A \in \ker \hat{g} = \text{Hom}_R(D, \ker g)
\]

Hence \(\text{Im } f \leq \ker g\) and so \(0 \to A \to B \to C \to 0\) is exact.

Finally choose \(D = \text{Im } f\). Then \(\text{id}_{\text{Im } f \to B} \in \ker \hat{g}\) and so

\[
\text{id}_{\text{Im } f \to B} = f \circ \gamma
\]

for some \(\gamma \in \text{Hom}(\text{Im } f, A)\). So by 4.2.5, \(A\) splits over \(A\). \(\square\)

Here is the dual version of the previous lemma:
Lemma 4.4.2 [homex1] Let $R$ be a ring. Given a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ equivalent.

(a) 
\[ A \xrightarrow{f} B \xrightarrow{g} C \]

is exact and $C$ splits over $\text{Im} \ g$.

(b) For all $R$-modules $D$,
\[ \text{Hom}_R(A, D) \xlongleftarrow{f^*} \text{Hom}_R(B, D) \xlongleftarrow{g^*} \text{Hom}_R(C, D) \]

is exact.

Proof: Dual to the one for 4.4.1. We leave the details to the reader.

The following three theorem are immediate consequences of the previous two:

Theorem 4.4.3 [homex2] Let $R$ be ring. Then the following are equivalent

(a) 
\[ 0 \to A \xrightarrow{f} B \xrightarrow{g} C \]

is exact.

(b) For every $R$ module $D$,
\[ 0 \to \text{Hom}(D, A) \xrightarrow{f^*} \text{Hom}(D, B) \xrightarrow{g^*} \text{Hom}(D, C) \]

is exact.

\[ \square \]

Theorem 4.4.4 [homex3] Let $R$ be ring. Then the following are equivalent

(a) 
\[ A \xrightarrow{f} B \xrightarrow{g} C \to 0 \]

is exact.

(b) For every $R$ module $D$,
\[ \text{Hom}_R(A, D) \xlongleftarrow{f^*} \text{Hom}_R(B, A) \xlongleftarrow{g^*} \text{Hom}_R(C, A) \leftarrow 0 \]

is exact.

\[ \square \]

Theorem 4.4.5 [homex4] Let $R$ be a ring. Given a sequence of $R$-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to$. Then the following three statements are equivalent:
4.4. THE FUNCTOR HOM

(a) 
\[0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0\]

is split exact.

(b) For all \(R\)-modules \(D\),
\[0 \to \text{Hom}_R(D, A) \xrightarrow{\hat{f}} \text{Hom}_R(D, B) \xrightarrow{\hat{g}} \text{Hom}_R(D, C) \to 0\]

is exact.

(c) For all \(R\)-modules \(D\),
\[0 \leftarrow \text{Hom}_R(A, D) \xleftarrow{\hat{f}^*} \text{Hom}_R(B, D) \xleftarrow{\hat{g}^*} \text{Hom}_R(C, D) \leftarrow 0\]

is exact.

\[\square\]

**Theorem 4.4.6** [homdir] Let \(A\) and \(B_i, i \in I\) be \(R\)-modules. Then

(a) \(\text{Hom}_R(\bigoplus_{i \in I} B_i, A) \cong \prod_{i \in I} \text{Hom}_R(B_i, A)\)

(b) \(\text{Hom}_R(A, \prod_{i \in I} B_i) \cong \prod_{i \in I} \text{Hom}_R(A, B_i)\)

(c) \(\text{Hom}_R(A, \bigoplus_{i \in I} B_i) \cong \bigoplus_{i \in I} \text{Hom}_R(A, B_i)\)

**Proof:** Pretty obvious, the details are left to the reader. \(\square\)

Let \(R\) and \(S\) be rings. An \((R, S)\)-bimodule is abelian group \(M\) so that \(M\) is a left \(R\)-module, a right \(S\) module such that

\[(rm)s = r(ms)\]

for all \(r \in R\), \(s \in S\) and \(m \in M\).

For example \(R\) is a \((R, R)\) modules if we view \(R\) as a left \(R\)- and right \(R\)-module by multiplication from the left and right, respectively.

**Lemma 4.4.7** [bimo] Let \(R\) and \(S\) be rings. Let \(\phi : A \to A'\) be \(R\)-linear and let \(B\) a \((R, S)\)-bimodule. Then

(a) \(\text{Hom}_R(A, B)\) is a right \(S\)-module by

\[(fs)(a) = f(a)s.\]

(b) 
\(\phi^* : \text{Hom}_R(A', B) \to \text{Hom}_R(A, B), f \mapsto f \circ \phi\)

is \(S\)-linear.
(c) Hom$_R(B, A)$ is a left $S$-module with action of $S$ given by
\[(sf)(b) = f(bs)\]

(d) \[\tilde{\phi} : \text{Hom}_R(B, A) \to \text{Hom}_R(B, A'), f \to \phi f\]

is $S$ linear.

**Proof:** Straightforward.

Let $R$ be a ring and $M$ a $R$-module. The *dual* of $M$ is the module
\[M^* := \text{Hom}_R(M, R)\]

As $R$ is an $(R, R)$-bimodule, $M^*$ is a right $R$-module. The elements of $M^*$ are called *linear functionals* on $M$.

From 4.4.6 we have
\[\bigoplus_{i \in I} M_i^* \cong \prod_{i \in I} M_i^*\]

By ?? $R^* \cong R$, (but the reader should be aware that here $R$ is a right $R$-module that is the action is given by right multiplication.)

We conclude
\[F(I)^* \cong R^I\]
and so if $I$ is finite then $F(I)^*$ is isomorphism to the free right-module on $I$.

An $R$-module $M$ is called *cyclic* of $M = Rm$ for some $m \in M$.

**Lemma 4.4.8 [M*cy]** Let $R$ be a ring and $M = Rm$ a cyclic $R$ modules. Let $I = \text{Ann}_R(m)$ and $J = \{r \in R \mid Ir = 0\}$.

(a) $J$ is an right ideal in $R$.

(b) \[\tau : M^* \to J, f \to f(m)\]

is an isomorphism of right $R$-modules.

**Proof:** (a) Let $j \in J$, $r \in R$ and $i \in I$. Then $i(jr) = (ij)r = 0r = 0$ and so $jr \in J$. Thus (a) holds.

(b) Let $a \in \text{Ann}_R(m)$. Then $af(m) = f(am) = f(0) = 0$ and so $f(m) \in J$. So $\tau$ is well defined. It is clearly $\mathbb{Z}$-linear and
\[(fr)(m) = f(m)r\]

So $\tau(fr) = \tau(f)r$ and $\tau$ is right $R$-linear.
Let \( j \in J \). Then \( I_j = 0 \) and so the map \( \xi(j) : M \to R, rm \to rj \)
is well defined and \( R \)-linear.

\[
\tau(\xi(j)) = \xi(j)(m) = \xi(j)(1m) = 1j = j
\]

and

\[
(\xi(\tau(f)))(rm) = r\tau(f) = rf(m) = f(rm)
\]

and so \( \xi(\tau(f)) = f \) and \( \tau \) is a bijection.

If \( R \) is commutative, left and right modules are the same. So we might have that \( M \cong M^* \) as \( R \)-modules. In this case \( M \) is called self-dual. For example free modules of finite rang over a commutative ring are self-dual. Let \( R \) be a ring, the double dual of a module \( M \) is \( M^{**} := (M^*)^* \). Define

\[
\vartheta : M \to M^{**}, \vartheta(m)(f) = f(m).
\]

It is readily verified that \( \vartheta \) is \( R \)-linear. If \( M = F_R(I) \) is free of finite rang we see that \( \vartheta \) is an isomorphism. If \( M = F_R(I) \) is free of infinite rang, then \( \vartheta \) is a monomorphism but usually not an isomorphism.

In general \( \vartheta \) does not need to be one to one. For example if \( R = \mathbb{Z}, n \in \mathbb{Z}^+ \) and \( M = \mathbb{Z}/n\mathbb{Z} \), then it is easy to see that \( M^* = 0 \). Indeed let \( \phi \in M^* \) and \( m \in M \). Then \( nm = 0 \) and so \( n\phi(m) = \phi(nm) = 0 \). Thus \( \phi(m) = 0 \) Since \( M^* = 0 \), also \( M^{**} = 0 \).

Let us investigate \( \ker \vartheta \) in general. Let \( m \in M \) then \( \vartheta(m) = 0 \) if and only if \( \phi(m) = 0 \) for all \( \phi \in M^* \).

### 4.5 Tensor products

Let \( R \) be a commutative ring and \( A, B, C \) \( R \)-modules. A function \( f : A \times B \to C \) is called \( R \)-bilinear if for each \( a \) in \( A \) and \( b \) in \( B \) the maps

\[
f(a,*) : B \to C, y \to f(a,y) \quad \text{and} \quad f(*,b) : A \to C, x \to f(x,b)
\]

are \( R \)-linear.

For example the ring multiplication is \( R \)-linear. Also if \( M \) is any \( R \)-module. Then \( M^* \times M \to R, (f, m) \to f(m) \)

Let \( R \) be any ring, \( A \) a right and \( B \) a left \( R \)-module. Let \( C \) be any abelian group. A map \( f : A \times B \to C \) is called \( R \)-balanced, if is \( \mathbb{Z} \) bilinear and

\[
f(ar, b) = f(a, rb)
\]

for all \( a \in A, b \in B, r \in R \). \( M^* \times M \to R, (f, m) \to f(m) \) is an example of a \( R \)-balanced map.
Definition 4.5.1 \([\text{dtensor}]\) Let \(A\) be a right and \(B\) a left module for the ring \(R\). A tensor product for \((A, B)\) is an \(R\)-balanced map:

\[
\otimes : (A \times B) \to A \otimes_R B, \quad (a, b) \mapsto a \otimes b
\]

such that for all \(R\)-balanced maps \(f : A \times B \to C\) there exists a unique \(\mathbb{Z}\)-linear

\[
\tilde{f} : A \otimes B \to C \quad \text{with} \quad f(a, b) = \tilde{f}(a \otimes b).
\]

Theorem 4.5.2 \([\text{extens}]\) Let \(R\) be a ring, \(A\) be a right and \(B\) a left \(R\)-module. Then there exits a tensor product for \((A, B)\).

Proof: Let \(A \otimes_R B\) the abelian group with generators \(\{x(a, b) \mid a \in A, b \in B\}\) and relations

\[
x(a, b) + x(a', b) = x(a + a', b),\quad a, a' \in A, b \in B,
\]

\[
x(a, b) + x(a, b') = x(a, b + b'),\quad a \in A, b, b' \in B
\]

and

\[
x(ar, b) = x(a, rb),\quad a \in A, b \in B, r \in R
\]

Write \(a \otimes b\) for \(x(a, b)\) and define

\[
\otimes : A \times B \to A \otimes B, \quad (a, b) \mapsto a \otimes b
\]

. We leave it as any easy exercise to verify that this is indeed an tensor product. \(\square\)

Let \(R\) be a ring. Then \(\otimes : R \times_R R \to R, (r, s) \mapsto rs\) is a tensor product. Indeed given any \(R\)-balanced map, \(f : R \times R \to C\). Define

\[
\tilde{f} : R : R \to C, r \mapsto f(r, 1)
\]

As \(f\) is \(\mathbb{Z}\)-bilinear, \(\tilde{f}\) is \(\mathbb{Z}\)-linear. Also

\[
\tilde{f}(r \otimes s) = \tilde{f}(rs) = f(rs, 1) = f(r, s)
\]

So indeed \(\otimes\) is a tensor product. With the same argument we have:

Lemma 4.5.3 \([\text{AtenR}]\) Let \(R\) be a ring, \(A\) a right and \(B\) a left \(R\)-module. Then

\[
A \otimes_R R \cong A \quad \text{and} \quad R \otimes_R B \cong B
\]

With a little bit more work we will prove

Lemma 4.5.4 \([\text{tensy}]\) Let \(R\) be a ring, \(J\) a right ideal in \(R\) and \(I\) a left ideal in \(R\). Then

\[
\otimes : R/J \times_R R/I \to R/J + I, (r + J, s + I) \mapsto (rs + (I + J)
\]

is a tensor product for \((R/J, R/I)\).
Proof:
Note here that $I + J$ is neither a left nor a right ideal in $R$. It is just an additive subgroup, $R/I + J$ is an abelian group but in general not a ring. First we need to check that $\otimes$ is well defined:

$$(r + j)(s + i) + (I + J) = rs + (js + ri + ji) + (I + J) = rs + (I + J)$$

Note here that as $J$ is a right ideal $js + ji \in J$ and as $I$ is a left ideal $ri \in I$.

Clearly $\otimes$ is $R$-balanced. Suppose now that $f : R/J \times R/I \to C$ is $R$-balanced.

Define $\bar{f} : R/ (I + J) \to C, r + (I + J) \to f(r + J, 1 + I)$

Again we first need to verify that this is well-defined.

$$f(r + i + j, 1 + I) = f((r + J) + (i + J), 1 + I) = f(r + I, 1 + I) + f((1 + J)i, 1 + I) =$$

$$= f(r + I, 1 + I) + f(1 + J, i(1 + I)) = f(r + I, 1 + I) + f(1 + I, 0_{R/I}) = f(r + J, 1 + I)$$

So $\bar{f}$ is well defined and clearly $\mathbb{Z}$ linear.

$$\bar{f}(r + J \otimes s + I) = \bar{f}(rs + I + J) = f(rs + J, 1 + I) = f((r + J)s, 1 + I) = f(r + j, s + I)$$

and $\otimes$ is indeed a tensor product.

If $R$ is PID we conclude

$$R/Rm \otimes_R R/Rn \cong R/ \gcd(n,m)R$$

In particular, if $n$ and $m$ are relative prime $R/Rm \otimes R/Rn = 0$

Let $M$ be a finite dimensional vector space over the division ring $\mathbb{D}$. Let $x \in M, \phi \in M^*$, $R = \text{End}_D(M), I = \text{Ann}_R(x)$ and $J = \text{Ann}_R(y)$. Then $M \cong R/I$ and $M^* = R/J$. Thus $M^* \otimes_R M \cong R/(I + J)$. We leave it as an exercise to verify that $R/I + J \cong D$. We conclude that

$$M^* \times M \to D, (f, m) \to f(m)$$

is a tensor product of $(M^*, M)$.

Lemma 4.5.5 [tenbi] Let $R, S, T$ be rings, $\alpha : A \to A'$ $(R, S)$-linear and $\beta : B \to B'$ $(S, T)$-linear.

(a) $A \otimes_S B$ is an $(R, T)$ bimodule in such a way that

$$r(a \otimes b) = (ra \otimes bt)$$

for all $r \in R, a \in A, b \in B, s \in S$. 
(b) There exists a unique $\mathbb{Z}$-linear map
\[ \alpha \otimes \beta : A \otimes S \rightarrow B \rightarrow A' \otimes B' \] with $a \otimes b \rightarrow \alpha(a) \otimes \beta(b)$ for all $a \in A, b \in B$. Moreover, $\alpha \otimes \beta$ is $(R,T)$-linear.

**Proof:** (a) Let $r \in R$, and $t \in Y$. We claim that
\[ \phi(r,t) : A \times B \rightarrow A \otimes S B, (a,b) \rightarrow ra \otimes bt \] is $S$-balanced. Indeed it’s clearly $\mathbb{Z}$-bilinear and
\[ r(as) \otimes bt = (ra)s \otimes bt = ra \otimes s(bt) = ra \otimes (sb)t \]
So it’s $S$-balanced. Hence we obtain a map a $\mathbb{Z}$-linear
\[ \Phi(r,t) : A \otimes S B \rightarrow A \otimes S B, \quad a \otimes b \rightarrow ra \otimes bs. \]
Let $r,r' \in R$ and $t \in T$. It is easy to verify that
\[ \Phi(r + r', t)(a \otimes b) = (\Phi(r, t) + \Phi(r', t))(a \otimes b) \]
and
\[ \Phi(rr', 1)(a \otimes b) = (\Phi(r, 1) \circ \phi(r', 1))(a \otimes b) \]
Thus by the uniqueness assertion in the definition of the tensor product,
\[ \Phi(r + r', t) = \Phi(r, t) + \Phi(r', t) \quad \text{and} \quad \Phi(rr', 1) = \Phi(r, 1) \circ \Phi(r', 1). \]
Thus $A \otimes B$ is a left $R$-module by $rv = \Phi(r, 1)(v)$. Similarly $A \otimes B$ is a right $T$-module by $vt = \Phi(1, t)v$. Also $r((a \otimes b)t = ra \otimes bs = (r(a \otimes b))t$ So $(rv)t = r(vt)$ for all $r,t \in T, v \in A \otimes_R B$. Thus (a) holds.

(b) The map
\[ A \times B \rightarrow A' \otimes S B', (a,b) \rightarrow \alpha(a) \otimes \beta(b) \]
is $S$-balanced. So $\alpha \otimes \beta$ exists. That its $(R,T)$-linear is easily verified using arguments as in (a).

**Proposition 4.5.6** [seten] Let $D$ be a right $R$-module and
\[ A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0 \]
an exact sequence of $R$. Then
\[ D \otimes_R A \xrightarrow{id_D \otimes f} D \otimes_R B \xrightarrow{id_D \otimes g} D \otimes C \rightarrow 0 \]
is exact sequence of $\mathbb{Z}$-modules.
4.5. TENSOR PRODUCTS

Proof: As $D \times C$ is generated by the $d \otimes c$ and $g$ is onto, id)$D \otimes g$ is onto. Also

$$((\text{id}_D \otimes g) \circ (\text{id}_D \otimes f))(d \otimes a) = d \otimes (g(f(a))) = 0$$

So

$$\text{Im}(\text{id}_D \otimes f) \leq \ker(\text{id}_D \otimes g)$$

Let $E = \text{Im} f$ and

$$H = \text{Im} \text{id}_D \otimes \text{id}_E \rightarrow_B = \langle d \otimes e, d \in D, e \in E \rangle \subseteq D \otimes_R B$$

Note that $H = \text{Im}(\text{id}_D \otimes f)$. We will show that $H = F := \ker(\text{id}_D \otimes g)$. Without loss

$C = B/H$ and $g$ is the canonical epimorphism. We claim that the map

$$D \times B/E \rightarrow (D \otimes B)/H, (d, b + E) \rightarrow d \otimes b + H$$

is well defined and $R$-balanced.

Indeed $d \otimes (b + e) + H = (d \otimes b) + (d \otimes e) + H = d \otimes b + H$ So it well defined. Its clearly $R$-balanced.

Hence we obtain an onto $\mathbb{Z}$-linear map:

$$D \otimes_R B/E \rightarrow (D \otimes B)/H, \text{ with } d \otimes (b + E) \rightarrow (d \otimes b) + H.$$ 

id$_D \otimes g$ induces an isomorphism

$$(D \otimes B)/F \rightarrow D \otimes_R B/E, \text{ with } (d \otimes b) + F \rightarrow d \otimes (b + E)$$

The composition of these two maps give on onto map

$$\tau : (D \otimes B)/F \rightarrow (D \otimes B)/H \text{ with } (d \otimes b) + F \rightarrow (d \otimes b) + E.$$ 

As $D \otimes B$ is generated by the $d \otimes b$ we get $\tau(v + F) = v + E$ for all $v \in D \otimes B$. Since $\tau(0) = 0$ we conclude that $f \in E$ for all $f \in F$. Thus $F \leq E$ and $E = F$. \qed

Lemma 4.5.7 [tendir]

(a) Let $(A_i, i \in I)$ be a family of right $R$ modules and $(B_j, j \in J)$ a family of left $R$-modules. Then

$$\bigoplus_{i \in I} \otimes_R \bigoplus_{j \in J} A_i \otimes B_j \cong \sum_{i \in I} \sum_{j \in J} A_i \otimes B_j$$

(b) Let $R$ be a ring and $I, J$ sets. Then

$$F(I) \otimes F(J) \cong F(I \times J)$$

as a $\mathbb{Z}$-modules.
(b) Let $R$ and $S$ be rings with $R \leq S$. Let $I$ be a set and view $S$ as an $(S, R)$-bimodule. Then

\[ S \otimes_R F_R(I) \cong F_S(I) \]

as $S$-module.

**Proof:** (a) is readily verified using the universal properties of direct sums and tensor products.

(b) Since $R \otimes_R R \cong R$, (b) follows from (a).

(c) As $S \otimes_R R \cong S$, (c) follows from (a). \qed

**Lemma 4.5.8** Let $A$ be a right $R$ module, $B$ a $(R, S)$-bimodule and $C$ a left $S$-module. Then there exits $\mathbb{Z}$-linear isomorphism

\[ (A \otimes_R B) \otimes SC \] with $a \otimes b \otimes c \rightarrow a \otimes (b \otimes c)$

for all $a \in A, b \in B, c \in C$.

**Proof:** Straightforward form the universal properties of tensor products. \qed

In future we will just write $A \otimes_R B \otimes S C$ for any of the two isomorphic tensor products in the previous lemma. A similar lemma holds for more than three factors. $A \otimes_R B \otimes S C$ can also be characterized through $(R, S)$-balanced maps from $A \times B \times C \rightarrow T$, where $T$ is an abelian group. We leave the details to the interested reader.

**Proposition 4.5.9** Let $A$ be a right $R$ module, $B$ a $(R, S)$-bimodule and $C$ a right $S$-module. Then the map:

\[ \Xi : \text{Hom}_S(A \otimes_R B, C) \rightarrow \text{Hom}_R(A, \text{Hom}_S(B, C)), \Xi(f)(a)(b) = f(a \otimes b) \]

is a $\mathbb{Z}$-isomorphism.

**Proof:** Note that $\Xi(f)(a) : B \rightarrow C, b \rightarrow f(a, b)$ is indeed $S$-linear. Also $\Xi(f) : A \rightarrow \text{Hom}_S(B, C)$ is $R$-linear and $\Xi$ is $\mathbb{Z}$-linear. It remains to show that $\Xi$ is a bijection. We do this by defining an inverse. Let $\alpha : A \rightarrow \text{Hom}_S(B, C)$ be $R$-linear. We claim that the map

\[ A \times B \rightarrow C; (a, b) \rightarrow \alpha(a)(b) \]

is $R$ balanced. Indeed it is $\mathbb{Z}$-bilinear and

\[ \alpha(ar)(b) = (\alpha(a)r)(b) = \alpha(a)(rb). \]

So there exist

\[ \Theta(\alpha) : A \otimes B \rightarrow C \text{ with } \Theta(\alpha)(a \times b) = \alpha(a)(b) \]
for all $a \in A$, $b \in B$. It is readily verified that $\Theta(\alpha)$ is $S$-linear. So

$$\Theta : \text{Hom}_R(A, \text{Hom}_S(B, C)) \to \text{Hom}_S(A \otimes_R B, C)$$

We claim that $\Theta$ and $\Xi$ are inverses:

$$\Xi(\Theta(\alpha))(a)(b) = \Theta(\alpha)(a \otimes b) = \alpha(a)(b)$$

So $\Xi(\Theta(\alpha)) = \alpha$.

$$\Theta(\Xi(f))(a \otimes b) = \Xi(f)(a)(b) = f(a \otimes b)$$

and so $\Theta(\Xi(f)) = f$. \hfill $\square$

Here is a special case of the previous proposition. Suppose $R$ is a commutative ring and $A$ and $B$, $R$-modules. Applying 4.5.9 with $C = R$. We get that

$$(A \otimes B)^* \cong \text{Hom}_R(A, B^*)$$

Suppose that $R$ is commutative and $A, B$ are $R$-modules we obtain a $\mathbb{Z}$-linear map:

$$\sigma : A^* \otimes B^* \to (A \otimes B)^* \text{ with } \gamma(\alpha \otimes \beta)(a \otimes b) = \alpha(a)\beta(b).$$

Indeed this follows from $\alpha \otimes \beta : A \otimes B \to R \otimes R \cong R$.

If $A$ and $B$ are free of finite rang it is easy to see that this is an isomorphism. If $A$ and $B$ are free, $\sigma$ is still one to one, but not necessarily onto. Suppose that $A_k = R/I_k$, $k \in \{1, 2\}$, is a cyclic $R$-module. Put $J_k = \text{Ann}_R(I_k)$. Then by ??, $A_k^* \cong J_k$. Also $A_1 \otimes A_2 \cong R/(I_1 + I_2)$. Now $\text{Ann}_R(I_1 + I_2) = \text{Ann}_R(I_1) \cap \text{Ann}_R(I_2) = J_1 \cap J_2$. Thus $(A_1 \otimes_R A_2)^* \cong J_1 \cap J_2$. $\sigma$ from above ( with $A = A_1, B = A_2$) now reads:

$$\sigma : J_1 \otimes_R J_2 \to J_1 \cap J_2 \quad (j_1, j_2) \to j_1j_2$$

We will know give an example where $\sigma = 0$ but $J_1 \otimes J_2 \neq 0$. Let $S$ be a ring and $M$ an $(S, S)$-bimodule. Define $M \times S$ to be the ring with additive group $M \oplus S$ and multiplication

$$(m_1, s_1) \cdot (m_2, s_2) = (m_1s_2 + s_1m_2, s_1s_2)$$

It is easy to verify that $M \times S$ is a ring. As an example we verify that the multiplication is associative

$$(m_1, s_1) \cdot (m_2, s_2) \cdot (m_3, s_3) = m_1s_2 + s_1m_2, s_1s_2 \cdot (m_3, s_3) = (m_1s_2s_3 + s_1m_2s_3 + s_2s_3m_3, s_1s_2s_3)$$

A similar calculation shows that the right side is also equal to $(m_1, s_1) \cdot ((m_2, s_2) \cdot (m_3, s_3))$. Identify $(m, 0)$ with $m$ and $(0, s)$ with $s$. Then

$$M \times S = M + S, s_1 \cdot s_2 = s_1s_2, s \cdot m = sm, m \cdot s = ms \text{ and } m_1 \cdot m_2 = 0$$

for all $s, s_1, s_2 \in S$ and $m, m_1, m_2 \in m$. Also $M$ is an ideal in $M \times S$ and $(M \times S)/M \cong S$. Indeed the map $M \times S \to S, (m, s) \to s$ is an onto ring homomorphism with kernel $M$. 
Suppose now that $S$ is commutative and $M$ a faithful $S$ module. Put $R = M \times S$. Then $R$ is commutative. As $M^2 = 0$ and $\text{Ann}_S(M) = 0$, $\text{Ann}_R(M) = M$. Also $M \cap M = M = M + M$. We conclude $(R/M)^* \cong M$, $R/M \otimes R/M \cong R/M$, $(R/M \otimes R/M)^* \cong M$ and

$$\sigma : M \otimes_R M \to M, (m_1, m_2) \to m_1 m_2 = 0$$

Suppose that $M = F_S(I)$ is a free $S$-module. Then as an $R$-module,

$$M \cong \bigoplus_{i \in I} R/M$$

Thus

$$M \otimes_R M \cong \bigoplus_{i \in I} \bigoplus_{j \in I} R/M$$

and so $M \otimes_R M \neq 0$ (unless $I \neq \emptyset$).

### 4.6 Free modules and torsion modules

In this section $R$ is a ring with identity and all $R$-modules are assumed to be unitary.

Let $M$ be a $R$-module and $(m_i, i \in I)$ a family of elements in $M$. By 4.3.2 there exists a $R$-linear map

$$\alpha : \bigoplus_{i \in I} R \to M \text{ with } i \to m_i$$

If $\alpha$ is an isomorphism, $(m_i \mid i \in I)$ is called a basis for $M$. It is more or less obvious that a subset $B$ of $M$ is a basis if and only if every element $m$ in $M$ can be uniquely written as

$$m = \sum_{b \in B} r_b b \text{ with } r_b \in R \text{ for all } b \in R.$$ As usually we assume here that almost all $r_b$ are zero. If $M$ has a basis $B$ then $M$ is isomorphic to the free module on $B$. For this reason we call $M$ itself a free module. We say that a subset $L$ of $M$ is linear independent if $L$ is a basis for $RL$, note that this is the case if and only if

$$\sum_{l \in L} r_l l = 0 \implies r_l = 0 \text{ for all } l \in L$$

Is a submodule of a free module free? The answer is almost always no. For example if $R = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{Z}^+$, $n$ not a prime, and $m$ is a proper divisor of $m$ then $m\mathbb{Z}/n\mathbb{Z}$ is a submodule of $R$ which is not free. A obvious necessary condition for all submodules of all free modules for a ring $R$ to be free is that all submodules of $R$ itself are free. The next theorem shows that this condition is also sufficient.

**Theorem 4.6.1 [subfree]**

(a) Suppose that all left ideals in the ring $R$ are free as $R$-modules. Then every submodule of a free module is free.
(b) If $R$ is a principal ring and $M$ is a $R$-submodule of $F_R(I)$ for some set $I$, then $M \cong F_R(J)$ for some set $J \subseteq I$.

**Proof:** (a) Let $M$ be a free module with basis $B$ and $A$ a $R$-submodule in $M$. According to the well ordering principal (A.5) we can choose a well ordering on $B$. For $b \in B$ define

$$M_b^* = \sum_{e \in B, e \in B} \in Re$$

and $M_b = M_b^*$. Let $A_b = M_b \cap A$ and $A_b^* = M_b^* \cap A$. Then

$$A_b/A_b^* = A_b/A_b \cap M_b^* \cong A_b + M_b^*/M_b^* \leq M_b/M_b^* \cong Rb \cong R$$

By assumption every submodule of $R$ is free and so $A_b/A_b^*$ is free. Let $E_b \subset A_b$ so that $(e + A_b^*, e \in E_b)$ is a basis for $A_b/A_b^*$. Let $E = \bigcup_{b \in B} E_b$. We claim that $E$ is a basis for $A$.

Let $m \in M$. Then $m = \sum_{b \in B} r_b b$ with $r_b \in R$ and almost all $m_b = 0$. So we can choose $b_m \in B$ maximal with respect $r_{b_m} \neq 0$. Clearly for $e \in E_b$, $b_e = b$. In general, $b_m$ is minimal in $B$ with $m \in M_{b_m}$.

Now suppose that $\sum_{e \in E} r ee = 0$ so that almost all, but not all $r_e = 0$. Let $b$ be maximal with $b = b_e$ and $r_e \neq 0$ for some $e \in E$. The $e \in E_b$ for all $e$ with $b_e = e$ and $e \in A_b^*$ for all $e$ with $r_e \neq 0$ and $b_e \neq b$. Thus

$$0 = \sum_{e \in E} r ee + A_b^* = \sum_{e \in E_b} r ee + A_b^*$$

But this contradicts the linear independents of the $e + A_b^*, e \in E_b$.

Hence $E$ is linear independent. Suppose that $A \not\subseteq RE$ and pick $a \in A \setminus RE$ with $b = b_a$ minimal. Then $a \in A_b$. Hence

$$a + A_b^* = \sum_{e \in E_b} r_e e + A_b^*$$

Put $d = \sum_{e \in E_b} r_e e$. Then $d \in RE \leq A, a - d \in A_b^*$. By minimality of $b$, $a - d \in RE$ and so $a \in d + RE = RE$.

So $A \leq RE, A = RE$ and $E$ is a basis for $A$.

(b) If $R$ is a principal ring then $|E_b| \leq 1$ for all $b \in B$ so (b) holds. \qed

If $R$ is commutative (with identity) only PID have the property that every left ideal in $R$ is free. Indeed if $a, b \in R^\#$, then $ba - ab = 0$ and so $a$ and $b$ are linear dependent. Hence every ideal is cyclic as a module and so a principal ideal. Suppose that $ab = 0$ for some non-zero $a, b \in R$. Then $bRa = 0$ and so $Ra$ is not free, a contradiction. Thus $R$ is also an integral domain and so a PID.

**Corollary 4.6.2 [subfingen]** Let $R$ be a principal ring, $M$ an $R$-module and $W$ an $R$-submodule of $M$. If $M = RI$ for some $I \subseteq M$, then $W = RJ$ for some $J \subseteq W$ with $|J| \leq |I|$. In particular, if $M$ is finitely generated as $R$-module, so is $M$. 
Proof: Let $\phi : F_R(I)$ be $R$-linear with $\phi(i) = i$ for all $i \in I$. Let $A = \phi^{-1}(W)$. By 4.6.1 $A$ has a basis $J^*$ with $|J^*| \leq |I|$. Let $J = \phi(J^*)$. Then $J$ generated $W$ as an $R$-module and $|J| \leq |J^*| \leq |I|$. 

\[\text{Definition 4.6.3 [dtorsion]}\] Let $M$ be a unitary $R$-module and $m \in M$.

(a) $m$ is called a torsion element if $\text{Ann}_R(m) \neq 0$.

(b) $M$ is called a torsion module if all elements are torsion elements.

(c) $M$ is called torsion free if $0$ is the only torsion element.

(d) $M$ has finite exponent of $\text{Ann}_R(M) \neq 0$.

Note that $m$ is not a torsion element if and only if $\{m\}$ is linear independent.

\[\text{Lemma 4.6.4 [torsion]}\] Let $M$ be a module for the integral domain $R$.

(a) The torsion elements form a submodule $T(M)$.

(b) If $M$ is generated by finitely many torsion elements, then $M$ has finite exponent.

(c) $M/T(M)$ is torsion free.

Proof: (a) Let $a, b$ be torsion elements and pick $r, s \in R^\#$ with $ra = sb = 0$. As $R$ is an integral domain $rs \neq 0$. Also

$$rs(Ra + Rb) = Rsra + Rrsb = 0$$

Hence all elements in $Ra + Rb$ are torsion. So the torsion elements indeed form a submodule.

(b) Suppose that $M = RA$, where $A$ is a finite set of torsion elements. For $a \in A$ pick $t_a \in R^\#$ with $t_a a = 0$. Put $t = \prod_{a \in A} t_a$. Then $t \neq 0$ and $tM = 0$

(c) Let $x + T(M)$ be a torsion element. Pick $0 \neq r \in R$ with $rx \in T(M)$. Then $rx$ is torsion and so $s(rx) = 0$ for some $0 \neq s \in R$. Hence $(sr)x = 0$ and as $R$ is an integral domain, $sr \neq 0$. So $x \in T(M)$ and $M/T(M)$ is torsion free. 

\[\text{Theorem 4.6.5 [freetorsion]}\] Let $M$ be an $R$-module.

(a) Any linear independent subset of $M$ lies in a maximal linear independent subset.

(b) Let $L$ be a maximal linear independent subset of $M$. Then $M/RL$ is a torsion module.
4.6. FREE MODULES AND TORSION MODULES

Proof: (a) Let $E$ be a linear independent subsets of $M$. Let $\mathcal{L}$ be the set of linear independent subsets of $M$ containing $E$. Order $\mathcal{L}$ by inclusion. The union of a chain in $\mathcal{L}$ is an upper bound for the chain. So Zorn’s Lemma A.1 implies that $M$ has a maximal linear independent subset $L$.

(b) Let $W = RL$. Suppose that $M/W$ is not torsion and pick $m \in M$ so that $m + W$ is not torsion. Then $m$ is not torsion and $Rm \cap W = 0$. Hence $L \cup \{m\}$ is linear independent, a contradiction to the maximal choice of $L$. \hfill \Box

We remark that if $L$ is a maximal linear independent subset of $M$, then $RL$ does not have to be a maximal free submodule. Indeed the following example shows that $M$ does not have to have a maximal free submodule. (Zorn’s lemma does not apply when the union of a chain of free submodules might not be free)

Let $R = \mathbb{Z}$ and $M = \mathbb{Q}$ with $\mathbb{Z}$ acting by right multiplication. As $\mathbb{Q}$ has no zero divisors, $M$ is torsion free. In particular, every non-zero element $a$ is linear independent. We claim \{a\} is a maximal linear independent subset. Indeed, $a, b \in \mathbb{Q}$. Then $a = \frac{n}{m}$ and $b = \frac{p}{q}$ with $n, m, q, p \in \mathbb{Z}$. Then $(mp)a - (nq)b = nm - nm = 0$ and $a$ and $b$ are linear dependent.

We conclude that every free submodule of $M$ is of the form $\mathbb{Z}a, a \in \mathbb{Q}$. Let $t \in \mathbb{Z}$ with $t > 1$ then $\mathbb{Z}a \leq mb\mathbb{Z}\frac{a}{t}$ and so $M$ has no maximal free submodules.

$\mathbb{Q}$ as a $\mathbb{Z}$ module has another interesting property: every finitely generated submodules is cyclic. Indeed, if $A$ is generated by $\frac{m_i}{m_i}, 1 \leq i \leq k$, put $m = \text{lcm}_{1 \leq i \leq k} m_i$ and then $mA \cong A$ and $mA \leq \mathbb{Z}$. So $mA$ and $A$ are cyclic.

Since division rings have no non-zero unitary torsion modules 4.6.5 has the following corollary:

Corollary 4.6.6 [vectorspace] Let $V$ be a vector space over the division ring $D$. Then $V$ has a basis and every linear independent subset of $V$ can be extended to a basis of $V$. \hfill \Box

Lemma 4.6.7 [idsubfree] Let $M$ be a torsion free $R$-module for the integral domain $I$.

Suppose that one of the following holds:

1. $M$ is finitely generated.

2. If $N$ is a submodule of $M$ so that $M/N$ is a torsion module, then $M/N$ has finite exponent.

Then $M$ is isomorphic to a submodule of a free module $W$. Moreover $W$ can be chosen as a submodule of $M$.

Proof: Note that by 4.6.4 condition 1. implies condition 2.. So we may assume that 2. holds. By 4.6.5 there exists a free submodule $W$ of $V$ so that $M/W$ is torsion. By there exists $0 \neq r \in R$ with $rM/W = 0$ Hence $rM \leq W$.

Consider the map $\alpha : M \to W, m \to rm$
As $R$ is commutative, $\alpha$ is a $R$-linear. As $M$ is $\alpha$ is one to one. Thus $m \cong \alpha(M) = rM \leq W$. 

**Theorem 4.6.8 [torfree]** Let $M$ be a finitely generated module for the PID $R$. Then there exists a free submodule $F \leq M$ with $M = F \oplus T(M)$.

**Proof:** By 4.6.4, $M/T(M)$ is torsion free, so by 4.6.7 $M/T(M)$ is isomorphic to a submodule of a free module. Hence by 4.6.1 $M/T(M)$ is free. Finally by ?? $M/T(M)$ splits over $T(M)$. 

### 4.7 Modules over PID’s

A non-zero $R$-module $M$ is called simple if 0 and $M$ are the only $R$-submodules of $M$. For example if $I$ is a left ideal in $R$, then $R/I$ is simple if and only if $I$ is a maximal left ideal.

**Theorem 4.7.1 [primary]** Let $R$ be a PID and $p \in R$ a prime. Suppose that $M$ is an $R$-module with $p^kM = 0$ for some $k \in \mathbb{Z}^+$. Then

(a) If $M = Rm$ is cyclic, $M \cong R/(p^l)$ for some $0 \leq l \leq k$. Moreover, every $R$-submodule of $Rm$ is of the form $Rp^t$ for some $0 \leq t \leq l$.

(b) Let $W$ be a $R$-submodule in $M$. Then $W$ is a direct summand of $M$ if and only if $p^tM \cap W \leq p^tW$ for all $t \in \mathbb{N}$.

(c) $M$ is a direct sum of cyclic submodules.

**Proof:** Put $P = (p)$. Recall that $P^0$ is defined as $R$. Without loss $k$ is minimal with respect to $p^kM = 0$.

(a) Let $J = \text{Ann}_R(m)$. Then $M \cong R/J$. Let $W$ be a an $R$-submodule of $M$. Then $W = Im$ for some ideal $I$ of $R$ with $J \leq I$. Since $R$ is a PID, $I = Ri$ for some $i \in I$. Since $p^kM = 0$, $p^k \in J \leq I$ and so $i \mid p^k$. Thus $I = (p^s)$ and $J = (p^l)$ for some $s \leq l \leq k$. Since $W = Im = Rp^t$, all parts of (a) are proved.

(b) " $\implies$ " Suppose that $M = W \oplus K$ for some $R$-submodule $K$ of $M$. Then $p^tM = p^tW \oplus p^tK$ and so $p^tM \cap W = p^tW$.

" $\impliedby$ " Suppose that $p^tW \cap W = p^tW$ for all $t \in \mathbb{N}$. We proceed by induction on $k$. If $k = 0$ we get $M = 0$ and there is nothing to prove. Note that $P^{k-1}(PM) = 0$ and

$$P^t(PM) \cap PW = (P^{t+1}M \cap W) \cap PW = P^{t+1}W \cap PW = P^t(PW).$$

Thus by induction $PW$ is a direct summand of $PM$. Let $PM = D \oplus PW$ for some submodule $D$ of $PM$. Note that $D \cap W = D \cap PM \cap W = D \cap PW = 0$.

Let $\mathcal{M}$ be the set of all submodules $E$ in $M$ with $D \leq E$ and $E \cap W = 0$. The $D \in \mathcal{M}$. Order $\mathcal{M}$ by inclusion. The union of a chain in $\mathcal{M}$ is in $\mathcal{M}$. So by Zorn’s lemma A.1,
4.7. MODULES OVER PID’S

$\mathcal{M}$ has a maximal member $E$. Suppose $M \neq E + W$ and let $m \in M \setminus (E + W)$. Then $pm \in pM = D + pW$. So there exists $w \in W$ with $pm - pw \in D \leq E$. So replacing $m$ by $m - w$ we assume that $pm \in E$. Let $t \in R$ with $tm \in E + W$. If $t \notin P$, then as $PM \leq E + W$ and $P$ is a maximal, $\text{Re}m \leq E + W$, a contradiction. So $t = rp$ for some $r \in R$ and $tm = rpm \in E$. Thus $\text{Re}m \leq E$ and

$$(\text{Re}m + E) \cap W \leq ((\text{Re}m + E) \cap (E + W)) \cap W = ((\text{Re}m \cap (E + W)) + E) \cap W \leq E \cap W = 0$$

a contradiction the maximal choice of $E$.

So $M = E + W = E \oplus W$ and $W$ is a direct summand of $M$.

(c) Let $\mathcal{D}$ be the set of sets of cyclic submodules of $M$. We say that $D \in \mathcal{D}$ is linear independent if $\sum D = \oplus D$ and we say that $D$ is a direct summand if $\sum D$ is a direct summand of $M$. Let $\mathcal{M}$ be the set of all linear independent, direct summands in $\mathcal{D}$. Order $\mathcal{M}$ by inclusion. Let $\mathcal{C}$ be a chain in $\mathcal{M}$ and $D = \bigcup \mathcal{C}$. Clearly $D \in \mathcal{D}$. Also $D$ is linear independent.

We claim that

$$\sum D = \bigcup_{C \in \mathcal{C}} \sum C.$$ 

Clearly the right hand side is contained in the left. Let $x \in \sum D$. Then $x \in U_1 + U_2 + \ldots + U_n$ for some $U_i \in D$. Since $D = \bigcup \mathcal{C}$ there exits $C_i \in D$ with $U_i \in C_i$. Since $\mathcal{D}$ is a chain we may assume $C_1 \subseteq C_2 \subseteq \ldots \subseteq C_n$, hence $U_i \in C_n$ for all $1 \leq i \leq n$ and so

$$x \in U_1 + U_2 + \ldots + U_n \leq \sum C_n \leq \bigcup_{C \in \mathcal{C}} \sum C$$

This proves the claim.

From the claim

$$(\sum D) \cap p^sM = \bigcup_{C \in \mathcal{C}} (\sum C \cap p^sM) = \bigcup_{C \in \mathcal{C}} \sum p^sC = p^s \sum D$$

Thus by (b) $\sum D$ is a direct summand of $M$. So $D \in \mathcal{D}$ and $D$ is an upper bound for $\mathcal{C}$. So by Zorn’s lemma, $\mathcal{D}$ has a maximal member $D$. By definition of $\mathcal{D}$, $M = \sum D \oplus E$ for some $R$-submodule $E$ of $D$.

Suppose that $E \neq 0$. Pick $l$ minimal with $p^lE = 0$. Then $p^{l-1}E \neq 0$ and we can choose $e \in E$ with $p^{l-1}e \neq 0$. We claim that $Re$ is a direct summand of $E$. For this we want to apply (b) to $Re$ and $R$. Let $0 \leq t < l$. By (a) every submodule of $Re$ is of the form $p^sRe$. In particular, $Re \cap p^tE = p^sRe$ for some $s$. But $p^{l-t}(Re \cap p^tE) = 0$, so $p^{l-t}p^se = 0$ and $s \geq t$. Thus

$$Re \cap p^tE = p^sRe \leq p^tRe$$

So by (b) $Re$ is a direct summand of $E$. But then $\sum D + Re$ is a direct summand of $M$. Also $Re \cap \sum D \leq E \cap \sum D = 0$ and $D \cup \{Re\}$ is linear independent. But thus contradicts the maximal choice of $D$.

Hence $E = 0$ and $M = \sum D = \bigoplus D$ and (c) holds.
Theorem 4.7.2 [decprim] Let $R$ be a PID and $M$ a torsion module for $R$. Let $\mathcal{P}$ be the set of non-zero prime ideals in $M$. For $P \in \mathcal{P}$ let $M_P = \bigcup_{k \in \mathbb{Z}^+} \text{Ann}_M(P^k)$. Then

$$M = \bigoplus_{P \in \mathcal{P}} M_P.$$  

**Proof:** Let $m \in M$ and pick $r \in R^\#$ with $rm = 0$. Then there exists pairwise nonassociate primes $p_i \in R$ and positive integer $k_i$, $1 \leq k \leq n$ with

$$r = p_1^{k_1} \cdots p_n^{k_n}.$$  

Put $a_i = \prod_{j \neq i} p_j^{k_j}$. Then $r = p_i^{k_i}a_i$. Also $\gcd_{i=1}^n a_i = 1$ and so $1 = \sum s_i a_i$ for some $s_i \in R$. Put $m_i = s_i a_i m$. Then $m = \sum_{i=1}^n m_i$ and

$$p_i^{k_i} m_i = p_i^{k_i} s_i a_i m = s_i (p_i^{k_i} a_i) m = s_i (r m) = 0.$$  

Thus $m_i \in \text{Ann}_M(P_i^{k_i}) \leq M_{(p_i)}$ and so

$$M = \bigoplus_{P \in \mathcal{P}} M_P.$$  

Let $P \in \mathcal{P}$. Put

$$M_{P'} = \bigoplus_{P \neq Q \in \mathcal{P}} M_Q.$$  

In remains to show that $M_{P'} \cap M_P = 0$. For this let $k \in \mathbb{Z}^+$ and $0 \neq m \in M_{P'}$. Then $am = 0$ for some $a \in R$ with $a \notin P$. Let $P = (p)$. Then $1 = ra + sp^k$ for some $r, s \in R$. Thus $m = ram + sp^k m = sp^k m$. Hence $p^k m \neq 0$ and $m \notin M_P$. \hfill $\Box$

Theorem 4.7.3 [pidmod] Let $M$ be a finitely generated module for the PID $R$. Then $M$ is direct sum of finitely many cyclic modules. Moreover, each of the summand can be chosen be isomorphic to $R/P^k$ for some prime ideal $P$ and some $k \in \mathbb{Z}^+$.  

**Proof:** By 4.6.8, $M = F \oplus T(M)$, where $F$ is free. So $F$ is a direct sum of copies of $R$. Note that $R \cong R/0$ and 0 is a prime ideal. Also by 4.7.2 $T(M) = \bigoplus_{P \in \mathcal{P}} M_P$. As $M$ is finitely generated and $M_p$ is a homomorphic image of $M$, $M_p$ is finitely generated. So (see 4.6.4) $p^k M_p = 0$ for some $k \in \mathbb{N}$. Thus by 4.7.1 $M_p$ is the direct sum of cyclic modules, and each of the cyclic modules is isomorphic to $R/(p^k)$. We leave it as an exercise to verify that all the direct sums involved are actually finite sums. \hfill $\Box$

Corollary 4.7.4  

(a) Let $A$ be a finitely generated abelian group. Then $A$ is the direct sum of cyclic groups.

(b) Let $A$ be an elementary abelian $p$-group for some prime $p$. (That is $A$ is abelian and $pA = 0$). Then $A$ is the direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$. 
4.7. MODULES OVER PID’S

**Proof:** Note that an abelian group is nothing else as a module over \( \mathbb{Z} \). So (a) follows from 4.7.3 and (b) from 4.7.1. (b) can also be proved by observing that \( A \) is also a module over the field \( \mathbb{Z}/p\mathbb{Z} \) and so has a basis. \( \square \)
4.8 Composition series

**Definition 4.8.1** Let $R$ be a ring, $M$ an $R$-module and $C$ a set of $R$-submodules in $R$. We say that $C$ is a $R$-series on $M$ provided that

(i) $C$ is a chain, that is for any $A, B \in C$, $A \leq B$ or $B \leq A$.

(ii) $0 \in C$ and $M \in C$.

(iii) $C$ is closed under unions and intersections, that is if $\mathcal{D} \subseteq C$, then

$$\bigcup \mathcal{D} \in C \text{ and } \bigcap \mathcal{D} \in C.$$ 

For example any finite chain

$$0 = M_0 < M_1 < M_2 < M_3 < \ldots < M_{n-1} < M_n = M$$

of $R$-submodules of $M$ is an $R$-series.

If $R = M = \mathbb{Z}$ and $p$ is a prime then

$$0 < \ldots < p^{k+1} \mathbb{Z} < p^k \mathbb{Z} < p^{k-1} \mathbb{Z} < \ldots < p \mathbb{Z} < \mathbb{Z}$$

is a $\mathbb{Z}$-series. More generally, if $n_1, n_2, n_3, \ldots$ is any sequence of integers larger than 1, then

$$0 < n_1 \ldots n_{k+1} \mathbb{Z} < n_1 \ldots n_k \mathbb{Z} < \ldots < n_1 n_2 \mathbb{Z} < n_1 \mathbb{Z} < \mathbb{Z}$$

is a $\mathbb{Z}$ series on $\mathbb{Z}$.

**Definition 4.8.2** Let $R$ be a ring, $M$ an $R$-module and $C$ an $R$-series on $M$.

(a) A jump in $C$ is a pair $(A, B)$ with $A, B \in C$, $A \leq B$ and so that

$$D \leq A \text{ or } B \leq D \text{ for all } D \in C.$$ 

Jump($C$) is the set of all jumps of $C$.

(b) If $(A, B)$ is a jump of $C$ then $B/A$ is called a factor of $C$.

(c) $C$ is a $R$-composition series on $M$ provided that all the factors of $C$ are simple $R$-modules.

Let $C$ be $R$-series on $M$. For $B \in C$ define

$$B^- = \bigcup \{ A \in C \mid A \leq B \}.$$ 

Note that $B^- \in C$ and $B^- \leq B$. 

4.8. COMPOSITION SERIES

Suppose that $B^- \neq B$. Let $D \in \mathcal{C}$. Then $B \leq D$ or $D \leq B$. In the latter case, $D \leq B^-$ and so $(B^-, B)$ is a jump of $\mathcal{C}$.

Conversely, if $(A, B)$ is a jump it is easy to see that $A = B^-$. Thus

$$\text{Jump}(\mathcal{C}) = \{(B^-, B) \mid B \in \mathcal{C}, B^- \neq B\}.$$

Consider the series

$$0 < n_1 \ldots n_{k+1}\mathbb{Z} < n_1 \ldots n_k\mathbb{Z} < \ldots < n_1n_2\mathbb{Z} < n_1\mathbb{Z} < \mathbb{Z}.$$

As $n_1 \ldots n_{k+1}\mathbb{Z}/n_1 \ldots n_k\mathbb{Z} \cong \mathbb{Z}/n_k\mathbb{Z}$ as $R$-modules, this series is a composition series if and only if each $n_k$ is a prime. If we chose $n_k = p$ for a fixed prime $p$ we get a composition series all of whose factors are isomorphic. On the other hand we could choose the $n_k$ to be pairwise distinct primes and obtain a composition series so that now two factors are isomorphic.

**Proposition 4.8.3 [compmax]** Let $R$ be a ring and $M$ a $R$-module. Let $\mathcal{M}$ be the set of chains of $R$-submodules in $M$. Order $\mathcal{M}$ by inclusion and let $\mathcal{C} \in \mathcal{M}$. Then $\mathcal{C}$ is a composition series if and only if $\mathcal{C}$ is a maximal element in $\mathcal{M}$.

**Proof:**

$\implies$ Suppose that $\mathcal{C}$ is a composition series but is not maximal in $\mathcal{M}$. Then $\mathcal{C} \subseteq \mathcal{D}$ for some $\mathcal{D} \in \mathcal{M}$. Hence there exists $D \in \mathcal{D} \setminus \mathcal{C}$. We will show that there exists a jump of $\mathcal{C}$ so that the corresponding factor is not simple, contradicting the assumption that $\mathcal{C}$ is a composition series. Define

$$D^+ = \bigcap \{E \in \mathcal{C} \mid D \leq E\} \quad \text{and} \quad D^- = \bigcup \{E \in \mathcal{C} \mid E \leq D\}.$$ 

As $\mathcal{C}$ is closed under unions and intersections both $D^+$ and $D^-$ are members of $\mathcal{C}$. In particular, $D^- \neq D \neq D^+$. From the definition of $D^+$, $D \leq D^+$, also $D^- \leq D$ and so

$$D^- \leq D \leq D^+.$$

Thus $D/D^+$ is a proper $R$-submodule of $D^+/D^-$ and it remains to verify that $(D^-, D^+)$ is a jump. For this let $E \in \mathcal{C}$. As $\mathcal{D}$ is totally ordered, $E \leq D$ or $D \leq E$. In the first case $E \leq D^-$ and in the second $D^+ \leq E$.

$\iff$ Let $\mathcal{C}$ be a maximal element of $\mathcal{M}$. We will first show that

$(\ast)$ Let $E$ be an $R$-submodule of $G$ such that for all $C \in \mathcal{C}$, $E \leq C$ or $C \leq E$. Then $E \in \mathcal{C}$.

Indeed, under these assumptions, $\{E\} \cup \mathcal{C}$ is a chain of submodules and so the maximality of $\mathcal{C}$ implies $E \in \mathcal{C}$. 

From (*) we conclude \(0 \in \mathcal{C}\) and \(M \in \mathcal{C}\). Let \(\mathcal{D} \subseteq \mathcal{C}\) and put \(E = \bigcup \mathcal{D}\). We claim that \(E\) fulfills the assumptions of (*). For this let \(C \in \mathcal{C}\). If \(C \leq D\) for some \(D \in \mathcal{D}\) then \(C \leq D \leq E\). So suppose that \(C \not\leq D\) for each \(D \in \mathcal{D}\). As \(\mathcal{C}\) is totally ordered, \(D \leq C\) for each \(D \in \mathcal{D}\). Thus \(E \leq D\). So we can apply (*) and \(E \in \mathcal{C}\). Thus \(\mathcal{C}\) is closed under unions.

Similarly, \(\mathcal{C}\) is closed under intersections. Thus \(\mathcal{C}\) is a series and it remains to show that all its factors are simple. So suppose that \((A,B)\) is a jump of \(\mathcal{C}\) so that \(B/A\) is not simple. Then there exists a proper \(R\)-submodule \(\overline{E}\) of \(B/A\). Note that \(\overline{E} = E/A\) for some \(R\)-submodule \(E\) of \(M\) with \(A \leq E \leq B\).

As \((A,B)\) is a jump, \(E \not\in \mathcal{C}\). Let \(C \in \mathcal{C}\). Then \(C \leq A\) or \(B \leq C\). So \(C \leq E\) or \(E \leq C\). Thus by (*), \(E \in \mathcal{C}\), a contradiction.

\[\square\]

**Corollary 4.8.4 [excomp]** Every \(R\)-modules has a composition series.

**Proof:** Let \(\mathcal{M}\) be as in 4.8.3. We leave it as an routine application of Zorn’s Lemma A.1 to show that \(\mathcal{M}\) has a maximal element. By 4.8.3 any such maximal element is a composition series.

In the next lemma we will find series for direct sums and direct products of modules. For this we first need to introduce the concept of cuts for a totally ordered set \((I, \leq)\).

We say that \(J \subseteq I\) is a cut of \(I\) if for all \(j \in J\) and all \(i \in I\) with \(i \leq j\) we have \(i \in J\). Let \(\text{Cut}(I)\) be the set of all cuts of \(I\). Note that \(\emptyset \in \text{Cut}(I)\) and \(I \in \text{Cut}(I)\). Order \(\text{Cut}(I)\) by inclusion. We claim that \(\text{Cut}(I)\) is totally ordered. Indeed, let \(J, K \in \text{Cut}(I)\) with \(K \not\subseteq J\). Then there exists \(k \in K \setminus J\). Let \(j \in J\). Since \(k \not\in J\) and \(J\) is a cut, \(k \not\leq j\). Since \(I\) is totally ordered, \(j < k\) and since \(K\) is a cut, \(j \in K\). So \(J \subseteq K\) and \(\text{Cut}(I)\) is totally ordered.

Let \(i \in I\) and put \(i^+ = \{ j \in I \mid j \leq i\}\). Note that \(i^+\) is a cut of \(I\). The map \(I \to \text{Cut}(I)\), \(i \to i^+\) is an embedding of totally ordered sets. Put \(i^- = \{ j \in I \mid j < i\}\). Then also \(i^-\) is a cut.

We leave it as an exercise to verify that unions and intersection of arbitrary sets of cuts are cuts.

As an example consider the case \(I = \mathbb{Q}\) ordered in the usual way. Let \(r \in \mathbb{R}\) and define \(r^- = \{ q \in \mathbb{Q} \mid q < r\}\). Clearly \(r^-\) is a cut. We claim that every cut of \(\mathbb{Q}\) is exactly one of the following cuts:

\[\emptyset; \; \mathbb{Q}; \; q^+ (q \in \mathbb{Q}); \; r^- (r \in \mathbb{R})\]

Indeed, let be \(J\) be a non-empty cut of \(\mathbb{Q}\). If \(J\) has no upper bound in \(\mathbb{Q}\), then \(J = \mathbb{Q}\). So suppose that \(J\) has an upper bound. By a property of the real numbers, every bounded non-empty subset of \(\mathbb{R}\) has a least upper bound. Hence \(J\) has a least upper bound \(a\). Then \(J \subseteq r^+\).

If \(r \in J\), then \(r \in \mathbb{Q}\) and \(r^+ \subseteq J \subseteq r^+\). So \(J = r^+\).
If \( r \not\in J \) we have \( J \subseteq r^- \). We claim that equality holds. Indeed let \( q \in r^- \). As \( r \) is a least upper bound for \( J \), \( q \) is not an upper bound for \( J \) and so \( q < j \) for some \( j \in J \). Thus \( q \in J \) and \( J = r^- \).

**Lemma 4.8.5 [serdirect]** Let \((I, \leq)\) be a totally ordered set and \( R \) a ring. For \( i \in I \) let \( M_i \) be a non zero \( R \)-module. Let \( M = \{ \bigoplus_{i \in I} M_i, \prod_{i \in I} M_i \} \). For \( J \) a cut of \( I \) define

\[
M_J^+ = \{ m \in M \mid m_i = 0 \forall i \in I \setminus J \}
\]

and if \( J \neq \emptyset \),

\[
M_J^- = \{ m \in M \mid \exists j \in J \text{ with } m_i = 0 \forall i \geq j \}.
\]

Put \( M_{\emptyset}^- = 0 \).

(a) For all \( k \in I \), \( M_{k^+}^- = M_{k^-}^+ \) and \( M_{k^+}^- / M_{k^-}^+ \cong M_k \).

(b) Let \( M = \bigoplus_{i \in I} M_i \). Then

(\( ba \)) \( \mathcal{C} := \{ M_J^+ \mid J \in J \in \text{Cut}(I) \} \) is an \( R \)-series on \( M \).

(\( bb \)) Jump(\( \mathcal{C} \)) = \{ (M_{k^+}^-, M_{k^+}^+) \mid k \in I \}.

(\( bc \)) \( \mathcal{C} \) an \( R \)-composition series if and only if each \( M_k, k \in I \) is a simple \( R \)-module.

(c) Let \( M = \prod_{i \in I} M_i \). Then

(\( ba \)) \( \mathcal{C} := \{ M_J^+, M_J^- \mid J \in J \in \text{Cut}(I) \} \) is an \( R \)-series on \( M \).

(\( bb \)) Jump(\( \mathcal{C} \)) := \{ (M_J^-, M_J^+) \mid \emptyset \neq J \in \text{Cut}(I) \}.

(\( bc \)) \( \mathcal{C} \) is an \( R \)-composition series if and only if each non-empty subset of \( I \) has a maximal element and each \( M_k, k \in I \) is a simple \( R \)-module.

**Proof:** (a) The first statement follows directly from the definitions. For the second note that the map \( M_{k^+}^- \rightarrow M_k, m \rightarrow m_k \) is onto with kernel \( M_{k^-}^+ \).

(b) & (c) Note that \( M_{j^-}^- \leq M_J^- \).

Let \( \text{Cut}^*(I) \) be the set of cuts without a maximal element. So

\[
\text{Cut}(I) = \{ k^+ \mid k \in K \} \cup \text{Cut}^*(I).
\]

Let \( J \in \text{Cut}^*(I) \). We claim that \( M_J^- = M_J^+ \) if \( M = \bigoplus_{i \in I} M_i \) and \( M_J^- \neq M_J^+ \) if \( M = \prod_{i \in I} M_i \).

So suppose first that \( M = \bigoplus_{i \in I} M_i \) and let \( 0 \neq m \in M_J^+ \) and pick \( k \in J \) maximal with \( m_k \neq 0 \) (this is possible as only finitely many \( m_i \)’s are not 0). Since \( J \) has no maximal element there exists \( j \in J \) with \( k < j \). Then \( m_i = 0 \) for all \( i \geq j \) and so \( m \in M_J^- \).

Suppose next that \( M = \prod_{i \in I} M_i \). For \( j \in J \) pick \( 0 \neq m_j \in M_j \). For \( i \in I \setminus J \) let \( m_i = 0 \). Then \( (m_i) \in M_J^+ \) but \( (m_i) \notin M_J^- \).
From the claim we conclude that in both cases
\[ \mathcal{C} := \{ M_J^+, M_J^- \mid J \in \text{Cut}(I) \} \]

We will show now that \( \mathcal{C} \) is a chain. For this let \( J \) and \( K \) be distinct cuts. Since \( \text{Cut}(I) \) is totally ordered we may assume \( J \subseteq K \). Then
\[ M_J^- \leq M_J^+ \leq M_K^- \leq M_K^+. \]
and so \( \mathcal{C} \) is totally ordered.

Also \( 0 = M_\emptyset^+ \) and \( M = M_I^+ \).

Let \( \mathcal{D} \) be a subset of \( \mathcal{C} \). We need to show that both \( \bigcap \mathcal{D} \) and \( \bigcup \mathcal{D} \) are in \( \mathcal{D} \). Let \( D \in \mathcal{D} \). Then \( D = M_J^{\epsilon_D} \) for some \( J_D \in \text{Cut}(I) \) and \( \epsilon_D \in \{\pm\} \).

Put \( J = \bigcap_{D \in \mathcal{D}} J_D \). Suppose first that \( M_J^- \in \mathcal{D} \).

Then \( M_J^- \subseteq D \) for all \( D \in \mathcal{D} \) and
\[ \bigcap \mathcal{D} = M_J^- . \]

So suppose that \( M_J^- \notin \mathcal{D} \). Then \( M_J^+ \leq D \) for all \( D \in \mathcal{D} \) and so \( M_J^+ \subseteq \bigcap \mathcal{D} \). We claim that
\[ \bigcap \mathcal{D} = M_J^+ . \]

Indeed, let \( m \in \bigcap \mathcal{D} \) and \( i \in I \setminus J \). Then \( i \notin J_D \) for some \( D \in \mathcal{D} \). As
\[ m \in D = M_J^{\epsilon_D} \leq M_J^{\epsilon_D} \]
we get \( m_i = 0 \). Thus \( m \in M_J^+ \), proving the claim.

So \( \mathcal{C} \) is closed under arbitrary unions.

Let \( K = \bigcup \{ J_D \mid D \in \mathcal{D} \} \).

Suppose that \( M_K^+ \in \mathcal{D} \). Then \( M \subseteq M_K^+ \) for all \( D \in \mathcal{D} \) and
\[ \bigcup \mathcal{D} = M_K^+ . \]

So suppose that \( M_K^+ \notin \mathcal{D} \). Then \( \bigcup \mathcal{D} \subseteq M_K^- \). We claim that
\[ \bigcup \mathcal{D} = M_K^- . \]

If \( K = \emptyset \) each \( J_D \) is the empty set. So we may assume \( K \neq \emptyset \). Let \( m \in M_K^- \). Then by definition there exists \( k \in K \) with \( m_i = 0 \) for all \( i \geq k \). Pick \( D \in \mathcal{D} \) with \( i \in J_D \). Then
\[ m \in M_J^{\epsilon_D} \leq M_J^{\epsilon_D} = D \leq \bigcup \mathcal{D} . \]
So the claim is true and \( \mathcal{C} \) is closed under unions.

Hence \( \mathcal{C} \) is an \( R \)-series on \( M \).
4.8. COMPOSITION SERIES

Next we investigate the jumps of \( \mathcal{C} \). As seen above every cut is of the form \((B^-, B)\) for some \( B = M_j \in \mathcal{C} \) with \( B \neq B^- \).

Suppose first that \( J = k^+ \) for \( k \in I \). As \( M_{k^-} = M_{k^+}^\epsilon \) we may and do assume \( \epsilon = + \). Thus \( M_{k^-} = M_{k^+}^\epsilon = (M_{k^+}^\epsilon)^- \) and \( M_{k^-}^\epsilon = M_{k^+}^\epsilon \) is a jump with factor isomorphic to \( M_k \).

Suppose next that \( J \in \text{Cut}^*(I) \). Then \( M_J = \bigcup_{j \in J} M_j^\epsilon \leq (M_J^\epsilon)^- \). We conclude that \( (M_J^\epsilon)^- = (M_J)^- \) if \( M = \bigoplus_{i \in I} M_i \) then as seen above \( M_J = M_J^\epsilon \). So we only get a jump if \( \epsilon = + \) and \( M = M = \prod_{i \in I} M_i \).

The factor \( M_J^\epsilon / M_J^- \) can be described as follows. Identify \( M_J^\epsilon \) with \( \prod_{j \in J} M_j^\epsilon \). Define \( x, y \in \prod_{j \in J} M_j^\epsilon \) to be equivalent if and only if there exists \( j \in J \) with \( x_i = y_i \) for all \( i \in J \) with \( j \leq i \). It is easy to check that this is an equivalence relation, indeed \( x \) and \( y \) are equivalent if and only if \( y - x \in M_J^- \). In particular, \( M_J^\epsilon / M_J^- \) is the set of equivalence classes. We claim that \( M_J^\epsilon / M_J^- \) is never a simple module. For this let \( J = J_1 \cup J_2 \) with \( J_1 \cap J_2 = \emptyset \) so that for each \( j_1 \in J_1 \) there exists \( j_2 \in J_2 \) with \( j_1 < j_2 \), and vice versa. (We leave the existence of \( J_1 \) and \( J_2 \) as an exercise.) Then \( M_J^\epsilon / M_J^- \) is the direct sum of the images of \( \prod_{j \in J} M_j^\epsilon \) in \( M_J^\epsilon / M_J^- \).

Finally we claim that every non-empty subset of \( I \) has a maximal element if and only if every non-empty cut of \( I \) has a maximal element. One direction is obvious. For the other let \( J \) be a non-empty subset of \( I \) and define \( J^* = \{ i \in I \mid i \leq j \text{ for some } j \in J \} \). Clearly \( J^* \) is a cut and \( J \subseteq J^* \). Suppose \( J^* \) has a maximal element \( k \). Then \( k \leq j \) for some \( j \in J \). As \( j \in J^* \) we conclude \( j \leq k \) and so \( j = k \) and \( k \) is the maximal element of \( J \).

It is now easy to see that (bc) and (cc) hold and all parts of the lemma are proved. \( \Box \)

**Corollary 4.8.6** [serfree] Let \( R \) be a ring and \( I \) a set. Let \( M \) be one of \( F_R(I) \) and \( R^I \). Then there exists an \( R \)-series \( \mathcal{C} \) of \( M \) so that all factors of \( \mathcal{C} \) are isomorphic to \( R \) and \( |\text{Jump}(\mathcal{C})| = |I| \). Moreover, if \( R \) is a division ring \( \mathcal{C} \) is a composition series.

**Proof:** By the well-ordering principal A.5 there exists a well ordering \( \leq^* \) be a well ordering on \( I \). Define a partial order \( \leq \) on \( I \) by \( i \leq j \) if and only if \( j \leq^* i \). Then every non-empty subset of \( I \) has a maximal element and all non empty cuts of \( I \) are of the form \( k^+ \), \( k \in K \).

The result now follows from 4.8.5 \( \Box \)

As an example let \( R = \mathbb{Q} \). If \( I = \mathbb{Q} \) we see that the countable vector space \( F_{\mathbb{Q}}(\mathbb{Q}) \) as an uncountable composition series. But note that the number of jumps is countable. If \( I = \mathbb{Z}^- \) we conclude that uncountable vector space \( \mathbb{Q}^{\mathbb{Z}^-} \) as a countable composition series. So the number of jumps in a composition series can be smaller than the dimensions of the vector space. But the next proposition shows that the number of jumps never exceeds the dimension.

**Proposition 4.8.7** [carcombas] Let \( \mathbb{D} \) be a division ring and \( V \) a vector space over \( \mathbb{D} \). Let \( \mathcal{C} \) be a \( \mathbb{D} \)-series on \( V \), and \( \mathcal{B} \) a \( \mathbb{D} \)-basis for \( V \). Then

\[ |\text{Jump}\mathcal{C}| \leq \mathcal{B}. \]

In particular, any two basis for \( V \) have the same cardinality.
CHAPTER 4. MODULES

Proof: Choose some well ordering on $B$. Let $0 \neq v \in V$. Then $v = \sum_{b \in B} d_b(v)b$ with $d_b(v) \in \mathbb{D}$, where almost all $d_b(v), b \in B$ are zero. So we can choose $h(v) \in B$ maximal with respect to $d_{h(v)}(v) \neq 0$.

Define a map

$$\phi: \text{Jump}(C) \to B$$

$$(A, B) \to \min\{h(v) \mid v \in A \setminus B\}$$

We claim that $\phi$ is one to one. Indeed suppose that $(A, B)$ and $(E, F)$ are distinct jumps with $b = \phi((A, B)) = \phi((E, F))$. As $C$ is totally ordered and $(A, B)$ and $(E, F)$ are jumps we may assume $A \leq B \leq E \leq F$. Let $v \in B \setminus A$ with $h(v) = b$ and $d_b(v) = 1$. Let $w \in F \setminus E$ with $h(w) = b$ and $d_b(w) = 1$. Since $v \in A \leq E, w-v \in F \setminus E$. Also $d_b(w-v) = 1 - 1 = 0$ and so $h(w-v) < b$ a contradiction to $b = \phi(E, F)$.

So $\phi$ is one to one and $|\text{Jump}(C)| \leq |B|$.

The second statement follows from the first and 4.8.6

Lemma 4.8.8 [findjumps] Let $C$ be a series for $R$ on $M$.

(a) Let $0 \neq m \in M$. Then there exists a unique jump $(A, B)$ of $C$ with $m \in B$ and $m \not\in A$.

(b) Let $D, E \in C$ with $D < E$. Then there exists a jump $(A, B)$ in $C$ with

$$D \leq A < B \leq E$$

Proof: (a) Let $B = \bigcap\{C \in C \mid m \in C\}$ and $A = \bigcup\{C \in C \mid m \not\in C\}$.

(b) Let $m \in E \setminus D$ and let $(A, B)$ be as in (a).

The following lemma shows how a series can be reconstructed from its jumps.

Lemma 4.8.9 [sertojumps] Let $R$ be a ring, $M$ an $R$-module and $C$ an $R$-series on $M$. Let $\hat{C} = \{C \in C \mid C \neq C^-\}$. Then the map

$$\alpha: \text{Cut}(\hat{C}) \to C, K \to \bigcup K$$

is a bijection.

Proof: Note first that as $C$ is closed under unions $\alpha(K)$ is indeed in $C$. We will show that the inverse of $\alpha$ is

$$\beta: C \to \text{Cut}(\hat{C}), D \to \{A \in \hat{C} \mid A \leq D\}$$

It is easy to verify that $\beta(D)$ is a cut.

Clearly, $K \subseteq \beta(\alpha(K))$. Let $E \in \hat{C}$ with $E \not\in K$. Then as $K$ is a cut, $A < E$ for all $A \in K$. But then $A \leq E^-$ and so $\alpha(K) \leq E^- < E$. Thus $E \not\in \alpha(K)$ and $E \not\in \beta(\alpha(K))$.

Hence $\beta(\alpha(K)) = K$. 
Clearly \( \alpha(\beta(D)) \leq D \). Suppose that \( \alpha(\beta(D)) < D \). Then by 4.8.8b there exists a jump \((A, B)\) of \( C \) with \( \alpha(\beta(D)) \leq A < B \leq D \). But then \( B \in \beta(D) \) and so \( B \leq \alpha(\beta(D)) \), a contradiction. \( \Box \)

**Lemma 4.8.10 [intcompser]** Let \( C \) be a series for \( R \) on \( M \) and \( W \) an \( R \)-submodule in \( M \). Then

(a) \[
C \cap W := \{ D \cap W \mid D \in C \}
\]

is an \( R \)-series on \( M \).

(b) Let \[
\text{Jump}^W(C) = \{ (A, B) \in \text{Jump}(C) \mid A \cap W \neq B \cap W \}.
\]

Then the map \[
\text{Jump}^W(C) \to \text{Jump}(C) \cap W, \quad (A, B) \to (A \cap W, B \cap W)
\]
is a bijection. Moreover,
\[
B \cap W/A \cap W \cong (B \cap W) + A/A \leq B/A
\]

(c) If \( C \) is a \( R \)-composition series on \( M \) then \( C \cap W \) is a \( R \)-composition series on \( W \). Moreover, there exists an embedding \( \phi : \text{Jump}(C \cap W) \to \text{Jump}(C) \), so that corresponding factors are \( R \)-isomorphic. The image of \( \phi \) consists of all the jumps \((A, B)\) of \( C \) with \( B = A + (B \cap W) \).

**Proof:** (a) Clearly \( C \cap W \) is a chain of \( R \)-submodules in \( W \). Also \( 0 = 0 \cap W \in C \cap W \), \( W = M \cap W \in C \cap W \) and it is easy to verify that \( M \cap W \) is closed under unions and intersections.

(b) Let \((A, B) \in \text{Jump}^W(C)\). We will first verify that \((A \cap W, B \cap W)\) is a jump of \( C \cap W \). Let \( D \in C \cap W \). Then \( D = E \cap W \) for some \( E \in C \). As \((A, B)\) is a jump, \( E \leq A \) or \( B \leq E \). Thus \( D = E \cap W \leq A \cap W \) or \( B \cap W \leq E \cap W = D \). To show that the map is bijective we will construct its inverse. For \( D \in C \cap W \) define
\[
D^- = \bigcup \{ C \in C \mid C \cap W \leq D \} \quad \text{and} \quad D^+ = \bigcap \{ C \in C \mid D \leq C \cap W \}.
\]

Then it easy to verify that \( D^+ \cap W = D = D^- \cap W \). Let \((D, E)\) be a jump in \( C \cap W \). Let \( C \in C \). Since \((D, E)\) is a jump in \( C \cap W \), \( C \cap W \leq D \) or \( E \leq C \cap W \). In the first case \( C \leq D^+ \) and in the second \( E^+ \leq C \). So \((D^+, E^-)\) is a jump of \( C \). It is readily verified that maps \((D, E) \to (D^+, E^-)\) is inverse to the map \((A, B) \to (A \cap W, B \cap W)\).

The last statement in (b) follows from
\[
B \cap W/A \cap W = (B \cap W)/(B \cap W) \cap A \cong (B \cap W + A)/A.
\]
(c) Note that $A \cap W \neq B \cap W$ if and only if $(B \cap W) + A/A \neq 0$. Since $C$ is a composition series, $B/A$ is simple. Thus $(B \cap W) + A/A \neq 0$ if and only if $B = (B \cap W) + A$. Thus by (b) all factors of $C \cap W$ are simple and $C \cap W$ is a $R$-composition series on $W$. \hfill \Box

**Theorem 4.8.11 (Jordan-Hölder)** [jorhol] Let $R$ be a ring and $M$ a module. Suppose $R$ has a finite composition series $C$ on $M$ and that $D$ is any composition series for $R$ on $M$. Then $D$ is finite and there exists a bijection between the set of factors of $C$ and the set of factors of $D$ sending a factor of $C$ to an $R$-isomorphic factor of $D$.

**Proof:** Let $W$ be the maximal element of $D - M$. Then $D - M$ and (by 4.8.10) $C \cap W$ are composition series for $W$. By induction on $|D|$, $D \cap W$ is finite and has the same factors as $D - M$.

For $E \in C \cap W$ define $E^+$ and $E^-$ as in 4.8.10. Let $\text{cal}E = \{E^+, E^- \mid E \in D \cap W\}$. Then $E$ is a finite series on $M$. Since $W^+ = M \n W$ we can choose $L \in E$ minimal with respect to $L \n W$. Then $L = E^\epsilon$ for some $E \in C \cap W$ and $\epsilon \in \{\pm\}$. Suppose first that $L = E^-$. Since $0^- = 0 \leq W$, $E \neq 0$ and so there exists $F \in C \cap W$ such that $(F, E)$ is a jump in $C \cap W$. But then $(F^+, E^-) \in \text{Jump}^W(C)$, $F^+ \leq W$ and by 4.8.10c, $E^- = F^+ + (E^- \cap W) \leq W$ a contradiction. So $E^+ = L \neq E^-$. By 4.8.8b there exists a jump $(A, B)$ of $C$ with $E^- \leq A < B \leq E^+$. Then $E = E^- \cap W \leq A \cap W \leq B \cap W \leq E^+ \cap W = E$ and so $E = A \cap W = B \cap W$. So by definition (see 4.8.8b), $(A, B) \notin \text{Jump}^W(C)$. Also $B \n W$ and so as $M/W$ is simple, $M = B + W$. If $A \n W$, then also $M = A + W$ and $B = B \cap M = B \cap (A + W) = A + (B \cap W) \leq A$ a contradiction. Hence $A \leq W$ and $A = B \cap W$. Thus

$$B/A = B/B \cap W \cong B + W/W = M/W$$

We claim that $\text{Jump}(C) = \text{Jump}^W(C) \cup \{(A, B)\}$. So let $(X, Y)$ be a jump of $C$ not contained in $\text{Jump}^W(C)$. By 4.8.10c, $Y \n X + (Y \cap W)$ and so also $Y \n X + W$. Thus $Y \n W$ and $X \leq W$. As $A \leq W$, $Y \n A$. As $(A, B)$ is a jump $B \leq Y$. As $B \n W$, $B \n X$ and so $X \leq A$. Thus $X \leq A < B \leq Y$ and as $(X, Y)$ is a jump, $(A, B) = (X, Y)$.

By 4.8.10c, the factors of $\text{Jump}^W(C)$ are isomorphic to the factors of $C \cap W$ and so with the factors of $D - M$. As $B/A \cong M/W$ it only remains to show that $D$ is finite. But thus follows from 4.8.9. \hfill \Box

### 4.9 Matrices

Let $R$ be a ring and $I, J$ sets. Define

$$\mathcal{M}_R(I, J) = \{(m_{ij})_{i \in I, j \in J} \mid m_{ij} \in R\}$$

$M = (m_{ij})_{i \in I, j \in J}$ is called an $I \times J$-matrix over $R$. For $j \in J$, put $M^j = (m_{ij})_{i \in I}$, $M^j \in R^I$ is called the $j$'th column of $M$. For $i \in I$ put $M_i = (m_{ij})_{j \in J}$, $M_i$ is called the $i$'th row of
4.9. MATRICES

Note that as abelian groups, \( \mathcal{M}_R(I, J) \cong R^{I \times J} \). Define

\[
\mathcal{M}'_R(I, J) = \{ M \in \mathcal{M}_R(I, J) \mid \forall j \in J, \{i \in I, m_{ij} \neq 0\} \text{ is finite} \}
\]

Let \( M \in \mathcal{M}_R(I, J) \). Then \( M \in \mathcal{M}'_R(I, J) \) if and only if each column of \( M \) lies in \( \bigoplus_j R \).

If \( I, J, K \) are sets we define a multiplication

\[
\mathcal{M}_c(I, J) \times \mathcal{M}_c(J, K) \to \mathcal{M}_c(I, K)
\]

by

\[
(a_{ij})(b_{jk}) = \left( \sum_{j \in J} a_{ij}b_{jk} \right)_{i \in I, k \in K}
\]

Fix \( k \in K \). Then there exists only finitely \( j \in J \) with \( b_{jk} \neq 0 \), so the above sum is well defined. Also for each of these \( j \)'s there are only finitely many \( i \in I \) for which \( a_{ij} \) is not 0. Hence there exists only finitely many \( i \)'s for which \( \sum_{j \in J} a_{ij}b_{jk} \) is not 0. So \( (a_{ij})(b_{jk}) \in \mathcal{M}'_R(I, K) \).

Put \( \mathcal{M}_R(I) = \mathcal{M}_R(I, I) \) and \( \mathcal{M}'_R(I) = \mathcal{M}'_R(I, I) \).

**Lemma 4.9.1 [matmap]** Let \( R \) be a ring and \( V, W, Z \) free \( R \)-modules with bases \( I, J \) and \( K \), respectively.

(a) Define \( m_A(j, i) \in R \) by \( A(i) = \sum_{j \in J} m_A(i, j)j \) and put \( M_A(J, I) = (m_A(j, i)) \). Then the map

\[
M(J, I) : \text{Hom}_R(V, W) \to \mathcal{M}'_{R^{op}}(J, I)
\]

\[
A \to M_A(J, I)
\]

is an isomorphism of abelian groups.

(b) Let \( A \in \text{Hom}_R(V, W) \) and \( B \in \text{Hom}_R(W, Z) \). Then

\[
M_B(K, J)M_A(J, I) = M_{BA}(K, I).
\]

(c) Let \( M(I) := M(I, I) \). Then \( M(I) : \text{End}_R(V) \to \mathcal{M}'_{R^{op}}(I) \) is ring isomorphism.

**Proof:**

(a) Note first that as \( J \) is a basis of \( W \), the \( m_A(j, i) \)'s are well defined. To show that \( M_A(J, I) \) is a bijection we determine it inverse. Let \( M = (m_{ji}) \in \mathcal{M}_{R^{op}}(J, I) \). Define \( A_M \in \text{Hom}_R(V, W) \) by

\[
A_M(\sum_{i \in I} r_i j) = \sum_{j \in J} \left( \sum_{i \in I} r_i m_{ji} \right) j
\]

It is easy to check that \( A_M \) is \( R \)-linear and that the map \( M \to A_M \) is inverse to \( M_A(J, I) \).

(b) \( (BA)(i) = B(A(i)) = B(\sum_{j \in J} m_A(j, i)j) = \sum_{j \in J} m_A(j, i)B(j) = \)
\[
\sum_{j \in J} m_A(j, i) (\sum_{k \in K} m_B(k, j)k) = \sum_{k \in K} (\sum_{j \in J} m_A(j, i)m_B(k, j)) k
\]

Thus
\[
m_{BA}(k, i) = \sum_{j \in J} m_A(j, i)m_B(k, j) = \sum_{j \in J} m_B(k, j)^{op} m_A(j, i)
\]

So (b) holds.
(c) Follows from (b) and (c).

Definition 4.9.2 Let \( R \) be a ring, \( V \) and \( W \) \( R \)-modules, \( A \in \text{End}_R(V) \) and \( B \in \text{End}_R(W) \). We say that \( A \) and \( B \) are similar over \( R \) if there exists a \( R \)-linear isomorphism \( \Phi : V \to W \) with \( \Phi \circ A = B \circ \Phi \).

We leave it as an exercise to show that "similar" is an equivalence relation. Also the condition \( \Phi \circ A = B \circ \Phi \) is equivalent to \( B = \Phi \circ A \circ \Phi^{-1} \).

Let \( I \) and \( J \) be sets and \( \phi : I \to J \) a function. If \( M = (m_{ij}) \) is a \( J \times J \) matrix, let \( M^\phi \) be the \( I \times I \) matrix \((m_{\phi(i)\phi(j)})\).

Lemma 4.9.3 Let \( R \) be a ring, \( V \) and \( W \) \( R \)-modules, \( A \in \text{End}_R(V) \) and \( B \in \text{End}_K(V) \). Suppose that \( V \) is free with basis \( I \). Then \( A \) and \( B \) are similar if and only if there exists a basis \( J \) for \( W \) and a bijection \( \phi : I \to J \) with
\[
M_A(I) = M_B^\phi(J)
\]

Proof: Suppose first that \( A \) and \( B \) are similar. Then there exists an \( R \)-linear isomorphism \( \Phi : V \to W \) with \( \Phi \circ A = B \circ \Phi \). Let \( J = \Phi(I) \). As \( I \) is a basis for \( V \) and \( \Phi \) is an isomorphism, \( J \) is a basis for \( W \). Let \( \phi = \Phi \mid_I \). We compute
\[
B(\phi(i)) = \Phi(A(i)) = \Phi(\sum_{i \in I} M_A(\hat{i}, \tilde{i})i) = \sum_{i \in I} M_A(\hat{i}, \tilde{i})\phi(i)
\]

Hence \( M_B(\phi(\hat{i}), \phi(\tilde{i})) = M_A(\hat{i}, \tilde{i}) \) and \( M_A(I) = M_B^\phi(J) \).

Suppose conversely that there exist a basis \( J \) for \( W \) and a bijection \( \phi : I \to J \) with \( M_A(I) = M_B^\phi(J) \). Then \( m_A(\hat{i}, i) = m_B(\phi(\hat{i}), \phi(i)) \).

Let \( \Phi : V \to W \) be the unique \( R \)-linear map from \( V \) to \( W \) with \( \Phi(i) = \phi(i) \) for all \( i \in I \). As \( I \) and \( J \) are bases, \( \Phi \) is an isomorphism. Moreover,
\[
\Phi(A(i)) = \Phi(\sum_{\hat{i} \in I} M_A(\hat{i}, \tilde{i})\hat{i}) = \sum_{\hat{i} \in I} m_A(\hat{i}, \tilde{i})\phi(\hat{i}) = \sum_{\hat{i} \in I} m_B(\phi(\hat{i}), \phi(i))\phi(\hat{i}) = \sum_{\tilde{j} \in J} m_B(j, \phi(i))\tilde{j} = B(\phi(i))
\]

Hence \( \Phi \circ A \) and \( B \circ \Phi \) agree on \( I \) and so \( \Phi \circ A = B \circ \Phi \).
Let \( R \) be a ring and \( V \) a module over \( R \). Let \( A \in \text{End}_R(V) \). Define \( \alpha : R \to \text{End}_\mathbb{Z}(V) \) by \( \alpha(r)v = rv \); we will usually right \( \text{id}_V \) for \( \alpha(r) \). Note that \( A \) commutes with each \( \text{id}_V \) and so by 3.5.1 there exists a ring homomorphism \( \alpha_A : \mathbb{R}[x] \to \text{End}_\mathbb{Z}(V) \) with \( r \mapsto \text{id}_V \) and \( x \mapsto A \). Let \( f = \sum_{i=0}^n r_i x^i \in \mathbb{R}[x] \). We will write \( f(A) \) for \( \alpha_A(f) \). Then \( f(A) = \sum_{i=0}^n r_i A^i \).

It follows that \( V \) is a \( \mathbb{R}[x] \)-module with

\[
v \cdot f = f(A)(v) = \sum_{i=0}^n r_i A^i(v)
\]

To indicate the dependence on \( A \) we will sometimes write \( V_A \) for the \( \mathbb{R}[x] \) module \( V \) obtain in this way.

**Lemma 4.9.4** [issim] Let \( R \) be a ring and \( V \) and \( W \) \( R \)-modules. Let \( A \in \text{End}_R(V) \) and \( B \in \text{End}_R(V) \). Then the \( \mathbb{R}[x] \)-modules \( V_A \) and \( W_B \) are isomorphic if and only if \( A \) and \( B \) are similar over \( R \).

**Proof:** Suppose first that \( V_A \) and \( V_B \) are isomorphic. Then there exists an \( \mathbb{R}[x] \)-linear isomorphism \( \Phi : V \to W \). In particular \( \Phi \) is \( R \)-linear and \( \Phi(xv) = x\Phi(v) \) for all \( v \in V \). By definition of \( V_A \) and \( W_B \) thus means \( \Phi(A(v)) = B(\Phi(v)) \) and so \( A \) and \( B \) and are similar.

Conversely, if \( A \) and \( B \) are similar there exists an \( R \)-linear isomorphism \( \Phi : V \to W \) with \( \Phi \circ A = B \circ \Phi \). Hence \( \Phi(rv) = r\Phi(v) \) and \( \Phi(xv) = x\Phi(v) \) for all \( r \in R \) and \( v \in V \). Since \( \Phi \) is \( \mathbb{Z} \)-linear this implies \( \Phi(fv) = f\Phi(v) \) for all \( f \in \mathbb{R}[x] \). Hence \( \Phi \) is an \( \mathbb{R}[x] \)-linear isomorphism.

**Lemma 4.9.5** [baspolring] Let \( R \) be a ring and \( f = \sum_{i=0}^n a_i x^i \) a monic polynomial of degree \( n > 0 \). Let \( I = \mathbb{R}[x]f \) be the left ideal in \( \mathbb{R}[x] \) generated by \( f \).

(a) \( \{x^i \mid i \in \mathbb{N}\} \) is a basis for \( \mathbb{R}[x] \) as a left \( R \)-module.

(b) For \( 0 \leq i < n \) let \( h_i \) be a monic polynomial of degree \( i \). Then \( \{h_i + I \mid 0 \leq i < n\} \) is basis for \( \mathbb{R}[x]/I \).

(c) Let \( A \in \text{End}_{\mathbb{R}}(\mathbb{R}[x]/I) \) be defined by \( A(h + I) = hx + I \).

(\( \text{ca} \)) The matrix of \( A \) with respect the basis

\[
1 + I, x + I, \ldots x^{n-1} + I
\]

is

\[
M(f) := \begin{pmatrix}
0 & 0 & 0 & \ldots & 0 & -a_0 \\
1 & 0 & 0 & \ldots & 0 & -a_1 \\
0 & 1 & 0 & \ldots & 0 & -a_2 \\
0 & 0 & 1 & \ldots & 0 & -a_3 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & -a_{n-2} \\
0 & 0 & 0 & \ldots & 0 & -a_{n-1}
\end{pmatrix}
\]
Theorem 4.6.1 (cb) Suppose that \( f = g^m \) for some monic polynomial \( g \) of degree \( s \) and some \( m \in \mathbb{Z}^+ \). Let \( E_1^s \) be the matrix \( k \times k \) with \( e_{ij} = 0 \) if \( (i, j) \neq (1, s) \) and \( e_{1s} = 1 \). Then the matrix of \( A \) with respect to the basis

\[
1 + I, x + I, \ldots, x^{s-1} + I, xg + I, \ldots, x^{m-1} + I, xg^{m-1} + I, x^{s-1}g^{m-1} + I,
\]

has the form

\[
M(g, m) := \begin{pmatrix}
M(g) & 0 & 0 & \ldots & 0 & 0 & 0 \\
E_1^s & M(g) & 0 & \ddots & 0 & 0 & 0 \\
0 & E_1^s & M(g) & \ddots & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \ddots & M(g) & 0 & 0 \\
0 & 0 & 0 & \ddots & E_1^s & M(g) & 0 \\
0 & 0 & 0 & \ddots & 0 & E_1^s & M(g)
\end{pmatrix}
\]

Proof: (a) is obvious as any polynomial can be uniquely written as \( R \)-linear combination of the \( x^i \).

(b) We will first show by induction on \( \deg h \) that every \( h + I, h \in R[x] \) is a \( R \) linear combination of the \( h_i, 0 \leq i < n \). By 3.6.4 \( h = qf + r \) for some \( q, r \in R[x] \) with \( \deg r < \deg f = n \). Since \( h + I = r + I \) we may assume that \( h = r \) and so \( i := \deg h < n \). Let \( a \) be the leading coefficient of \( h \). Then \( \deg h - ah_i < \deg h \) and so by induction is a linear combination of the \( h_i \)'s.

Suppose now that \( \sum_{i=0}^{n-1} \lambda_i(h_i + I) = 0 + I \) for some \( \lambda_i \in \mathbb{K} \), not all 0. Then \( h := \sum_{i=0}^{n-1} \lambda_i h_i \in I \). Let \( j \) be maximal with \( \lambda_j \neq 0 \). Then clearly \( j = \deg h \) and the leading coefficient of \( h \) is \( \lambda_j \). In particular \( h \neq 0 \).

Note that all non-zero polynomials in \( I \) have degree larger or equal to \( n \). But this contradicts \( 0 \neq h \in I \) and \( \deg h = j < n \). Thus (b) holds.

(ca) is the special case \( g = f \) and \( m = 1 \) of (cb). So it remains to prove (cb). Note that \( \deg x^i g^j = i + js \). Hence by (b) \( \{ x^i g^j + I \mid 0 \leq i < s, 0 \leq j < m \} \) is a basis for \( R[x]/I \).

Let \( y_{i,j} := x^i g^j + I \). Then

\[
A(y_{i,j}) = x^{i+1} g^j + I.
\]

Thus

\[
A(y_{i,j}) = y_{i+1,j} \text{ for all } 0 \leq i < s - 1, 0 \leq j < m.
\]

Let \( g = \sum_{i=0}^{s-1} b_i x^i \). As \( g \) is monic \( b_s = 1 \) and so \( x^s = g - \sum_{i=0}^{s-1} b_i x^i \).

Hence

\[
A(y_{s-1,j}) = x^s g^j + I = (g^{i+1} + \sum_{i=0}^{s-1} b_i x^i g^j) + I = (g^{i+1} + I) - \sum_{i=0}^{s-1} b_i y_{i,j}.
\]
If \( j < m - 1 \), \( g^{j+1} + I = y_{0,j+1} \) and so
\[
A(y_{s-1,j}) = y_{0,j+1} - \sum_{i=0}^{s-1} b_i y_{i,j}
\]

If \( j = m - 1 \) then \( g^{j+1} = g^m = f \in I \) and so
\[
A(y_{s-1,m-1}) = -\sum_{i=0}^{s-1} b_i y_{s-1,m-1}
\]

Thus (cb) holds.

**Theorem 4.9.6 (Jordan Canonical Form)**

Let \( \mathbb{k} \) be a field, \( V \) a non-zero finite dimensional vector space over \( \mathbb{k} \) and \( A \in \text{End}_\mathbb{k}(V) \). Then there exist irreducible monic polynomials \( f_1, \ldots, f_t \in \mathbb{k}[x] \), positive integers \( m_1, \ldots, m_t \) and a basis \( y_{ijk}, 0 \leq i < \deg f_k, 0 \leq j < m_k, 1 \leq k \leq t \) of \( V \) so that the matrix of \( A \) with respect to this basis has the form
\[
M(f_1, m_1 | \ldots | f_t, m_t) := \begin{pmatrix}
M(f_1, m_1) & 0 & \ldots & 0 & 0 \\
0 & M(f_2, m_2) & \ddots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \ddots & M(f_{t-1}, m_{t-1}) & 0 \\
0 & 0 & \ldots & 0 & M(f_t, m_t)
\end{pmatrix}
\]

**Proof:** View \( V \) as a \( \mathbb{k}[x] \)-module by \( f v = f(A)(v) \) for all \( f \in \mathbb{k}[x] \) and \( v \in V \) (see before 4.9.4). Since \( \mathbb{k}[x] \) is a PID (3.3.14) we can use Theorem 4.7.3. Thus \( V_A \) is the direct sum of modules \( V_k, 1 \leq k \leq t \) with \( V_k \cong \mathbb{k}[x]/(f_k^{m_k}) \), where \( f_k \in \mathbb{k}[x] \) is either 0 or prime, and \( m_k \in \mathbb{Z}^+ \). By 4.9.5(a) \( \mathbb{k}[x] \) is infinite dimensional over \( \mathbb{k} \). As \( V \) is finite dimensional, \( f_k \neq 0 \). So we may choose \( f_k \) to be irreducible and monic. By 4.9.5(cb), \( V_k \) has a basis \( y_{ijk}, 0 \leq i < \deg f_k, 0 \leq j < m_k \) so that the matrix of \( A \mid V_k \) with respect to this basis is \( M(f_k, m_k) \). Combining the basis for \( V_k, 1 \leq k \leq t \), to a basis for \( V \) we see that the theorem is true. \( \square \)

The matrix \( M(f_1, m_1 | f_2, m_2 | \ldots | f_t, m_t) \) from the previous theorem is called the **Jordan canonical form** of \( A \). We should remark that our notion of the Jordan canonical form differs slightly from the notion found in most linear algebra books. It differs as we do not assume that all the roots of the minimal polynomial (see below) of \( A \) are in \( \mathbb{k} \). Note that if \( \mathbb{k} \) contains all the roots then \( f_k = x - \lambda_k \) and \( M(f_k) \) is the \( 1 \times 1 \) matrix \( (\lambda_k) \) and \( E^{1s} \) is the \( 1 \times 1 \) identity matrix. So the obtain the usual Jordan canonical form.
We remark that the pairs \((f_k, m_k), 1 \leq k \leq t\) are unique up to ordering. Indeed let \(f\) be an irreducible monic polynomial of degree \(s\) and \(m\) a positive integer. Then the number of \(k\)'s with \((f_k, m_k) = (f, m)\) is \(\frac{d}{s}\) where \(d\) is the dimension of the \(\mathbb{K}\)-space 

\[ \ker f^m(A)/\ker f^m(A) \cap \text{Im } f(A) \]

We leave the details of this computation to the dedicated reader.

The following two polynomials are useful to compute the Jordan canonical form of \(A\). The \textit{minimal polynomial} \(m_A\) and the \textit{characteristic polynomial} \(\chi_A\).

\(m_A\) is defined has the monic polynomial of minimal degree with \(m_A(A) = 0\). i.e \(m_A\) is monic and \((m_A)\) is the kernel of the homomorphism \(\alpha_A : \mathbb{K}[x] \to \text{End}_\mathbb{K}(V)\). \(m_A\) can be computed from the Jordan canonical form. For each monic irreducible polynomial let \(\epsilon_f\) be maximal so that \((f, \epsilon_f)\) is one of the \((f_k, m_k)\) ( with \(\epsilon_f = 0\) if \(f\) is not one of the \(f_k\). ) Then

\[ m_A = \prod f^{\epsilon_f} \]

The characteristic polynomial is defined as

\[ \chi_A = (-1)^n f_1^{m_1} f_2^{m_2} \cdots f_k^{m_k} \]

where \(n\) is the dimension of \(V\). The importance of the characteristic polynomials comes from the fact that \(\chi_A\) can be computed without knowledge of \(f_k\)'s. Indeed

\[ \chi_A = \det(A - x\text{id}_V). \]

To see this we use the Jordan canonical form of \(f\). Note that

\[ \det(A - x\text{id}_V) = \prod_{k=1}^{t} \det(M(f_k, m_k) - xI) \]

and

\[ \det(M(f, m) - xI) = (\det(M(f) - xI))^n. \]

Finally it is easy to verify that

\[ \det(M(f) - xI) = (-1)^{\deg f} f. \]
Chapter 5

Fields

5.1 Extensions

Let $\mathbb{K}$ be a field. An extension of $\mathbb{K}$ is an integral domain $L$ with $\mathbb{K} \leq L$. We denote such an extension by $L : \mathbb{K}$. If in addition $L$ is a field, we say that $L : \mathbb{K}$ is a field extension. Note that $L$ is a vector space over $\mathbb{K}$. Define $[L : \mathbb{K}] = \dim_\mathbb{K} L$. $[L : \mathbb{K}]$ is called the degree of $L$ over $\mathbb{K}$. If $[L : \mathbb{K}]$ is finite, $L : \mathbb{K}$ is called a finite extension. If $I \subseteq L$ then $\mathbb{K}[I]$ denotes the subring of $L$ generated by $\mathbb{K}$ and $I$. If $L$ is a field then $\mathbb{K}(I)$ denotes the subfield of $L$ generated by $\mathbb{K}$ and $I$.

Note that $L$ is a vector space over $\mathbb{K}$. Define $[L : \mathbb{K}] = \dim_\mathbb{K} L$. $[L : \mathbb{K}]$ is called the degree of $L$ over $\mathbb{K}$. If $[L : \mathbb{K}]$ is finite, $L : \mathbb{K}$ is called a finite extension. If $I \subseteq L$ then $\mathbb{K}[I]$ denotes the subring of $L$ generated by $\mathbb{K}$ and $I$. If $L$ is a field then $\mathbb{K}(I)$ denotes the subfield of $L$ generated by $\mathbb{K}$ and $I$.

Note that we used the symbol $\mathbb{K}[I]$ also to denote the polynomial ring in the variables $I$. To avoid confusion we will from now denote polynomials ring by $\mathbb{K}[x_i, i \in I]$. The field of fraction of $\mathbb{K}[x_i, i \in I]$ is denoted by $\mathbb{K}(x_i, i \in I)$.

Lemma 5.1.1 [baseext] Let $\mathbb{K}$ be a field and $L : \mathbb{K}$ an extension. Let $a \in L$ and let $\Phi_a$ be the unique ring-homomorphism $\Phi_a : \mathbb{K}[x] \to \mathbb{K}[a]$, with $x \to a$ and $k \to k \forall k \in \mathbb{K}$.

Also let $\ker \Phi_a = (m_a^\mathbb{K})$ with $m_a^\mathbb{K} = 0$ or monic. The one of the following holds

1. $\Phi_a$ is an isomorphism, $[\mathbb{K}[a] : \mathbb{K}] = \infty$, $m_a^\mathbb{K} = 0$ and $(a^i, 0 \leq i < \infty)$ is a basis for $\mathbb{K}[a]$.

2. $\Phi_a$ is not one to one, $[\mathbb{K}[a] : \mathbb{K}] = \deg m_a$ is finite, $m_a^\mathbb{K}$ is irreducible, $\mathbb{K}[a]$ is a field and $(a^i, 0 \leq i < \deg m_a^\mathbb{K})$ is a basis for $\mathbb{K}[a]$.

Proof: Let $m_a = M_a^\mathbb{K}$. Since $L$ is an integral domain, $\mathbb{K}[a]$ is an integral domain. Since $\mathbb{K}[x]/(m_a) \cong \mathbb{K}[a]$, $(m_a)$ is a prime ideal. Hence $m_a = 0$ or $m_a$ is a prime. If $m_a = 0$, (1) holds. Suppose that $m_a \neq 0$. Let $f \in \mathbb{K}[x]$. As $\mathbb{K}[x]$ a Euclidean domain, $f \equiv g \pmod{m_a}$ for some $g \in \mathbb{K}[x]$ with $\deg g < \deg m_a$. Also if $g, h$ are polynomials of degree less than $\deg m_a$ and $g \equiv h \pmod{m_a}$ then $g = h$. Hence $(a^i, 0 \leq i < \deg m_a)$ is basis for $\mathbb{K}[a]$. 

143
Note that $m_a$ is a prime ideal and $\mathbb{K}[x]$ is a PID. So by 3.3.6, $\mathbb{K}[a]/(m_a)$ is a field. Thus 2. holds. □

The polynomial $m|\mathbb{K}a$ from the previous theorem is called the minimal polynomial of $a$ over $\mathbb{K}$. If $m^\mathbb{K}_a \neq 0$, then $a$ is called algebraic over $\mathbb{K}$. In this case $m^\mathbb{K}_a$ is the monic, irreducible polynomial of minimal degree with respect to $m^\mathbb{K}_a(a) = 0$. We say that $L: \mathbb{K}$ is algebraic if all $a \in L$ are algebraic over $\mathbb{K}$. In this case $m^{\mathbb{K}}_K a$ is the monic, irreducible polynomial of minimal degree with respect to $m^{\mathbb{K}}_a(a) = 0$. We say that $L: \mathbb{K}$ is algebraic if all $a \in L$ are algebraic over $\mathbb{K}$. Note that if $a$ is algebraic over $\mathbb{K}$, $\mathbb{K}[a]$ is a field and so $a$ is invertible in $L$. So any algebraic extension is a field extension. Also by the previous theorem any finite extension is algebraic and so a field extension. Note that every finite integral domain is a finite extension of some $\mathbb{Z}/p\mathbb{Z}$. So we obtain a second proof that every finite integral domain is a field (cf. 3.1.4).

If $a$ (resp. $L$) is not algebraic over $\mathbb{K}$ we say that $a$ (resp. $L$) is transcendental over $\mathbb{K}$.

**Lemma 5.1.2 [finitecover]**

(a) Let $\mathbb{K}$ be a field, $L : \mathbb{K}$ an extension and $I \subseteq L$. Then

$$K[I] = \bigcup \{\mathbb{K}[J] \mid J \subseteq I, J \text{ is finite}\}.$$ 

(b) Let $\mathbb{K}$ be a field, $L : \mathbb{K}$ a field extension and $I \subseteq L$. Then

$$K(I) = \bigcup \{\mathbb{K}(J) \mid J \subseteq I, J \text{ is finite}\}.$$ 

**Proof:** (a) Let $R = \bigcup \{\mathbb{K}[J] \mid J \subseteq I, J \text{ is finite}\}$. Clearly $\mathbb{K} \cup I \subseteq R \subseteq \mathbb{K}[I]$ and we just need to verify that $R$ is a subring of $L$. For this let $r_1, r_2 \in R$. Then $r_i \in \mathbb{K}[J_i]$ for some finite subset $J_i$ of $I$. Then $r_1 \pm r_2$, and $r_1 r_2$ all are contained in $\mathbb{K}[J_1 \cup J_2] \subseteq R$. So $R$ is indeed a subring and $R = \mathbb{K}[I]$.

(b) Similar to (a). □

**Lemma 5.1.3 [fof]**

(a) Let $R$ be a ring, $M$ $R$-module and $S$ a subring of $R$. Let $A \subseteq R$, $B \subseteq M$ and put $\mathcal{B} = \{ab \mid a \in A, b \in B\}$

(aa) If $R = SA$ and $M = RB$ then $M = S\mathcal{D}$.

(ab) If $A$ is linear independent over $S$ and $B$ is linear independent over $R$ then $\mathcal{D}$ is linear independent over $S$.

(ac) If $A$ is an $S$-basis for $R$ and $B$ is an $R$-basis for $M$, then $\mathcal{D}$ is a $S$ basis for $M$.

(b) Let $\mathbb{E} : \mathbb{K}$ be a field extension and $V$ a vector space over $\mathbb{E}$. Then

$$\dim_{\mathbb{K}} V = [\mathbb{E} : \mathbb{K}] \cdot \dim_{\mathbb{E}} V.$$
(c) Let $E : K$ be a field extension and $L : E$ an extension. Then

$$[L : K] = [L : E][E : K].$$

In particular, if $L : E$ and $E : K$ are finite, also $L : K$ is finite.

**Proof:** (aa) Let $m \in M$. Then $m = \sum_{b \in B}r_b b$ with $r_b \in R$. Hence $r_b = \sum_{a \in A} s_{ab}a$ with $s_{ab} \in S$. Thus $m = \sum_{(a,b) \in A \times B} s_{ab}ab$. So (aa) holds

(ab) Suppose that $\sum_{(a,b) \in A \times B} s_{ab}ab = 0$. Then $\sum_{b \in B}(\sum_{a \in A} s_{ab}a)b = 0$. Since $B$ is linear independent over $R$, we conclude $\sum_{a \in A} s_{ab}a = 0$ for all $b \in B$. As $A$ is linear independent over $S$ we get $s_{ab} = 0$ for all $a \in A$ and all $b \in B$. Thus (ab) holds.

(ac) follows from (aa) and (ab). (b) and (c) follow from (ac). \qed

**Lemma 5.1.4 [menk]** Let $F : E K$ and $b \in F$. If $b$ is algebraic over $K$, $b$ is algebraic over $E$ and $m_b^K$ divides $m_b^{K'}$ in $K[x]$.

**Proof:** This follows from $m_b^K(b) = 0$ and $m_b^K \in E[x]$. \qed

Let $f \in K[x]$ we say that $f$ splits over $K$ if

$$f = k_0(x - k_1)(x - k_2) \ldots (x - k_n)$$

for some $k_i \in K, 0 \leq i \leq n$.

**Lemma 5.1.5 [adjroots]** Let $K$ be a field and $f \in K[x]$.

(a) If $E : K$ is finite, $f \in K[x]$ is irreducible and $E = K[a]$ for some root $a$ of $f$ in $E$, then the map

$$h + (f) \rightarrow E, h \rightarrow h(a)$$

is field isomorphism.

(b) If $f$ is not a constant, then there exists a finite field extension $E : K$ so that $f$ has a root in $E$ and $[E : K] \leq \deg f$.

(c) There exists a finite field extension $F : K$ so that $f$ splits over and $[F : K] \leq (\deg f)!$.

**Proof:** (a) Since $(m_a)$ contains a unique monic irreducible polynomial, namely $m_a$, we get $f \sim m_a$. So (b) follows from 5.1.1.

(b) Without loss $f$ is irreducible. Put $E = K[x]/(f)$. Then $[E : K] \leq \deg f$. Let $a = x + (f)$. Then $f(a) = f(x) + (f) = (f)$. So $a$ is a root of $f$ in $E$.

(c) Let $E$ be as in (b) and $e$ a root of $f$ in $E$. Then $f = (x - e)g$ for some $g \in E[x]$ with $\deg g = \deg f - 1$. By induction on $\deg f$ there exists a field extension $F : E$ so that $g$ splits over $F$ and $[F : E] \leq (\deg g)!$. Then $f$ splits over $F$ and

$$[F : K] = [F : E] \cdot [E : K] \leq (\deg f - 1)! \deg f = \deg f!.$$
Lemma 5.1.6 [adjalg] Let $L : \mathbb{K}$ be an extension and $A \subseteq L$ be a set of elements in $L$ algebraic over $\mathbb{K}$.

(a) If $A$ is finite, $\mathbb{K}[A] : \mathbb{K}$ is finite.

(b) $\mathbb{K}[A] : K$ is algebraic.

(c) The set of elements in $L$ algebraic over $\mathbb{K}$ form a subfield of $L$.


(b) Follows from (a) and 5.1.2a.

(c) Follows from (b) applied to $A$ being the set of all algebraic elements in $L$. \hfill \Box

Theorem 5.1.7 [algalg] Let $E : \mathbb{K}$ and $F : E$ be algebraic field extensions. Then $F : \mathbb{K}$ is algebraic.

Proof: Let $b \in F$ and $m = m_b^F$. Let $A$ be the set of coefficients of $m$. Then $A$ is a finite subset of $E$.

$E : \mathbb{K}$ is algebraic, 5.1.6 implies that $\mathbb{K}[A] : \mathbb{K}$ is finite. Also $m \in \mathbb{K}[A][x]$ and so $b$ is algebraic over $\mathbb{K}[A]$. Hence $\mathbb{K}[A][b] : \mathbb{K}[A]$ is finite. By 5.1.3c, $\mathbb{K}[A][b] : \mathbb{K}$ and so also $\mathbb{K}[b] : \mathbb{K}$ is finite. It follows that $b$ is algebraic over $\mathbb{K}$. \hfill \Box

Proposition 5.1.8 [lotsofroots] Let $\mathbb{K}$ be a field and $P$ a set of non constant polynomials over $\mathbb{K}$. Then there exists an algebraic extension $F : \mathbb{K}$ so that each $f \in P$ has a root in $F$.

Proof: If $P$ is finite this follows from 5.1.5(c) applied to $f = \prod_{g \in P} g$.

In the general case let $R = \mathbb{K}[x_f, f \in P]$ be the polynomial ring of $P$ over $\mathbb{K}$. Let $I$ be the ideal in $R$ generated by $f(x_f), f \in P$. We claim that $I \neq R$. So suppose that $I = R$, then $1 \in I$ and so $1 = \sum_{f \in P} r_f f(x_f)$ for some $r_f \in R$, where almost all $r_f = 0$. Note that each $r_f$ only involves finitely many $x_g, g \in P$. Hence there exists a finite subset $J$ of $I$ so that $r_f = 0$ for $f \notin J$, and $r_f \in \mathbb{K}[x_g, g \in J$ for all $f \in J$. So

$$1 = \sum_{f \in J} r_f f(x_f).$$

On the other hand by the finite case there exists a field extension $E : \mathbb{K}$ so that each $f \in J$ as a root $a_f \in E$. Let

$$\Phi : \mathbb{K}[x_g, g \in J] \to E$$

be the unique ring homomorphism with $\Phi(x_f) = a_f$ and $\Phi(k) = k$ for all $k \in K$. Since $f(x_f) = \sum_{i=0}^\infty k_i x_f^i$ for some $k_i \in \mathbb{K}$ we have $\Phi(f(x_f)) = \sum_{i=0}^\infty k_i a_f^i = f(a_f) = 0$. So applying $\Phi$ to the above equation we get

$$1 = \Phi(1) = \sum_{f \in J} \Phi(r_f)f(a_f) = 0$$
a contradiction.

Hence $I \neq R$ and by 3.2.8 $I$ is contained in a maximal ideal $M$ of $R$. Let $\mathbb{F} = R/M$. Then $\mathbb{F}$ is a simple ring and so by 3.2.10 $\mathbb{F}$ is a field. View $\mathbb{K}$ as a subfield of $\mathbb{F}$ by identifying $k$ and $k + M$. Put $a_f = x_f + M$. Then $f(a_f) = f(x_f) + M$. But $f(x_f) \in I \subseteq M$ and so $f(a_f) = 0$. □

**Lemma 5.1.9 [basalc]** Let $\mathbb{K}$ be a field. Then the following statements are equivalent.

(a) Every polynomial over $\mathbb{K}$ has a root in $\mathbb{K}$.

(b) Every polynomial over $\mathbb{K}$ splits over $\mathbb{K}$.

(c) $\mathbb{K}$ has no proper algebraic extension.

(d) $\mathbb{K}$ has no proper finite extension.

**Proof:** (a) ⇒ (b): Let $f \in \mathbb{K}[x]$ with $\deg f > 0$. By (a) $f = (x - a)g$ for some $g \in \mathbb{K}[x]$ with $\deg g < \deg f$. By induction $g$ splits over $\mathbb{K}$.

(b) ⇒ (a): Let $\mathbb{E} : \mathbb{K}$ be algebraic and $e \in E$. Since $m_e$ is irreducible, (b) implies $\deg m_e = 1$. Thus $e \in K$.

(c) ⇒ (d): Obvious.

(d) ⇒ (a): Let $f \in K$. By 5.1.5 $f$ has a root in some finite extension $E$ of $K$. By assumption $E = K$. So (a) holds. □

A field which fulfills the equivalent statement in the previous theorem is called algebraically closed.

Suppose that $\mathbb{E} : \mathbb{K}$ is an algebraic field extension such that $\mathbb{E}$ is algebraically closed, then $\mathbb{E}$ is called an algebraic closure of $\mathbb{K}$.

**Lemma 5.1.10 [chralgc]** Let $\mathbb{E} : \mathbb{K}$ be a algebraic field extension. Then the following are equivalent.

(a) $\mathbb{E}$ is an algebraic closure of $\mathbb{K}$.

(b) Every polynomials over $\mathbb{K}$ splits over $\mathbb{E}$.

**Proof:** Clearly (a) implies (b). So suppose (b) holds. Let $\mathbb{F}$ be an algebraic extension of $\mathbb{E}$. Let $a \in \mathbb{F}$. By 5.1.7 $a$ is algebraic over $\mathbb{K}$. As $m_a^K$ splits over $E$, $a \in \mathbb{E}$. So $\mathbb{E} = \mathbb{F}$ and $\mathbb{E}$ is algebraically closed. □

**Theorem 5.1.11 [exalgcl]** Every field has an algebraic closure.
Proof: Let \( K_0 \) be a field. By 5.1.8 applied to the set of non-constant polynomials there exists an algebraic field extension \( K_1 \) of \( K_0 \) so that every non-zero polynomial over \( K_0 \) has a root in \( K_0 \). By induction there exists fields

\[
K_0 \leq K_1 \leq K_2 \ldots
\]

so that that every non zero polynomial in \( K_i \) has a root in \( K_{i+1} \). Let \( E = \bigcup_{i=0}^{\infty} K_i \). It is easy to verify (cf. 5.1.2 ) that \( E \) is a field. As each \( K_i \) is algebraic over \( K_0 \), \( E : K_0 \) is algebraic. Let \( f \in E[x] \). Then \( f \in K_i[x] \) for some \( i \). Hence \( f \) has a root in \( K_{i+1} \) and so in \( E \). Thus by 5.1.9 \( E \) is algebraically closed. \( \square \)

Definition 5.1.12 Let \( \mathbb{K} \) be a field and \( P \) a set of non-constant polynomials over \( \mathbb{K} \). A splitting field for \( P \) over \( \mathbb{K} \) is an extension \( E : \mathbb{K} \) so that

(a) Each \( f \in P \) splits over \( E \).

(b) \( E = \mathbb{K}[A] \) where \( A := \{ a \in E \mid f(a) = 0 \text{ for some } f \in P \} \).

Corollary 5.1.13 [exsplit] Let \( \mathbb{K} \) be a field and \( P \) a set of non-constant polynomials over \( \mathbb{K} \). Then there exists a splitting field for \( P \) over \( \mathbb{K} \).

Proof: Let \( \mathbb{K} \) be an algebraic closure for \( \mathbb{K} \), \( B := \{ a \in \mathbb{K} \mid f(a) = 0 \text{ for some } f \in P \} \). and put \( E = \mathbb{K}[B] \). Then \( E \) is a splitting field for \( P \) over \( \mathbb{K} \). \( \square \)

5.2 Splitting fields, Normal Extensions and Separable Extensions

Let \( \phi : \mathbb{K}_1 \to \mathbb{K}_2 \) be a field monomorphism. Note that \( \phi \) extends to a monomorphism (which we denote with the same name)

\[
\phi : \mathbb{K}_1[x] \to \mathbb{K}_2[x], \sum a_ix^i \to \sum \phi(a_i)x^i.
\]

Note that if \( \phi \) is an isomorphism so is the extension.

Lemma 5.2.1 [extiso] Let \( \phi : \mathbb{K}_1 \to \mathbb{K}_2 \) be a field isomorphism and \( \mathbb{E}_i : \mathbb{K}_i \). Let \( f_1 \in \mathbb{K}_1[x] \) be irreducible and \( f_2 = \phi(f_1) \). Let \( e_i \) be a root of \( f_i \) in \( \mathbb{K}_i \). Then there exists a unique isomorphism \( \psi : \mathbb{K}_1[e_1] \to \mathbb{K}_2[e_2] \) with \( \psi|_{\mathbb{K}_1} = \phi \) and \( \psi(e_1) = e_2 \).

Proof: Using 5.1.5(a) we have

\[
\mathbb{K}_1[e_1] \cong \mathbb{K}_1[x]/(f_1) \cong \mathbb{K}_2[x]/(f_2) \cong \mathbb{K}_2[e_2]
\]

Note also that \( e_1 \to x + (f_1) \to x + (f_2) \to e_2 \). \( \square \)

Let \( F_1 : \mathbb{K} \) be field extension and \( \phi : F_1 \to F_2 \) a ring homomorphism. We say that \( \phi \) is \( \mathbb{K} \)-homomorphism if \( \phi \) is \( \mathbb{K} \)-linear. Note that this just means \( \phi(k) = k \) for all \( k \in \mathbb{K} \).
Lemma 5.2.2 [isosplitfield] Let \( \mathbb{K} \) be a field field and \( P \) a set of polynomials. Let \( E_1 \) and \( E_2 \) be splitting fields for \( P \).

(a) Let \( E_i : L_i : \mathbb{K} \), \( i = 1, 2 \) and \( \delta : L_1 \to L_2 \) a \( \mathbb{K} \)-isomorphism. Then there exists a \( \mathbb{K} \)-isomorphism \( \psi : E_1 \to E_2 \) with \( \psi|_{E_i} = \delta \).

(b) \( E_1 \) and \( E_2 \) are \( \mathbb{K} \)-isomorphic.

(c) Let \( f \in \mathbb{K}[x] \) be irreducible and \( e_i \) a root of \( f \) in \( E_i \). Then there exists a \( \mathbb{K} \)-isomorphism \( \psi : E_1 \to E_2 \) with \( \psi(e_1) = \psi(e_2) \).

(d) Let \( f \in \mathbb{K}[x] \) be irreducible and let \( e \) and \( d \) be roots of \( f \) in \( E_1 \). Then there exists \( \psi \in \text{Aut}_{\mathbb{K}}(E_1) \) with \( \psi(e) = d \).

(e) Any two algebraic closure of \( \mathbb{K} \) are \( \mathbb{K} \)-isomorphic.

**Proof:**

(a) Let \( \mathcal{M} \) be the set of all \( \mathbb{K} \)-linear isomorphism \( \phi : F_1 \to F_2 \) where \( F_i \) is an intermediate field of \( E_i : \mathbb{K} \). Order \( \mathcal{M} \) by \( \phi \leq \psi \) if \( \phi \) is the restriction of \( \psi \) to a subfield. Let \( \mathcal{M}^* = \{ \phi \in \mathcal{M} \mid \delta \leq \phi \} \). Since \( \delta \in \mathcal{M}^* \), \( \mathcal{M}^* \) is not empty. It is easy to verify that each chain in \( \mathcal{M}^* \) has an upper bound (cf.4.3.8). By Zorn's Lemma A.1 \( \mathcal{M}^* \) has a maximal element \( \psi : F_1 \to F_2 \). We claim that \( F_1 = E_1 \). Indeed let \( f \in P \) and \( e_1 \) a root of \( f \) in \( E_1 \). Let \( f_1 \in F_1[x] \) be an irreducible factor of \( f \) with \( f_1(e_1) = 0 \). Put \( f_2 = \phi(f_1) \). Then \( f_2 \) is an factor of \( \phi(f) = f \) and so \( f_2 \) has a root \( e_2 \in E_2 \). By 5.2.1 there exists \( \psi : F_1[e_1] \to F_2[e_2] \) with \( \psi|_{E_i} = \phi \). Hence by maximality of \( \phi \), \( F_1 = F_1[e_1] \). Thus \( e_1 \in F_1 \). Since \( E_1 \) is generated by the various \( e_i \) we get \( F_1 = E_1 \). Since \( F_1 \) is a splitting field for \( P \) and \( \phi \) is an isomorphism, \( F_2 \) is a splitting field for \( P \). Hence \( F_2 = E_2 \) and (a) holds.

(b) Apply (a) to \( \delta = \text{id}_{\mathbb{K}} \).

(c) By 5.2.1 there exists a \( \mathbb{K} \)-linear isomorphisms \( \delta : \mathbb{K}[e_1] \to \mathbb{K}[e_2] \) with \( \delta(e_1) = e_2 \). By (a) \( \delta \) can be extended to an isomorphism \( \psi : E_1 \to E_2 \). So (c) holds.

(d) Follows from (c) with \( E_2 = E_1 \).

(e) Follows from (b) with \( P \) the set of all non-constant polynomials. \( \square \)

Let \( \mathbb{K} \) be a field and \( P \) a set of polynomials over \( \mathbb{K} \). \( \mathbb{K}[P] \) will denote a splitting field for \( P \) over \( \mathbb{K} \). Note that \( \mathbb{K}[P] \) exists and is unique up a \( \mathbb{K} \)-isomorphism.

**Definition 5.2.3** Let \( L : E \) be a field extension and \( H \leq \text{Aut}(L) \).

(a) \( E \) is called \( H \)-stable if \( HE := \{ h(e) \mid h \in H, e \in E \} \leq E \).

(b) If \( E \) is \( H \)-stable, the image of \( H \) in \( \text{Aut}(E) \) under the restriction map \( \phi \to \phi|_E \) is denoted by \( HE \).

(c) \( L : E \) is called normal if \( L : E \) is algebraic and each irreducible \( f \in E[x] \) which has a root in \( L \) splits over \( L \).

**Lemma 5.2.4** [normalstable]
(a) Let $L : E : K$ and $E = K[P]$ for some set of non-constant polynomial over $K$. Then $E$ is $\text{Aut}_K(L)$ stable.

(b) Let $E : K$ is normal if an only if $E$ is a the splitting field for some set of polynomials over $K$.

**Proof:** (a) Let $f \in P$, $e$ a root of $f$ in $E$ and $\phi \in \text{Aut}_K(L)$. Then $\phi(e)$ is a root of $\phi(f) = f$ and as $f$ splits over $E$, $\phi(e) \in E$. Since $E$ is generated by the various $e$, $\phi(E) \subseteq E$ and (a) holds.

(b) If $E : K$ is normal, $E$ is the splitting field of the set of polynomial over $K$ with roots in $E$.

So suppose that $E = K[P]$. Let $L$ be an algebraic closure of $E$. Let $e \in E$ and $f = m^E_e$. Then $f$ splits over $L$. Let $d$ be a root of $E$ in $L$. By 5.2.2d there exists $\psi \in \text{Aut}_K(L)$ with $\psi(e) = d$. By (a), $\psi(E) \subseteq E$ and so $d \in E$. Hence $f$ splits over $E$ and $E : K$ is normal. □

**Lemma 5.2.5** [minnor] Let $L : K$ be an algebraic field extension and $E$ and $F$ intermediate fields. Suppose that $E : K$ is normal, then $m^E_b = m^F_b = m^{F\cap E}_b$ for all $b \in E$.

**Proof:** Let $g = m^F_b$ and $f = m^K_b$. As $E : K$ is normal $f$ splits over $E$. Since $g$ divides $f$, $g$ is a product of polynomials of the form $x - d$, $d$ a root of $f$. Since $d \in E$ we get $g \in E[x]$ and so $g \in E\alpha'F[x]$. Thus $g = m^{F\cap E}_b$. □

**Definition 5.2.6** (a) Let $E$ be a field. An irreducible polynomial $f \in E[x]$ is called separable over $E$ if $F$ has no multiple roots. An arbitrary polynomial in $E[x]$ is called separable over $E$ if all its irreducible factors are separable over $E$.

(b) Let $L : E$ be a field extension and $b \in L$. $b$ is separable over $E$, if $b$ is algebraic over $E$ and $m^E_b$ is separable over $E$. $L : E$ is a called separable over $K$ if each $b \in L$ is separable over $L$.

**Lemma 5.2.7** [frob] Let $K$ be a field, $\bar{K}$ an algebraic closure of $K$ and suppose that $\text{char} K = p$ with $p \neq 0$.

(a) The map $\text{Frob}(p) : K \to \bar{K}, k \to k^p$ is a field monomorphism.

(b) For each $b \in K$ and $n \in \mathbb{Z}^+$ there exists a unique $d \in \bar{K}$ with $d^p = b$. We will write $b^{1/p}$. for $d$.

(c) For each $n \in \mathbb{Z}$, the map $\text{Frob}(p^n) : K \to \bar{K}, k \to k^{p^n}$ is a field monomorphism.

(d) If $K$ is algebraically closed each $\text{Frob}(p^n)$ is an automorphism.

(e) If $f \in K[x]$ and $n \in \mathbb{N}$, then $f^{p^n} = \text{Frob}(p^n)(f)(x^{p^n})$.  

5.2. SPLITTING FIELDS, NORMAL EXTENSIONS AND SEPARABLE EXTENSIONS

(a) Clearly \((ab)^p = a^pb^p\). Note that \(p\) divides \(\binom{p}{i}\) for all \(1 \leq i < p\). So by the Binomial Theorem \((a + b)^p = a^p + b^p\). So \(\text{Frob}(p)\) is a field homomorphism. Since \(\text{Frob}(p)\) is not the zero map, \(\text{Frob}(p)\) is one to one.

(b) Let \(d\) be a root of \(x^{p^n} - b = 0\). Then \(d^{p^n} = b\). The uniqueness follows from (a).

(d) \(\text{Frob}(p^{-n})\) is the inverse of \(\text{Frob}(p^n)\).

(c) Follows from (d).

(e) Let \(f = \sum a_i x^i\). Then \(\text{Frob}(p^n)(f) = \sum a_i^{p^n} x^i\) and so

\[
\text{Frob}(p^n)(f)(x^{p^n}) = \sum a_i^{p^n} x^{p^ni} = (\sum a_i x^i)^{p^n} = f^{p^n}.
\]

\[\square\]

**Lemma 5.2.8 [bqink]** Let \(\mathbb{F} : \mathbb{K}\) be a field extension, \(p := \text{char } \mathbb{K} \neq 0\) and \(b \in \mathbb{F}\). Suppose that \(b^{p^n} \in \mathbb{K}\) for some \(n \in \mathbb{N}\). Then

(a) \(b\) is the only root of \(m^K_b\) (in any algebraic closure of \(\mathbb{K}\)).

(b) If \(b\) is separable over \(\mathbb{K}\), \(b \in \mathbb{K}\).

(c) \(d^{p^n} \in \mathbb{K}\) for all \(d \in \mathbb{K}[b]\).

**Proof:** Let \(q = p^n\).

(a) \(m^K_b\) divides \(x^q - b^q = (x - b)^q\). So (a) holds.

(b) If \(m^K_b\) is separable we conclude \(m^K_b = x - b\). So (b) holds.

(c) Let \(\phi = \text{Frob}(q)\). Then \(\{d^q \mid d \in \mathbb{K}[b]\} = \phi([\mathbb{K}[b]]) = \phi(\mathbb{K})[\phi(b)] \leq \mathbb{K}[b^q] \leq \mathbb{K}\).

\[\square\]

**Lemma 5.2.9 [bsep]** Let \(\mathbb{F} : \mathbb{E} : \mathbb{K}\) and \(b \in \mathbb{F}\). If \(b \in \mathbb{F}\) is separable over \(\mathbb{K}\). Then \(b\) is separable over \(\mathbb{E}\).

\[
\text{Note that } m^E_b \text{ divides } m^K_b. \text{ As } b \text{ is separable over } \mathbb{K}, \text{ } m^K_b \text{ has no multiple roots. So also } m^E_b \text{ has no multiple roots and } b \text{ is separable over } \mathbb{E}. \square
\]

**Lemma 5.2.10 [charseppol]** Let \(\mathbb{K}\) be a field and \(f \in \mathbb{K}[x]\) monic and irreducible.

(a) \(f\) is separable if and only if \(f' \neq 0\).

(b) If \(\text{char } \mathbb{K} = 0\), all polynomials are separable,

(c) Suppose \(\text{char } \mathbb{K} = p \neq 0\) and let \(b_1, b_2, \ldots, b_d\) be the distinct roots of \(f\) in an algebraic closure \(\bar{\mathbb{K}}\) of \(\mathbb{K}\). Let \(b\) be any root of \(f\). Then there exist an irreducible separable polynomial \(g \in \mathbb{K}[x]\), a polynomial \(h \in \text{Frob}(p^{-n})(\mathbb{K})[x]\) and \(n \in \mathbb{N}\) so that

\[
\text{(ca) } f = g(x^{p^n}) = h^{p^n}.
\]
(cb) \( g = \text{Frob}(p^n)(h) \).

(cc) \( g = (x - b_1^{p^n})(x - b_2^{p^n}) \cdots (x - b_d^{p^n}) \).

(cd) \( h = (x - b_1)(x - b_2) \cdots (x - b_d) \in \mathbb{K}[b_1, \ldots, b_d][x] \).

(ce) \( f = (x - b_1)p^n(x - b_2)p^n \cdots (x - b_d)p^n \).

(cf) \( f \) is separable over \( \mathbb{K} \) if and only if \( n = 0 \).

(ce) \( \mathbb{K}[b] : \mathbb{K}[b^p] = p^n \).

(ch) \( b \) is separable over \( \mathbb{K} \) if and only if \( \mathbb{K}[b] = \mathbb{K}[b^p] \).

(ci) \( b^p \) is separable over \( \mathbb{K} \).

**Proof:** (a) By 3.6.11 \( b \) is a multiple root of \( f \) if and only if \( f'(b) = 0 \). Since \( f \) is irreducible, \( f = m_\mathbb{K}^b \) and so \( f \) has a multiple root if and only if \( f \) divides \( f' \). As \( \deg f' \leq \deg f \), this the case if and only if \( f' = 0 \).

(b) follows from (a).

(c) We will first show that \( f = g(x^{p^n}) \) for some separable \( g \in \mathbb{K}[x] \) and \( n \in \mathbb{N} \). If \( f \) is separable, this is true with \( g = f \) and \( n = 0 \). So suppose \( f \) is not separable. By (a) \( f' = 0 \). Let \( f = \sum a_i x^i \). Then \( 0 = f' = \sum i a_i x^{i-1} \) and so \( i a_i = 0 \) for all \( i \). Thus \( p \) divides \( i \) for all \( i \) with \( a_i \neq 0 \). Put \( \tilde{f} = \sum a_{pi} \tilde{x}^i \). Then \( \tilde{f}(x^{p^n}) = \sum a_{pi} x^{pi} = f \). By induction on \( \deg f \), \( \tilde{f} = g(x^{p^n}) \) for some irreducible and separable \( g \in \mathbb{K}[x] \). Let \( n = m + 1 \), then \( f = g(x^{p^n}) \).

Since \( f \) is irreducible, \( g \) is irreducible.

Let \( h = \text{Frob}(p^{-n})(g) \in \mathbb{K}[x] \). Then \( g = \text{Frob}(p^n)(h) \). Thus by 5.2.7e, \( h^{p^n} = g(x^{p^n}) = f \).

Let \( b \in \bar{K} \). Then \( b \) is a root of \( f \) if and only if \( b^{p^n} \) is a root of \( g \). So \( \{b_1^{p^n}, \ldots, b_d^{p^n}\} \) is the set of roots of \( f \). As \( \text{Frob}(p^n) \) is one to one, the \( b_i^{p^n} \) are pairwise distinct. Since \( g \) is separable, \( g = \prod(x - e) \mid e \) a root of \( g \) \} and so (cc) holds.

(cd) now follows from \( h = \text{Frob}(p^{-n})(g) \).

(ce) follows form (cd) and (ca).

(cf) follows from (cc)

(cl) Note that \( g \) is the minimal polynomial of \( b_i^{p^n} \) over \( \mathbb{K} \), \( f \) is the minimal polynomial of \( b_i \) over \( \mathbb{K} \) and \( \deg f = p^n \deg g \). Thus

\[
\frac{[\mathbb{K}[b] : \mathbb{K}[b^p]]}{\deg g} = \frac{\deg f}{\deg g} = p^n.
\]

(ch) Suppose \( b \) is not separable. The \( n > 0 \) and so \( b^p \) is a root of \( g(x^{p^{n-1}}) \). So \( [\mathbb{K}[b^p] : \mathbb{K}] = p^{n-1} \) and \( \mathbb{K}[b] \neq \mathbb{K}[b^p] \).

Suppose that \( b \) is separable over. Then by 5.2.9 \( b \) is separable over \( \mathbb{K}[b^p] \). So by 5.2.8, \( b \in \mathbb{K}[b^p] \). Thus \( \mathbb{K}[b] = \mathbb{K}[b^p] \).

(ci) follows as \( b_i^{p^n} \) is a root of the separable \( g \). \( \square \)

**Definition 5.2.11** Let \( \mathbb{F} : \mathbb{K} \) be a field extension Let \( b \in \mathbb{F} \). Then \( b \) is purely inseparable over \( \mathbb{K} \) if \( b \) is algebraic over \( \mathbb{K} \) and \( b \) is the only root of \( m_b^K \). \( \mathbb{F} : \mathbb{K} \) is called purely inseparable if all elements in \( \mathbb{F} \) are purely inseparable over \( \mathbb{K} \).
Lemma 5.2.12 \textbf{[basicpursep]} Let $F : K$ be an algebraic field extension with $\text{char } K = p \neq 0$.

(a) Let $b \in K$ then $b$ is purely inseparable if and only if $b^{p^n} \in K$ for some $n \in \mathbb{N}$.

(b) $F : K$ is purely inseparable if and only the only elements in $F$ separable over $K$ are the elements of $K$.

(c) Let $P = \{b \in F \mid b^{p^n} \in K \text{ for some } n \in \mathbb{N}\}$. Then $P$ is the of elements in $F$ purely inseparable over $K$ and $P$ is a subfield of $F$.

(d) If $F : K$ is normal, then $F : P$ is separable.

(e) If $b \in F$ is separable over $K$, then $m^p_b = m^K_b$.

(f) $P \leq \text{Fix}_F(\text{Aut}_K(F))$ with equality if $F : K$ is normal.

\textbf{Proof}: Let $b \in F$. Let $f := m^K_b = g(x^{p^n})$ with $g \in K[x]$ separable. Put $q = p^n$ and $a = b^q$. Note that $a$ is separable over $K$. If $b$ is the only root of $f$ then by 5.2.10 then $g = x - a$, $f = x^q - a$ and $a \in K$. So (a) holds.

(b) Suppose first that that separable elements of $F : K$ are on $K$. As $a$ is separable over $K$ we conclude $a \in K$ and $b$ is purely inseparable. So $F : K$ is purely inseparable.

Suppose next that $F : K$ is purely inseparable. If $b$ is separable then by 5.2.10(cf), $n = 0$ and $b = a \in K$.

(c) By (a) $P$ is the set of pure inseparable elements. As $\text{Frob}(p^{-n})$ is a homomorphism, $\text{Frob}(p^{-n})(K)$ is a subfield of $F$. Also $\text{Frob}(p^{-n})(K) = \text{Frob}(p^{-(n+1)})$ and $P = \bigcup_{i=1}^\infty \text{Frob}(p^i)(K)$. So (c) holds as the ascending unions of subfields is a subfield.

(d) Since $b$ is a root of $f \in F$ and $F : K$ is normal, $f$ splits over $F$. Let $h = \text{Frob}(\frac{1}{q})(g)$. Then $f = h^q$ and by 5.2.10(cd) $h$ splits over $F$. In particular, $h \in F[x]$. Since $h^q = f \in K[x]$ we see that $d^q \in K$ for each coefficient $d$ of $f$. Hence $d \in P$ and $h \in P[x]$. By 5.2.10(cd) $h$ has no multiple roots. Also $h(b) = 0$ and so $b$ is separable over $P$.

(e) $t = m^p_b$. As $t \in P[x]$, $t^{q^i} \in K[x]$ for some power $q$ of $p$. Since $t^{q^i}[b] = 0$ we conclude $f$ divides $t^{q^i}$. As $f$ is separable, $f$ divides $t$ and so $f = t$.

(f) Let $b \in P$ and $\phi \in \text{Aut}_K(F)$. The $b^q \in K$ and so $\phi(b^q) = \phi(b^q) = b^q$. Thus $b = \phi(b)$ and $P \leq \text{Fix}_F(\text{Aut}_K(F))$.

Next let $b \notin P$ and suppose that $F : K$ is normal. Since $b \notin P$ and $F : K$ is normal, there exists a root $d \neq b$ in $F$. Since $F$ is a splitting field over $K$, 5.2.2d implies that there exists $\phi \in \text{Aut}_K(F)$ with $\phi(b) = d$. Hence $b \notin \text{Fix}_F(\text{Aut}_K(F))$. \hfill \qed

Lemma 5.2.13 \textbf{[sepsep]}

(a) Given $F : E : K$. Then $F : K$ is separable if and only $F : E$ and $E : K$ are separable.
(b) \( E : \mathbb{K} \) is separable if and only if \( E = \mathbb{K}[S] \) for some \( S \subseteq E \) such that all \( b \in S \) are separable over \( \mathbb{K} \).

Proof: If \( \text{char} \mathbb{K} = 0 \) there is nothing to prove. So assume \( \text{char} \mathbb{K} = p, p \) a prime. Before proving (a) and (b) prove

(\ast) Let \( L : \mathbb{K} \) be a field extension, \( I \subseteq L \) and \( b \in L \). If all elements and \( I \) are separable over \( \mathbb{K} \) and \( b \) is separable over \( \mathbb{K}[I] \), then \( b \) is separable over \( \mathbb{K} \).

Let \( s = m_b^{K(I)} \). By 5.1.2 \( \mathbb{K}(I) = \bigcup \{ \mathbb{K}(J) \mid J \subseteq I, J \text{ finite} \} \). Hence there exists a finite subset \( J \) of \( I \) with \( s \in \mathbb{K}[J][x] \). So \( b \) is separable over \( \mathbb{K}[J] \). So we may assume that \( I \) is finite and proceed by induction on \( |I| \). Let \( a \in I \). Then \( b \) is separable over \( \mathbb{K}[a][J-a] \) and so by induction \( b \) is separable over \( \mathbb{K}[a] \). Hence by 5.2.10ch, \( \mathbb{K}[a,b] = \mathbb{K}[a,b^p] \). Let \( E = \mathbb{K}[b^p] \). Then \( b \in \mathbb{K}[a,b] = \mathbb{K}[a,b^p] = E[a] \). By 5.2.9 \( a \) is separable over \( E \). Since \( b^p \in E \), \( E[b] : E \) is purely inseparable. So by 5.2.12e \( m_a^E = m_a^E(b) \). Thus \( |E[a] : E| = |E[a]/E[b]| \) and so \( E = E[b] \). So \( K[b] = \mathbb{K}[b^p] \) and by 5.2.10ch, \( b \) is separable over \( \mathbb{K} \).

(a) Suppose now that \( F : E \) and \( E : \mathbb{K} \) are separable. Let \( b \in F \) and let \( I = E \). Then by (\ast\ast), \( b \) is separable over \( \mathbb{K} \). So \( F : \mathbb{K} \) is separable.

Conversely suppose \( F : \mathbb{K} \) is separable. Then clearly \( E : \mathbb{K} \) is separable. By (\ast) also \( F : E \) is separable.

(b) \( \Rightarrow \) is obvious. So suppose \( E = \mathbb{K}[S] \) with all elements in \( S \) separable over \( \mathbb{K} \). Let \( b \in \mathbb{K}[S] \). Then by (\ast), \( b \) is separable over \( \mathbb{K} \) and so \( E : \mathbb{K} \) is separable. \( \square \)

Lemma 5.2.14 [puresep] Let \( F : \mathbb{K} \) be an algebraic field extension with \( \text{char} K = p \neq 0 \).

(a) The elements in \( F \) separable over \( \mathbb{K} \) form a subfield \( S \).

(b) \( F : S \) is purely inseparable.

Proof:

(a) Follows from 5.2.13a.

(b) Follows from ??ci. \( \square \)

Let \( \mathbb{K} \) with \( \text{char} K = p \neq 0 \). Let \( F = \mathbb{K}(s) \), the field of rational function in the indeterminant \( s \) over \( \mathbb{K} \). Let \( E = \mathbb{K}(s^p) \). The \( [F : E] = p \) and since \( s^p \in E, F : E \) is purely inseparable. \( 1, s, s^2, \ldots s^{p-1} \) is a basis for \( F \) as an \( E \)-space. More general, let \( F = \mathbb{K}(x_i, i \in I) \) and \( E = \mathbb{K}(x_i^p, i \in I) \). Again \( F : E \) is purely inseparable and the monomials

\[
x_{i_1}^{l_1} \ldots x_{i_k}^{l_k}
\]

with \( 0 \leq l_r < p \) form a basis for \( F \) over \( \mathbb{K} \). So we see that there exists purely inseparable extension of infinite degree.

Next we give an example of a field extension \( F : \mathbb{K} \) so that \( \mathbb{K} = \mathbb{P} \) but \( F \neq \mathbb{S} \). So \( F : \mathbb{P} \) is not separable. That is the conclusion of part (e) of ?? may be false if \( F : \mathbb{K} \) is not normal.
Let $p = 2$ and $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}(s,t)$, the field of rational fraction in the indeterminants $s$ and $t$ over $\mathbb{Z}/2\mathbb{Z}$.

Let $\xi$ be a root of $x^2 + x + 1 = 0$ in $\overline{\mathbb{K}}$ and let $\lambda$ be a root of $x^2 + (s + \xi t) = 0$.

As $\xi$ is algebraic over $\mathbb{Z}/2\mathbb{Z}$, $\xi \notin \mathbb{K}$. Suppose that $\lambda \in \mathbb{K}[\xi]$. Then $(f + g\xi)^2 = s + \xi t$ for some $f, g \in \mathbb{K}$. Thus $s + \xi t = f^2 + g^2\xi^2 = f^2 + g^2 + g^2\xi$. Hence $g^2 = t$ a contradiction. So $\lambda \notin \mathbb{K}[\xi]$. Let $\mathbb{F} = \mathbb{K}[\lambda, \xi]$. Then $\mathbb{F}^2 \leq \mathbb{K}[\xi]$. Therefore, $\mathbb{F} : \mathbb{K}$ is not separable and $\xi = \mathbb{K}[\xi]$.

Next we show that $\mathbb{F} = \mathbb{K}$. So let $b \in \mathbb{E}$ with $b^2 \in \mathbb{K}$. Then $b = f + g\xi + h\lambda + k\lambda\xi$ for some $f, g, h, k \in \mathbb{K}$. Note that $\lambda^2 = s + \xi t$, $\xi^2 = \xi + 1$ and $\xi^3 = \xi^2 + \xi = 1$. So we compute

$$b^2 = f^2 + g^2\xi^2 + h^2\lambda^2 + k^2\lambda^2\xi^2 = f^2 + g^2 + g^2\xi + h^2s + h^2\xi t + k^2(s + \xi t)\xi^2 = (f^2 + g^2 + h^2s) + (g^2 + h^2t)\xi + k^2s + k^2\xi + k^2 = (f^2 + g^2 + k^2 + (h^2 + k^2)s) + (g^2 + h^2t + k^2)\xi.$$

As $1, \xi$ are linear independent over $\mathbb{K}$ we get $g^2 + h^2t + k^2s = 0$. Since $1, t, s, st$ are linear independent over $\mathbb{K}^2$ we conclude $g = h = k = 0$ so $b = f \in \mathbb{K}$.

### 5.3 Galois Theory

**Hypothesis 5.3.1** Throughout this section $\mathbb{F}$ is a field, $G \leq \text{Aut}(\mathbb{F})$ and

$$\mathbb{K} = \text{Fix}_G(G) := \{ k \in \mathbb{F} \mid \phi(k) = k \forall \phi \in G \}.$$

For $H \leq G$ put $\mathcal{F} H = \text{Fix}_G(H)$ and for a subfield $\mathbb{F} : \mathbb{E} \leq \mathbb{F} : \mathbb{L}$ let $\mathcal{G} E = G \cap \text{Aut}_\mathbb{E}(F)$. Note that $\mathcal{F} G = \mathbb{K}$. We say that $H$ is $(G, \mathbb{F})$-closed if $H = \mathcal{G} \mathcal{F} H$ and similarly we say that $\mathbb{E}$ is $(G, \mathbb{F})$-closed if $\mathbb{E} = \mathcal{F} \mathcal{G} \mathbb{E}$. "closed" will always mean $(G, \mathbb{F})$-closed.

**Lemma 5.3.2** [basicclosed] Let $T \leq H \leq G$ and $\mathbb{F} : \mathbb{E} : \mathbb{L}$. Then

(a) $\mathcal{F} H \leq \mathcal{F} T$.

(b) $\mathcal{G} \mathbb{E} \leq \mathcal{G} \mathbb{L}$.

(c) $H \leq \mathcal{G} \mathcal{F} H$

(d) $\mathbb{E} \leq \mathcal{F} \mathcal{G} \mathbb{E}$.

(e) $\mathcal{F} H$ is closed.

(f) $\mathcal{G} \mathbb{E}$ is closed.

**Proof:** (a)-(d) follow directly from the definitions.

(e) By (c) $H \leq \mathcal{G} \mathcal{F} H$ and so by (a) $\mathcal{G} \mathcal{F} \mathcal{F} H \leq \mathcal{F} H$. On the other hand, by (b) applied to $\mathbb{E} = \mathcal{F} H$, $\mathcal{F} H \leq \mathcal{F} \mathcal{G} \mathcal{F} H$. So (e) holds.

(f) similar to (e) \qed
**Proposition 5.3.3 [bijclosed]** \( F \) induces a bijection between the closed subgroups of \( G \) and the closed subfields of \( \mathbb{F} \). The inverse is induced by \( G \).

**Proof:** By 5.3.2e, \( F \) sends a closed subgroup to a closed subfields and by 5.3.2, \( G \) sends a closed subfields to a closed subgroup. By definition of closed, \( F \) and \( G \) are inverse to each other then restricted to closed objects. \( \square \)

**Lemma 5.3.4 [upperbound]** Let \( H \leq T \leq G \) with \( T/H \) finite. Then \( [FH : FT] \leq |T/H| \).

**Proof:** Let \( k \in FH \) and \( W = tH \in T/H \). Define \( W(k) := t(k) \). Since \( (th)(k) = t(h(k)) = t(k) \) for all \( h \in H \), this is well defined. Define \( \Phi : FH \to \mathbb{F}^{T/H}, k \to (W(k))_{W \in T/H} \).

Let \( L \subseteq FH \) be a basis for \( FH \) over \( FT \). We claim that \( \Phi(L) \) is linear independent over \( \mathbb{F} \). Otherwise choose \( I \subseteq L \) with \( \Phi(I) \) is linear dependent over \( \mathbb{F} \) and \( |I| \) minimal. Note that \( |I| \) is finite. The there exists \( 0 \neq k_i \in \mathbb{F} \), with \( \sum_{i \in I} k_i \Phi(i) = 0 \). Let \( b \in I \) and without loss \( k_b = 1 \).

Note that \( \sum_{i \in I} k_i \Phi(i) = 0 \) means

\[
\sum_{i \in I} k_i W(i) = 0, \quad \forall W \in T/H.
\]

Suppose now that \( k_i \in FT \) for all \( i \). Using \( W = H \) we get \( \sum_{i \in I} k_i i = 0 \), a contradiction to the linear independence of \( I \) over \( FT \). So there exists \( d \in I \) and \( \mu \in T \) with \( \mu(k_d) \neq k_d \).

Note that \( \mu(t(k)) = (\mu t)(k) \) and so \( \mu(W(k)) = (\mu W)(k) \). Thus applying \( \mu \) to (*) we obtain.

\[
\sum_{i \in I} \mu(k_i)(\mu W)(i) = 0, \quad \forall W \in T/H
\]

As every \( W \in T/H \) is of the form \( \mu W' \) for some \( W' \in T/H \), (namely \( W' = \mu^{-1} W \)) we get

\[
\sum_{i \in I} \mu(k_i) W'(i) = 0, \quad \forall W \in T/H
\]

Subtracting (*) form (**) we conclude:

\[
\sum_{i \in I} (\mu(k_i) - k_i) W(i) = 0, \quad \forall W \in T/H.
\]

and so

\[
\sum_{i \in I} (\mu(k_i) - k_i) \Phi(i) = 0.
\]
The coefficient of $\Phi(b)$ in this equation is $\mu(1) - 1 = 0$. The coefficient of $\Phi(d)$ is $\mu(k_d) - k_d \neq 0$. We conclude that $\Phi(I - b)$ is linear dependent over $\mathbb{F}$ a contradiction the minimal choice of $|I|$.

So $\Phi(L)$ is linear independent over $\mathbb{F}$.

Thus

$$[\mathcal{F}H : \mathcal{F}T] = |L| = |\Phi(L)| \leq \dim_{\mathbb{F}} \mathbb{F}^{[T/H]} = |T/H|$$

So the theorem is proved.

We remark that the last equality in the last equation is the only place where we used that $|T/H|$ is finite.

**Lemma 5.3.5 [finiteorbit]** Let $b \in \mathbb{F}$ and $H \leq G$. Then the following are equivalent:

(a) $b$ is algebraic over $\mathcal{F}H$.

(b) $Hb := \{\phi(b) \mid \phi \in H\}$ is finite.

(c) There exists an irreducible $f \in \mathcal{F}H[x]$ so that

(1) $f(b) = 0$.

(2) $f$ is separable.

(3) $f$ splits over $\mathbb{F}$.

(4) $Hb$ is the set of roots of $f$.

(5) Let $H_b := \{\phi \in H \mid \phi(b) = b\}$. Then

$$|H/H_b| = \deg f = [\mathcal{F}H[a] : \mathcal{F}H]$$

**Proof:** Suppose (a) holds and let $f$ be the minimal polynomial of $b$ over $\mathcal{F}H$. Let $\phi \in H$. Then $\phi(b)$ is a root of $\phi(f) = f$. Since $f$ has only finitely many roots, (b) holds.

Suppose next that (b) holds. Let $f := \prod_{e \in Hb} x - e$. Since $\phi$ permutes $Hb$, $\phi(f) = \prod_{e \in Hb} x - \phi(b) = f$. Hence all coefficient of $f$ are fixed by $\phi$ and so $f \in \mathcal{F}H[x]$. Clearly $f$ fulfills (ca),(cb), (cc) and (cb). Let $g$ be the minimal polynomial of $b$ over $\mathcal{F}H$. Then $g$ divides $f$. Also $\phi(g) = g$ and so as $b$ is a root of $g$, $\phi(a)$ is also. Hence $f$ divides $g$ and $f = g$. In particular, $f$ is irreducible. By 2.10.5 $|H/H_b| = |Hb|$ and so also (ce) holds.

Clearly (c) implies (a).

**Lemma 5.3.6 [lowerbound]** Let $\mathbb{F} : \mathbb{E} : \mathbb{L}$ with $\mathbb{E} : \mathbb{L}$ finite. Then

$$|\mathcal{G}\mathbb{L}/\mathcal{G}\mathbb{E}| \leq [\mathbb{E} : \mathbb{L}].$$
Proof: If $E = L$, this is obvious. So we may assume $E \neq L$. Pick $e \in E \setminus L$. Then $e$ is algebraic over $L$ and since $L \leq \mathcal{F}H$, $e$ is also algebraic over $\mathcal{F}L$. Moreover, $g = m^e_{\mathcal{F}L}$ divides $f = m^e_L$. By 5.3.5 applied to $H = \cal{G}L$, $H/H_e = \deg g$. Note that $H_e = \cal{G}(L[e])$ and so

$$[\mathcal{G}L : \mathcal{G}(L[e])] = \deg g \leq \deg f = [L[e] : L]$$

By induction on $[E : L]$,

$$[\mathcal{G}(L[e]) : \mathcal{G}E] \leq [E : L[e]].$$

Multiplying the two inequalities we obtain the result. □

Theorem 5.3.7 [closedbyfinite]

(a) Let $H \leq T \leq G$ with $H$ closed and $T/H$ finite. Then $T$ is closed and

$$[\mathcal{F}H : \mathcal{F}T] = |T/H|.$$

(b) Let $F : E : L$ with $L$ closed and $E : L$ finite. Then $E$ is closed and

$$[\mathcal{G}L : \mathcal{G}E] = [E : L].$$

Proof: (a) Using 5.3.2, 5.3.4, 5.3.6 and $H = \mathcal{G}FH$ we compute

$$|T/H| \geq |\mathcal{F}H : \mathcal{F}T| \geq |\mathcal{G}FT/\mathcal{G}FH| = |\mathcal{G}FT : H| \geq |T : H|.$$ 

So all the inequalities are equalities. Thus $T = \mathcal{G}FT$ and

$$[\mathcal{F}H : \mathcal{F}T] = |T/H|.$$

(b) similar to (a). □

Lemma 5.3.8 [finclo]

(a) Let $H \leq G$ be finite. Then $H$ is closed and $[F : \mathcal{F}H] = |H|$.

(b) Let $F : E : K$ with $E : K$ finite. Then $E$ is closed and $|G/\mathcal{G}E| = [E : K]$.

Proof: (a) Note that $\mathcal{F}\{e\} = F$ and so $\mathcal{G}Fe = \{e\}$. Hence trivial group is closed and has finite index in $H$. So (a) follows from 5.3.7a

(b) similar to (a). □

Definition 5.3.9 $E : L$ is called Galois if $L = \text{Fix}_{E} \text{Aut}_{L}(E)$. 

5.3. GALOIS THEORY

**Theorem 5.3.10 (Fundamental Theorem Of Galois Theory) [FTGaT]** Let \( F : \mathbb{K} \) be finite and Galois. Let \( G = \text{Aut}_{\mathbb{K}}(F) \). Then \( \mathcal{F} \) is a bijection from the set of subgroups of \( G \) to the set of intermediate field of \( F : \mathbb{K} \). Let \( H \leq G \) and \( E = FH \). Then \([F : E] = |H| \) and \( H = \text{Aut}_{E}(F) \).

**Proof:** All but the very last statement follow from 5.3.8 and 5.3.3. So it remains to show that \( H = \text{Aut}_{E}(F) \). Replacing \( E \) by \( F \) we may assume \( E = FH \). Thus \( H = GF(H) = G = \text{Aut}_{F}(F) \). \( \square \)

In the following *stable* will mean \( G \)-stable.

**Lemma 5.3.11 [basicstable]** Let \( F : E : \mathbb{K} \) be stable.

(a) Fix\(_{E}(G^{E}) = \mathbb{K} \) and \( E : \mathbb{K} \) is Galois.

(b) If \( E : \mathbb{K} \) is finite, then \( G^{E} = \text{Aut}_{\mathbb{K}}(E) \).

**Proof:** (a) Fix\(_{E}(G^{E}) = \text{Fix}_{F}(G \cap E = \mathbb{K} \cap E = \mathbb{K}) \)

(b) Follows from (a) and 5.3.10 applied to \( H = G^{E} \). \( \square \)

**Lemma 5.3.12 [stablefnormalg]**

(a) Let \( H \) be a normal subgroup of \( G \). Then \( \mathcal{F}H \) is stable.

(b) Let \( F : E : \mathbb{K} \) be stable. Then \( G^{E} \) is normal in \( G \) and \( G^{E} \cong G/G^{E} \).

(c) Let \( H \leq G \) be closed. Then \( H \) is normal in \( G \) if and only if \( \mathcal{F}H \) is stable.

(d) Let \( E \) be a closed subfield of \( F \). Then \( E \) is stable if and only if \( G^{E} \) is normal in \( G \).

**Proof:** Let \( \phi \in G, h \in H \) and \( b \in F \). Then

\[ h(b) = b \iff \phi(h(b)) = \phi(b) \iff \phi(h(\phi^{-1}(\phi(b)))) = \phi(b) \iff (h^\phi)(\phi(b)) = \phi(b) \]

Thus \( \mathcal{F}(H^\phi) = \phi(\mathcal{F}H) \) and (a) holds.

Note the \( G^{E} \) is exactly the kernel of the restriction map, \( \phi \to \phi|_{E} \). So (b) follows form ??.

(c) and (d) follow from (a), (b) and 5.3.3 \( \square \)

**Lemma 5.3.13 [stablennormal]** Let \( F : E : L \) with \( E : L \) algebraic, \( L \leq \mathbb{K} \) and \( \mathbb{K} : L \) purely inseparable. Then \( E \) is stable if and only if \( E \) is stable.
Suppose first that $E$ is stable. Let $e \in E$ and $f = m_e^L$. By 5.3.5, $f$ splits over $F$ and $Ge$ is the set of roots of $f$. As $E$ is stable, $Ge \leq E$ and so $f$ splits over $E$. Since $K/L$ is pure inseparable, $f^q \in L[x]$ for some $q \in \mathbb{N}$. So $m_e^L$ divides $f^q$. We conclude that $m_e^L$ splits over $E$ and so $E : L$ is normal.

If $E : K$ is normal, then $E$ is stable by 5.2.4

Lemma 5.3.14 [sepstano] Let $F : E : K$ with $E : K$ algebraic.

(a) $E : K$ is separable.

(b) If $E$ is closed then $E$ is stable if and only if $GE$ is normal in $G$.

Proof: (a) follows from 5.3.5.
(b) follows from 5.3.13 and 5.3.12d.

Theorem 5.3.15 [galnorsep] Let $E : K$ be an algebraic field extension. The the following are equivalent:

(a) $E : K$ is Galois

(b) $E : K$ is separable and normal.

(c) $E$ is the splitting field of a set over separable polynomials over $K$.

Proof: Suppose first that $E : K$ is Galois. Then by 5.3.14 (applied with $F = E$ ), $E : L$ is separable and normal.

Suppose next that $E : K$ is normal and separable. Then by ??g, $E : K$ is Galois.

Finally (b) and (c) are equivalent by 5.2.4b and 5.2.13b.

Proposition 5.3.16 [allclosed] Suppose that $F : K$ is algebraic and Galois, and let $G = \text{Aut}_F(K)$. Let $F : E : K$.

(a) $GE = \text{Aut}_F(E)$, $F : K$ is Galois and $E$ is closed .

(b) $E : K$ is Galois if and only of $GE$ is normal in $G$.

(c) $N_G(GE)/GE \cong N_G(GE)^E = \text{Aut}_E(K)$

Proof: (a) The first part of (a) is obvious. By 5.3.15a,b $F : K$ is normal and separable. Hence also $F : E$ is normal and separable. So by 5.3.15, $F : E$ is Galois. The last part of (a) follows from the first two.

(b) As $F : K$ is separable, $E : K$ is separable. Hence by 5.3.15 $E : K$ is Galois if and only if $E : K$ is normal. As $E$ is closed, (b) follows from 5.3.14b.

(c) As $FGE = E$, $E$ is $N_G(GE)$-stable. So $N_G(GE)/GE \cong N_G(GE)^E$ by the 2.5.5. Clearly $N_G(GE)^E \leq \text{Aut}_E(K)$. Let $\phi \in \text{Aut}_E(K)$. By 5.2.2 $\phi = \psi |_E$ for some $\psi \in \text{Aut}_K(F)$. Then $\psi \in N_G(GE)$ and (c) holds. □
Definition 5.3.17 Let $E : K$ be an algebraic field extension. A normal closure of $E : K$ is an extension $L$ of $E$ so that $L : K$ is normal and no proper proper subfield of $L$ containing $E$ is normal over $K$.

Lemma 5.3.18 [normalclosure] Let $E : K$ be an algebraic field extension.

(a) Let $E = K(I)$ for some $I \subseteq E$. Then $L : E$ is a normal closure of $E : K$ if and only if $L$ is a splitting field for $\{m^K_b | b \in I\}$ over $K$.

(b) There exists a normal closure $L$ of $E : K$ and $L$ is unique up to $E$-isomorphism.

(c) Let $L$ be a normal closure of $E : K$. Then

(ca) $L : K$ is finite if and only if $E : K$ is finite.

(cb) $L : K$ is Galois if and only if $L : K$ is separable and if and only if $E : K$ is separable.

Proof: (a) Suppose first that $L$ is a normal closure of $E : K$. The $L : K$ is normal and each $m^K_b, b \in I$ has a root in $L$. Hence each $m^K_b$ splits over $L$. Let $D$ be the subfield generated by $K$ and the roots of the $m^K_b$ in $L$. Then $D$ is a splitting field for $\{m^K_b | b \in I\}$ over $K$. Thus by ???b, $D : K$ is normal. Moreover, $I \subseteq D$ and so $E = K(I) \leq D$. Hence by the definition of a normal closure $L = D$.

Suppose next that $L$ is a splitting field of $\{m^K_b | b \in I\}$ over $K$. Then $L : K$ is normal. Also if $L : D : E$, then $D$ contains a root of each $m^K_b, b \in I$ and so each $m^K_b$ splits over $D$. Thus $D = L$.

(b) Follows from (a) applied to $I = E$.

(c) If $E : K$ is finite, then $E = K(I)$ for some finite subset $I \subseteq E$. Note the splitting field of a finite set of polynomials over $K$ has finite degree over $K$ So $L : K$ is finite by (a).

(d) This follows from (a) and 5.3.15. \qed

Let $\overline{K} : E : K$ with $E : K$ algebraic and $\overline{K}$ algebraically closed. Then $\overline{K}$ contains a unique normal closure $L$ of $E : K$. $L$ is called the normal closure of $E : K$ in $\overline{K}$.

5.4 The Fundamental Theorem of Algebra

In this section we show that the field $\mathbb{C}$ of complex numbers is algebraically closed. Our proof is based on the following well known facts from analysis which we will not prove:

Every polynomial $f \in \mathbb{R}[x]$ of odd degree has a root in $\mathbb{R}$.

Every polynomials of degree 2 over $\mathbb{C}$ is reducible.

$\mathbb{C}$ is the splitting field of $x^2 + 1$ over $\mathbb{R}$.

Some remarks on this assumptions. The first follows from the intermediate value theorem and the fact that any odd polynomial has positive and negative values. The second
follows from the quadratic formula and the fact that every complex number has a complex square root \((\sqrt{\tau e^{\theta i}} = \sqrt{\tau} e^{\frac{\theta}{2} i})\). The last is just the definition of \(\mathbb{C}\).

Let \(s\) be a prime. We say that \(f \in \mathbb{K}[x]\) is a \(s'\)-polynomial if \(s\) does not divide \(\deg f\). We say that \(E : \mathbb{K}\) is a \(s'\)-extension if \(E : \mathbb{K}\) is finite and \(s\) does not divide \([E : \mathbb{K}]\).

**Lemma 5.4.1 [noprime]** Let \(\mathbb{K}\) be a field and \(s\) a prime. The following are equivalent.

(a) Every irreducible \(s'\)-polynomial over \(\mathbb{K}\) has degree 1.

(b) Every \(s'\)-polynomial over \(\mathbb{K}\) has a root in \(\mathbb{K}\).

(c) \(\mathbb{K}\) has no proper \(s'\)-extension.

**Proof:** (a) \(\Rightarrow\) (b): Let \(g\) be a \(s'\)-polynomial over \(\mathbb{K}\). If the degree of every irreducible factor of \(g\) is divisible by \(s\), also \(\deg g\) is divisible by \(s\). Hence there exists an irreducible \(s'\)-factor of \(g\). The \(f\) has degree 1 and so \(f\) has a root in \(\mathbb{K}\). This root is also a root for \(g\).

(b) \(\Rightarrow\) (c): Let \(E : \mathbb{K}\) be an \(s'\)-extension. Let \(b \in E\). Then \(\deg m_b^E = [\mathbb{K}[b] : \mathbb{K}]\) divides \([E : \mathbb{K}]\). Hence \(m_b^E\) is an irreducible \(s'\)-polynomial and so by (b) has a root \(d\) in \(\mathbb{K}\). As \(f\) is irreducible we get \(b = d \in \mathbb{K}\) and \(E = \mathbb{K}\).

(c) \(\Rightarrow\) (a): Let \(f\) be irreducible in \(\mathbb{K}[x]\). Then \(\mathbb{K}[x]/(f)\) is an \(s'\)-extension of \(\mathbb{K}\). By (c) this extension is not proper. Thus \(\deg f = 1\).

**Proposition 5.4.2 [pprimep]** Let \(\mathbb{F} : \mathbb{K}\) be an algebraic extension and \(s\) a prime. Suppose that

(i) Every \(s'\)-polynomial over \(\mathbb{K}\) has a root in \(\mathbb{K}\).

(ii) All polynomials of degree \(s\) over \(\mathbb{F}\) are reducible.

Then \(\mathbb{F}\) is algebraically closed.

**Proof:** Let \(\overline{\mathbb{F}}\) be an algebraic closure of \(\mathbb{F}\). Suppose \(\overline{\mathbb{F}} \neq \mathbb{F}\) and let \(b \in \overline{\mathbb{F}} \setminus \mathbb{F}\). Let \(E\) the normal closure of \(\overline{\mathbb{K}}[b] : \mathbb{K}\) in \(\overline{\mathbb{F}}\). By 5.3.18ca, \(E : \mathbb{K}\) is finite and normal and \(b \in E\).

Let \(G = \text{Aut}_{\mathbb{K}}(E)\) and \(L = \text{Fix}_{\mathbb{K}}(G)\). Then by \(??\) \(L : \mathbb{K}\) is purely inseparable. Suppose \(L \neq \mathbb{K}\). Then \(\text{char } K = p\), \(p\) a prime. If \(p \neq s\), then \(L : \mathbb{K}\) is an \(s'\)-extension and so by 5.4.1 \(L = \mathbb{K}\). Thus \(p = s\). If \(L \not\subseteq \mathbb{F}\) then \(a^p \in \mathbb{F}\) for some \(a \in L \setminus \mathbb{F}\). 5.2.8 implies \(\deg m_a^E = p = s\), a contradiction to (ii). Thus in any case \(L \subseteq \mathbb{F}\).

By 2.11.3 there exists a Sylow \(s\)-subgroup \(S\) of \(G\). Then \([\text{Fix}_{\mathbb{K}}(S) : L] = |G : S|\). Let \(d \in \text{Fix}_{\mathbb{K}}(S)\) be separable over \(\mathbb{K}\) \(f = m_d^E\). As \(\deg f\) divides \(|G : S|\), \(f\) is a \(s'\)-polynomial. By \(??\) \(f = m_d^E\). So by assumption \(f\) has a root in \(\mathbb{K}\). Thus \(d \in \mathbb{K}\). So \(\text{Fix}_{\mathbb{K}}(S) : \mathbb{K}\) is purely inseparable and \(\text{Fix}_{\mathbb{K}}(S) = L\). Hence by 5.3.10, \(G = S\) and \(G\) is a \(s\)-group. Since \(L \subseteq \mathbb{F}\) 5.3.10 implies \(\mathbb{K} \cap F = \text{Fix}_{\mathbb{K}}(H)\) for some \(H \leq G\). If \(H = 1\), \(E = \mathbb{K}\). Thus \(H \neq 1\) and there exists a maximal subgroup \(T\) of \(H\). By 2.10.11, \(T \leq H\) and \(|H/T| = s\). Let \(d \in \text{Fix}_{\mathbb{K}}(T) \setminus \text{Fix}_{\mathbb{K}}(H)\). Then \(\deg m_d^{\mathbb{K} \cap F} = s\). By \(??\) we conclude \(\deg m_d^E = s\). Thus \([\mathbb{F}[d] : \mathbb{F}] = s\) a contradiction to (ii).\(\square\)
Theorem 5.4.3 (Fundamental Theorem of Algebra) [fta] The field of complex numbers is algebraically closed.

Proof: By the three properties of \( \mathbb{C} : \mathbb{R} \) listed above we can apply 5.4.2 with \( s = 2 \). Hence \( \mathbb{C} \) is algebraically closed. \( \square \)

Lemma 5.4.4 [embalgcl] Let \( E : \mathbb{K} \) be algebraic and \( \bar{\mathbb{K}} \) an algebraic closure of \( \mathbb{K} \). Then \( E \) is \( \mathbb{K} \)-isomorphic to some \( \bar{\mathbb{K}} : E : \mathbb{K} \).

Proof: Let \( \bar{\mathbb{K}} \) be an algebraic closure of \( E \). Then \( \bar{\mathbb{K}} : \mathbb{K} \) is algebraic and so \( \bar{\mathbb{K}} \) is an algebraic closure of \( \mathbb{K} \). By 5.2.2e there exists an \( \mathbb{K} \)-isomorphism \( \phi : E \to \bar{\mathbb{K}} \). Let \( \bar{E} = \phi(E) \). \( \square \)

Lemma 5.4.5 [extreals] Up to \( \mathbb{R} \)-isomorphisms, \( \mathbb{C} \) is the only proper algebraic extension of \( \mathbb{R} \).

Proof: Note that \( \mathbb{C} \) is an algebraic closure of \( \mathbb{R} \). So by 5.4.4 any algebraic extension of \( \mathbb{R} \) is \( \mathbb{R} \)-isomorphic to an intermediate field \( E \) of \( \mathbb{C} : \mathbb{R} \). As \( [\mathbb{C} : \mathbb{R}] = 2 \), we get \( E = \mathbb{R} \) or \( E = \mathbb{C} \). \( \square \)

5.5 Finite Fields

In this section we study the Galois theory of finite fields.

Lemma 5.5.1 [finitetof] Let \( \mathbb{F} \) be a finite field and \( \mathbb{F}_0 \) the subring generated by 1. Then \( \mathbb{F}_0 \cong \mathbb{Z}/p\mathbb{Z} \) for some prime \( p \). In particular, \( \mathbb{F} \) is isomorphic to a subfield of the algebraic closure of \( \mathbb{Z}/p\mathbb{Z} \).

Let \( p = \text{char} \mathbb{F} \). Then \( p\mathbb{Z} \) is the kernel of the homomorphism \( \mathbb{Z} \to \mathbb{F}, n \to n1 \). Also \( \mathbb{F}_0 \) is its image and so \( F_0 \cong \mathbb{Z}/p\mathbb{Z} \). \( \square \)

Theorem 5.5.2 [finitefields] Let \( p \) be a prime, \( \mathbb{F}_0 \cong \mathbb{Z}/p\mathbb{Z} \) a field of order \( p \), \( \mathbb{F} \) an algebraic closure of \( \mathbb{F}_0 \) and \( G = \{ \text{Frob}(p^n) \mid n \in \mathbb{Z} \} \subseteq \text{Aut}(\mathbb{F}) \).

(a) \( \mathbb{F}_0 = \text{Fix}_p(G) = \text{Fix}_p \text{Frob}(p) \).

(b) A proper subfield of \( \mathbb{F} \) is closed if and only if its finite.

(c) All subgroups of \( G \) are closed.

(d) \( G \) is a bijection between the finite subfields of \( \mathbb{F} \) and the non-trivial subgroups of \( G \).
(e) Let \( q \in \mathbb{Z}, q > 1 \). Then \( \mathbb{F} \) has a subfield of order \( q \) if and only if \( q \) is a power of \( p \). If \( q \) is a power of \( p \) then \( F \) has a unique subfield of order \( q, \mathbb{F}_q \).

(f) Let \( n \in \mathbb{Z}^+ \) and \( q = p^n \). Then
\[
\mathbb{F}_q = \text{Fix}_\mathbb{F}(\text{Frob}(q)) = \{ a \in \mathbb{F} \mid a^q = a \}
\]

So \( \mathbb{F}_q \) consists exactly of the roots of \( x^q - x \).

(g) \( \mathbb{F}_{p^m} \leq \mathbb{F}_{p^n} \) if and only if \( m \) divides \( n \).

(h) Let \( n \in \mathbb{Z}^+, m \in \mathbb{N} \) and \( q = p^n \). Then \( \mathbb{F}_{q^m} : \mathbb{F}_q \) is Galois and
\[
\text{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m} = \{ \text{Frob}(q^i) \mid 0 \leq i < m \}.
\]

In particular, \( \text{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m} \) is cyclic of order \( m \).

**Proof:** Note first that \( G = \langle \text{Frob}(p) \rangle \) is a cyclic subgroup of \( \text{Aut}(\mathbb{F}) \). Let \( H \) be a non-trivial subgroup of \( G \). Then \( H = \langle \text{Frob}(q) \rangle \) where \( q = p^n \) with \( n \in \mathbb{Z}^+ \). Put \( \mathbb{F}_q = \mathcal{F}H = \text{Fix}(\text{Frob}(q)) \). Let \( b \in \mathbb{F}_q \). Then \( b \in \mathbb{F}_q \) if and only if \( b^q = b \). \( \mathbb{F}_q \) consist exactly of the roots of \( x^q - x \). Note that \((x^q - x)' = qx^{q-1} - 1 = -1 \) has no roots and so by 3.6.11 \( x^q - x \) has no multiple roots. Hence \( |\mathbb{F}_q| = q \). In particular \( \mathbb{F}_0 = \mathbb{F}_p \) and (a) holds. Also \( \mathbb{F}_0 \) is closed and every proper closed subfield of \( \mathbb{F} \) is finite.

Since \( \mathbb{F}_q = \mathcal{F}H, \mathbb{F}_q \) is closed by 5.3.2e. Sp \( \mathcal{F}\mathcal{G}\mathcal{F}_q = \mathbb{F}_q \). Since \( H \) is the only subgroup of \( G \) with fixed field \( \mathbb{F}_q, \mathcal{G}\mathcal{F}_q = H = \langle \text{Frob}(q) \rangle \). Thus \( H \) is closed.

By 5.3.8b, every finite extension of \( \mathbb{F}_0 \) in \( \mathbb{F} \) is closed. So every finite subfield of \( \mathbb{F} \) is closed. Thus (b) to (f) are proved.

(g)
\[
\mathbb{F}_{p^n} \leq \mathbb{F}_{p^m} \iff \mathcal{G}\mathcal{F}_{p^n} \leq \mathcal{G}\mathcal{F}_{p^m} \iff \langle \text{Frob}(p^n) \rangle \leq \langle \text{Frob}(p^m) \rangle.
\]

By 2.6.1b this is the case if and only if \( m \) divides \( n \).

(h) Since \( H \) is abelian, all subgroups of \( H \) are normal. Hence by 5.3.14 (applied to \( (\mathbb{F}, \mathbb{F}_q, H) \) in place of \( (\mathbb{F}, \mathbb{K}, G) \) \( \mathbb{F}_{q^m} \) is \( H \)-stable. Thus by 5.3.11 (again applied with \( H \) in place of \( G \) \( \mathbb{F}_{q^m} : \mathbb{F}_q \) is Galois and \( \text{Aut}_{\mathbb{F}_q} \mathbb{F}_{q^m} = H^{\mathcal{F}_{q^m}} \). By 5.3.12b,
\[
H^{\mathcal{F}_{q^m}} \cong H/\mathcal{F}\mathcal{F}_{q^m} = \langle \text{Frob}(q^i) \rangle/\langle \text{Frob}(q^m) \rangle \cong \mathbb{Z}/m\mathbb{Z}.
\]

Thus (h) holds. \( \square \)

### 5.6 Transcendence Basis

Let \( \mathbb{F} : \mathbb{K} \) be a field extension and \( s = (s_i)_{i \in I} \) a family of elements in \( \mathbb{F} \). By 3.5.1 there exists a unique \( \mathbb{K} \)-homomorphism \( K[x_i, i \in I] \to K[s_i, i \in I] \) which sends \( x_i \) to \( s_i \). As before we will write \( f(s) \) for the image of \( f \) under this homomorphism.
We say that \( s \) is \textit{algebraically independent} over \( \mathbb{K} \) if this homomorphism is one to one. \( s \) is \textit{algebraically dependent} if \( s \) is not algebraically independent. Note that \( s \) is algebraically dependent if and only if there exists \( 0 \neq f \in \mathbb{K}[x_i, i \in I] \) with \( f(s) = 0 \). In particular, if \( |I| = 1 \), \( s \) is algebraically dependent over \( \mathbb{K} \) if and only if \( s \) is algebraic over \( \mathbb{K} \). Also since each \( f \in \mathbb{K}[x_i, i \in I] \) only involves finitely many variables, \( s \) is algebraically independent if and only if every finite subfamily is algebraically independent.

If \( s_i = s_j \) for some \( i \neq j \) then \( s \) is a root of \( x_i - x_j \) and so \( s \) is algebraically dependent. On the other hand, if the \( s_i \) are pairwise distinct, the notion of algebraic independence only depends on the set \( S = \{ s_i \mid i \in I \} \). This allows us to speak about algebraic dependence of subsets of \( \mathbb{F} \). Formally \( S \subseteq \mathbb{F} \) is algebraically independent over \( \mathbb{F} \) if the family \( (s)_{s \in S} \) is algebraically independent.

\textbf{Lemma 5.6.1 \textit{[evrat]}} Let \( \mathbb{F} : \mathbb{K} \) be a field extension and \( s = (s_i)_{i \in I} \) be algebraically independent over \( \mathbb{K} \). Then there exists a unique \( \mathbb{K} \)-isomorphism \( \alpha : \mathbb{K}(x_i, i \in I) \rightarrow \mathbb{K}(I) \) with \( \alpha(x_i) = s_i \).

\textbf{Proof:} By definition of algebraic independent, the map \( \mathbb{K}[x_i, i \in I] \rightarrow K[s_i, i \in I] \) is an isomorphism. In particular, \( f(s) \neq 0 \) for all \( 0 \neq f \in \mathbb{K}[s_i, i \in I] \). So \( f(s) \) is invertible in \( \mathbb{K}[x_i, i \in I] \). By 3.4.4 \( f \rightarrow f(s) \) extends unique to a ring homomorphism \( \alpha : \mathbb{K}(x_i, i \in I) \rightarrow \mathbb{K}(s_i, i \in I) \).

As is a field, \( \alpha \) is one to one. As \( \text{Im} \alpha \) is a subfield of \( \mathbb{K}(s_i, i \in I) \) and contains \( \mathbb{K}[s_i, i \in I] \), \( \alpha \) is onto. \( \square \)

If \( h = \frac{f}{g} \in K(x_i, i \in I) \), then \( \alpha(h) = \frac{f(s)}{g(s)} \). We will write \( h(s) \) for \( \alpha(s) \).

Recall that \( \mathbb{F}_D \) denotes the field of fraction of an integral domain \( D \).

\textbf{Lemma 5.6.2 \textit{[KIJ]}}

(a) Let \( D \) be an integral domain and \( I \) a set. Then there exists a unique \( D \)-isomorphism

\[ \mathbb{F}_D[x_i, i \in I] \rightarrow \mathbb{F}_D(x_i, i \in I) \]

which sends \( x_i \) to \( x_i \forall i \in I \).

(b) Let \( \mathbb{K} \) be a field and \( I \) and \( J \) disjoint sets. Then there exists a unique \( \mathbb{K} \) linear isomorphism

\[ \mathbb{K}(x_i, i \in I)(x_j, j \in J) \rightarrow \mathbb{K}(x_k, k \in I \cup J) \]

which send \( x_i \rightarrow x_i, \forall i \in I \) and \( x_j \rightarrow x_j, \forall j \in J \).

\textbf{Proof:} (a) Note that \( x_i \) is contained both in \( \mathbb{F} := \mathbb{F}_D[x_i, i \in I] \) and in \( \mathbb{F}_D(x_i, i \in I) \). To avoid confusion we will write \( y_i \) for \( x_i \) if \( x_i \) is viewed as an element of \( \mathbb{F} \). As \( D \leq \mathbb{F} \) and \( \mathbb{F} \) is a field, we can and will view \( \mathbb{F}_D \) as a subfield of \( \mathbb{F} \). Then \( \mathbb{F} = \mathbb{F}_D(y_i, i \in I) \), the subring of \( \mathbb{F} \) generated by \( \mathbb{F}_D \) and the \( y_i, i \in I \). In view of 5.6.1 it suffices to show that \( y = (y_i)_{i \in I} \) is algebraically independent over \( \mathbb{F}_D \). So suppose that \( f(y) = 0 \) for some \( f \in \mathbb{F}_D[x_i, i \in I] \).
Then \( df \in D[x_i, i \in I] \) for some \( 0 \neq d \in D \). Let \( g = df \). Then \( g(y) = 0 \). But as \( D[x_i, i \in I] \) is an integral domain the map \( D[x_i, i \in I] \to \mathbb{F}^D[x_i, i \in I], h \mapsto h(y) \) is a monomorphism. Thus \( g = 0 \). As \( D \) is an integral domain we conclude \( f = 0 \).

(b) Put \( D := \mathbb{K}[x_i, i \in I] \). By 3.5.2, \( D[x_j, j \in J] \) and \( \mathbb{K}[x_k, k \in I \cup J] \) are canonically isomorphic. Note that \( \mathbb{K}(x_i, i \in I) \) is the field of fraction of \( D \) and \( \mathbb{K}(x_k, k \in I \cup J) \) is the field of fraction of \( \mathbb{K}[x_k, k \in I \cup J] \cong D[x_j, j \in J] \). Thus (b) follows from (a).

**Lemma 5.6.3** [indepindep] Let \( \mathbb{F} : \mathbb{K} \) be a field extension.

(a) Let \( S \) and \( T \) disjoint subsets of \( \mathbb{F} \). Then \( S \cup T \) is algebraically independent over \( \mathbb{K} \) if and only if \( S \) is algebraically independent over \( \mathbb{K} \) and \( T \) is algebraically independent over \( \mathbb{K}(S) \).

(b) Let \( S \) be an algebraically independent subset of \( \mathbb{F} : \mathbb{K} \) and \( b \in \mathbb{F} \) with \( b \notin S \). Then \( S + b \) is algebraically independent over \( \mathbb{K} \) if and only if \( b \) is transcendental over \( \mathbb{K} \).

**Proof:** (a) \( S \cup T \) is algebraically independent if and only if there exists an \( \mathbb{K} \)-isomorphism \( \mathbb{K}(x_r, r \in S \cup T) \to \mathbb{K}(S \cup T) \) with \( x_r \to r, \forall r \in S \cup T \). \( S \) algebraically independent over \( \mathbb{K} \) and \( T \) algebraically independent over \( \mathbb{K}(S) \) is equivalent to the existence of a \( \mathbb{K} \)-isomorphism \( \mathbb{K}(x_s, s \in S)(x_t, t \in T) \to K(S)(T) \) with \( x_s \to s, \forall s \in S \) and \( x_t \to t, \forall t \in T \). Since \( K(S \cup T) = K(S)(T) \) we conclude from 5.6.2b that the two property are equivalent.

(b) Follows from (a) applied to \( T = \{b\} \). \( \square \)

**Definition 5.6.4** Let \( \mathbb{F} : \mathbb{K} \) be a field extension. A transcendence basis for \( \mathbb{F} : \mathbb{K} \) is a algebraically independent subset \( S \) of \( \mathbb{F} : \mathbb{K} \) so that \( \mathbb{F} \) is algebraic over \( \mathbb{K}(S) \).

**Lemma 5.6.5** [basictransbasis] Let \( \mathbb{F} : \mathbb{K} \) be field extension and \( S \) an algebraically independent subset of \( \mathbb{F} : \mathbb{K} \).

(a) \( S \) is a transcendence basis if and only if \( S \) is a maximal (with respect to inclusion) algebraically independent subset of \( \mathbb{F} : \mathbb{K} \).

(b) \( S \) is contained in a transcendence basis for \( \mathbb{F} : \mathbb{K} \).

(c) \( \mathbb{F} : \mathbb{K} \) has a transcendence basis.

**Proof:** (a) \( S \) is a maximal algebraically independent set if and only if \( S + b \) is algebraically dependent for all \( b \in \mathbb{F} \setminus S \). By 5.6.3b, this is the case if and only if all \( b \in \mathbb{F} \) are algebraic over \( \mathbb{K}(S) \).

(b) Let \( \mathcal{M} \) be the set of algebraically independent subsets of \( \mathbb{F} : \mathbb{K} \) containing \( S \). Since \( S \in \mathcal{M}, \mathcal{M} \) is not empty. Order \( \mathcal{M} \) by inclusion. Then \( \mathcal{M} \) is a partially ordered set. We would like to apply Zorn’s lemma. So we need to show that every chain \( \mathcal{D} \) of \( \mathcal{M} \) has an upper bound. Note that the elements of \( \mathcal{D} \) are subsets on \( \mathbb{F} \). So we can build the union \( D := \bigcup \mathcal{D} \). Then \( E \subseteq D \) for all \( E \in \mathcal{D} \). Thus \( D \) is an upper bound for \( \mathcal{D} \) once we
establish that $D \in \mathcal{M}$. That is we need to show that $D$ is algebraically independent over $\mathbb{K}$. As observed before we just this amounts to showing that each finite subset $J \subseteq D$ is algebraically independent. Now each $j \in J$ lies in some $E_j \in \mathcal{D}$. Since $\mathcal{D}$ is totally ordered, the finite subset $\{E_j \mid j \in J\}$ of $\mathcal{D}$ has a maximal element $E$. Then $j \in E_j \subseteq E$ for all $j \in J$. So $J \subseteq E$ and as $E$ is algebraically independent, $J$ is as well.

Hence every chain in $\mathcal{M}$ has an upper bound. By Zorn’s Lemma A.1 $\mathcal{M}$ has a maximal element $T$. By (a) $T$ is a transcendence basis and by definition of $\mathcal{M}$, $S \subseteq T$.

(c) follows from (b) applied to $S = \emptyset$. 

\[ \text{Proposition 5.6.6 [cardtranbas]} \text{ Let } \mathbb{F} : \mathbb{K} \text{ be a field extension and } S \text{ and } T \text{ transcendence basis for } \mathbb{F} : \mathbb{K}. \text{ Then } |S| = |T|. \]

\[ \text{Proof:} \text{ Well order } S \text{ and } T. \text{ For } s \in S \text{ define } s^- : = \{ b \in S \mid b < s \} \text{ and } s^+ : = \{ b \in S, b \leq s \}. \text{ Similarly define } t^\pm \text{ for } t \in T. \text{ Let } s \in S. \text{ As } \mathbb{F} : \mathbb{K}(I) \text{ is algebraic there exists a finite subset } J \subseteq T \text{ so that } s \text{ is algebraic over } \mathbb{K}(s^-, J). \text{ Let } j \text{ be the maximal element of } J. \text{ Then } J \subseteq t^+ \text{ and so } s \text{ is algebraic over } K(s^-, j^+). \text{ Hence we can define a function } \phi : S \rightarrow T, \text{ where } \phi(s) \in T \text{ is minimal with respect to } s \text{ being algebraic over } \mathbb{K}(s^-, \phi(s)^+). \text{ Similarly define } \psi : T \rightarrow S.

\text{We will show that } \phi \text{ and } \psi \text{ are inverse to each other. Let } s \in S \text{ and put } t = \phi(s). \text{ Let } L = \mathbb{K}(s^-, t^-). \text{ We claim that } s \text{ is transcendental over } L. \text{ If not we can choose } J \text{ as above with } J \subseteq t^- \text{. But then } s \text{ is algebraic over } \mathbb{K}(s^-, j^+). \text{ Since } j < t \text{ this contradicts the minimal choice of } t. \text{ Note that } s \text{ is algebraic over } \mathbb{L}(t). \text{ If } t \text{ is algebraic over } \mathbb{L} \text{ we conclude that } s \text{ is algebraic over } \mathbb{L}, \text{ a contradiction. Hence } t \text{ is transcendental over } \mathbb{L}. \text{ In particular } \psi(t) \neq s. \text{ Since } s \text{ is algebraic over } \mathbb{L}(t), t, s \text{ are algebraic dependent over } \mathbb{L}. \text{ As } t \text{ is transcendental 5.6.5b implies that } t \text{ is algebraic over } \mathbb{L}(s) = \mathbb{K}(s^+, t^-). \text{ Thus by definition of } \psi, \psi(t) \leq s. \text{ Hence } \psi(t) = s \text{ and } \psi \circ \phi = \text{id}_S. \text{ By symmetry } \phi \circ \psi = \text{id}_T \text{ and so } \phi \text{ is a bijection.} \]

In view of the preceding lemma one defines the transcendence degree $\text{tr deg}(\mathbb{F} : \mathbb{K})$ of $\mathbb{F} : \mathbb{K}$ to be $|S|$, where $S$ is any transcendence basis for $\mathbb{F} : \mathbb{K}$.

Let $\mathbb{K}$ be a field and $s$ transcendental over $\mathbb{K}$. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{K}(s)$. Let $s_0 = s$ and inductively let $s_{i+1}$ be a root of $x^2 - s_i$. Then $s_i = s_{i+1}^2$. Then $\mathbb{K}(s_i) \leq \mathbb{K}(s_{i+1})$. Let $E = \bigcup_{i=0}^{\infty} \mathbb{K}(s_i)$. Then $E : \mathbb{K}(s_i)$ is algebraic. Also as $s$ is transcendental over $\mathbb{K}$, each $s_i$ is transcendental over $\mathbb{K}$. Thus each $\{s_i\}$ is a transcendence basis for $E : \mathbb{K}$. Note also that $K(b) \neq E$ for all $b \in E$. Indeed, as $b$ is algebraic over $\mathbb{K}$, $K(b) : \mathbb{K}$ is finite while $E : \mathbb{K}$ is infinite.

## 5.7 Algebraically Closed Fields

In this section we study the Galois theory of algebraically closed field.

\[ \text{Lemma 5.7.1 [isoalgclo]} \text{ Let } \phi : \mathbb{K}_1 \rightarrow \mathbb{K}_2 \text{ be a field isomorphism and } \mathbb{F}_i : \mathbb{K}_i \text{ and algebraically closed field extension of } \mathbb{K}_i \text{ with } \text{tr deg}(\mathbb{F}_1 : \mathbb{K}_1) = (\text{tr deg} \mathbb{F}_2 : \mathbb{K}_2). \text{ Then } \phi \text{ extends to an isomorphism } \psi : \mathbb{F}_1 \rightarrow \mathbb{F}_2. \]
**Proof:** Let $S_i$ be a transcendence basis for $F_i : K_i$. By assumption there exists a bijection $\lambda : S_1 \to S_2$. By 5.6.1 there exists a unique isomorphism

$$
\delta : K_1(S_1) \to K_2(S_2)
$$

with $\delta(k) = \phi(k), \forall k \in K_1$ and $\delta(s) = \phi(s), \forall s \in S_1$. Since $F_i : K_i(S_i)$ is algebraically closed, $F_i$ is an algebraically closure of $K_i(S_i)$. Hence by ??a, $\delta$ extends to an isomorphism $\psi : F_1 \to F_2$. \hfill \Box

Let $K$ be the field, Let $K_0$ be the intersection of all the subfield of $K$. Then $K_0 \cong \mathbb{Q}$ if char $K = 0$ and $K_0 \cong \mathbb{Z}/p\mathbb{Z}$ if char $K = p \neq 0$. $K_0$ is called the ground field of $K$.

**Corollary 5.7.2 [classalgclo]**

(a) Let $K$ be a field. Then for each cardinality $c$ there exists a unique (up to $K$-isomorphism) algebraically closed field extension $F : K$ with $\text{tr deg} F : K = c$. The algebraic closure of $K(x_i, i \in I)$, where $I$ is a set with $|I| = c$ is such an extension.

(b) Let $p = 0$ or a prime and $c$ a cardinality. Then there exists a unique (up to isomorphism) algebraically closed field with characteristic $p$ and transcendence degree $c$ over its ground field. The algebraic closure of $\mathbb{F}_p(x_i, i \in I)$, where $I$ is a set with cardinality $|I|$ and $\mathbb{F}_p$ is $\mathbb{Q}$ respectively $\mathbb{Z}/p\mathbb{Z}$, is such a field.

**Proof:** Follows immediately from 5.7.1 \hfill \Box

**Lemma 5.7.3 [perfectfields]** Let $K$ be a field. Then the following are equivalent.

(a) $K$ has no proper purely inseparable field extension.

(b) Let $K$ be an algebraic closure of $K$. Then $K : K$ is Galois.

(c) All polynomials over $K$ are separable.

(d) char $K = 0$ or char $K = p \neq 0$ and for each $b \in K$ there exists $d \in K$ with $d^p = b$.

(e) char $K = 0$ or char $K = p \neq 0$ and $\text{Frob}(p)$ is an automorphism.

**Proof:** (a) $\Rightarrow$ (b): Follows from ??.

(b) $\Rightarrow$ (c): As $K : K$ is Galois, 5.3.15 implies that $K : K$ is separable. Let $f \in K[x]$ be irreducible. Then $f$ has root in $K$. This root is separable over $K$ and so $f$ is separable.

(c) $\Rightarrow$ (d) Let $b \in K$ and $f$ an irreducible monic factor of $x^p - b$. The $f$ has a unique root in $K$ and is separable. Thus $f = x - d$ for some $d \in K$ with $d^p = b$.

(d) $\Rightarrow$ (e) By 5.2.7 $\text{Frob}(p)$ is a monomorphism. By (d) $\text{Frob}(p)$ is onto.

(e) $\Rightarrow$ (a) Let $F : K$ be purely inseparable. Let $b \in F$. Then $d := b^{p^n} \in K$ for some $n \in \mathbb{N}$. Then $b = \text{Frob}(p)^{-n}(d) \in K$ and $F = K$. \hfill \Box

A field $K$ which fulfills the equivalent conditions of the preceding lemma is called perfect.
Lemma 5.7.4 [fialgcloper] Finite fields and algebraically closed fields are perfect.

Proof: Let $\mathbb{K}$ be a field. If $\mathbb{K}$ is finite, then as $\text{Frob}(p)$ is one to one, its onto. If $\mathbb{K}$ is algebraically closed, $\text{Frob}(p)$ is an automorphism by 5.2.7d. \qed

Lemma 5.7.5 [trantran] Let $\mathbb{F} : \mathbb{K}$ be an algebraically closed field extension. Then $\text{Aut}_{\mathbb{K}}(\mathbb{F})$ acts transitively on the set of elements in $\mathbb{F}$ transcendental over $\mathbb{K}$.

Proof: Let $s_i \in \mathbb{F}$, $i = 1, 2$ be transcendental over $\mathbb{K}$. By 5.6.5b there exists a transcendence basis $S_i$ for $\mathbb{F} : \mathbb{K}$ with $s_i \in S_i$. Let $\lambda : S_1 \to S_2$ be a bijection with $\lambda(s_1) = s_2$. By 5.7.1 there exists $\psi \in \text{Aut}_{\mathbb{K}}(\mathbb{F})$ with $\psi(s) = \lambda(s)$ for all $s \in S_1$. Thus $\psi(s_1) = s_2$. \qed

Proposition 5.7.6 [galalgclo] Let $\mathbb{F} : \mathbb{K}$ be an algebraically closed field extension. and $G = \text{Aut}_{\mathbb{K}}(\mathbb{F})$. Let $\mathbb{F}$ consists of all the elements in $\mathbb{F}$ which are purely inseparable over $\mathbb{K}$ and $\mathbb{A}$ of all the elements which are algebraic over $\mathbb{A}$. Let $\mathbb{F} : \mathbb{E} : \mathbb{K}$ with $\mathbb{E} \neq \mathbb{K}$

(a) If $\mathbb{E}$ is $G$-stable then $\mathbb{E}^G = \text{Aut}_{\mathbb{K}}(\mathbb{E})$.

(b) $\mathbb{E}$ is $G$-stable if and only $\mathbb{E} : \mathbb{K}$ is normal.

(c) $\text{Fix}_\mathbb{F}(G) = \mathbb{F}$.

(d) $\mathbb{E}$ is $G$-closed if and only if $\mathbb{E}$ is perfect.

(e) $\text{Aut}_{\mathbb{A}}(\mathbb{F})$ is the unique minimal non-trivially closed normal subgroup of $G$.

Proof: (a) By 5.7.1 every $\phi \in \text{Aut}_{\mathbb{K}}(\mathbb{E})$ can be extended to $\psi \in \text{Aut}_{\mathbb{K}}(\mathbb{F})$. So (a) holds.

(b) If $\mathbb{E} : \mathbb{K}$ is normal the by 5.2.4a, $\mathbb{E}$ is $G$-stable. So suppose now that $\mathbb{E} : \mathbb{K}$ is $G$-stable. Suppose that $\mathbb{E} \not\subset \mathbb{A}$ and pick $e \in \mathbb{E}$ so that $e$ is transcendental over $\mathbb{K}$. By 5.7.5 $Gs$ consists of all the transcendental elements in $\mathbb{F}$. As $\mathbb{E}$ is $G$-stable, $Ge \subseteq \mathbb{F}$. So $\mathbb{E}$ contains all the transcendental elements. Let $b \in \mathbb{A}$.

If $b + e$ is algebraic over $\mathbb{K}$ we conclude that $\mathbb{K}(b + e) : \mathbb{K}$ are algebraic. Since $e \in \mathbb{K}(b + e)$ we conclude that $e$ is algebraic over $\mathbb{K}$, a contradiction.

Hence $b + e$ is transcendental. Thus $b + e \in \mathbb{E}$ and $b \in \mathbb{K}(b + e, e) \subseteq \mathbb{E}$. It follows that $\mathbb{F} = \mathbb{E}$, a contradiction to the assumptions.

Hence $\mathbb{E} \subseteq \mathbb{A}$. By (a) $\mathbb{A}^G = \text{Aut}_{\mathbb{K}}(\mathbb{A})$. Hence $\mathbb{E}$ is $\text{Aut}_{\mathbb{K}}(\mathbb{A})$ stable and so by 5.3.13 $\mathbb{E} : \mathbb{K}$ is normal.

(c) By ?? $\text{Fix}_\mathbb{F}(G) \leq \mathbb{A}$. Thus (c) follows form ??g.

(d) Replacing $\mathbb{K}$ by $\mathbb{E}$ and $G$ by $\text{Aut}_\mathbb{F}(G)$ we may assume $\mathbb{K} = \mathbb{E}$. Also by (a) we may assume $\mathbb{F} = \mathbb{A}$. So $F$ an algebraic closure of $\mathbb{K}$. Note $\mathbb{E}$ is closed if and only if $\mathbb{F} : \mathbb{E}$ is Galois. So by ?? if and only if $\mathbb{E}$ is perfect.

(e) By (b) $\mathbb{A}$ is the unique maximal stable proper subfield of $\mathbb{F}$. So (e) follows from 5.3.12. \qed
Chapter 6

Multilinear Algebra

Throughout this chapter ring means commutative ring with identity $1 \neq 0$. All modules are assumed to be unitary. We will write (non)-commutative ring for a ring which might not be commutative.

6.1 Multilinear functions and Tensor products

Let $(M_i, i \in I)$ be a family of sets. For $J \subseteq I$ put $M_J = \prod_{j \in J} M_j$ and for $m = (m_i)_{i \in I} \in M_I$ put $m_J = (m_j)_{j \in J} M_J$. If $I = J \cup K$ with $L \cap K = \emptyset$, the map $M_I \to M_J \times M_K, m \to (m_J, m_K)$ is a bijection. We use this canonical bijection to identify $M_I$ with $M_J \times M_K$.

Let $W$ be a set and $f : M_I \to W$ a function. Let $b \in M_K$. Then we obtain a function a function $f_b : M_J \to W, a \to f(a, b)$.

**Definition 6.1.1** Let $R$ a ring, $M_i, i \in I$ a family of $R$-modules and $W$ an $R$-module. Let $f : M_I \to W$ be a function. $f$ is $R$-multilinear if for all $i \in I$ and all $b \in M_{I-i}$ the function

$$f_b : M_i \to W, a \to f(a, b)$$

is $R$-linear.

Note here that $f_b$ $R$-linear just means $f(ra, b) = rf(a, b)$ and $f(a+\tilde{a}, b) = f(a, b)+f(\tilde{a}, b)$ for all $r \in R, a \in M_i, b \in M_{I-i}$ and $i \in I$.

The function $f : R^n \to R, (a_1, a_2, \ldots, a_n) \to a_1 a_2 \ldots a_n$ is multilinear. But the function $g : R^n \to R, (a_1, \ldots, a_n) \to a_1$ is not $R$-linear.

**Lemma 6.1.2** [restricting multilinear maps] Let $M_i, i \in I$ be a family of $R$-modules, $f : M_I \to W$ an $R$-multilinear map, $I = J \sqcup K$ and $b \in M_K$. Then $f_b : M_J \to W$ is $R$-multilinear.

**Proof:** Let $j \in J$ and $a \in M_{J-j}$. Then $(a, b) \in M_{I-j}$ and $(f_b)a = f(a, b)$ is $R$-linear. So $f_b$ is $R$-multilinear. \(\square\)
Lemma 6.1.3 [alternative definition of multilinear] Let $R$ be a ring, $M_i, i \in I$ a finite family of $R$-modules, $W$ an $R$-module and $f : M_I \rightarrow W$ be a function. Then $f$ is multilinear if and only if

$$f((\sum_{j \in J_i} r_{ij}m_{ij})_{i \in I}) = \sum_{\alpha \in J_K} (\prod_{i \in K} r_{i\alpha(i)})f((m_{i\alpha(i)})_{i \in I})$$

whenever $(J_i, i \in I)$ is a family of sets, $m_{ij} \in M_i$ and $r_{ij} \in R$ for all $i \in I$ and $j \in J_i$.

**Proof:** Suppose first that $f$ is multilinear. If $|I| = 1$ we need to show that $f(\sum_{j \in J} r_jm_j) = \sum_{j \in J} r_j f(m_j)$ But this follows easily from the fact that $f$ is linear and induction on $J$. So suppose that $|I| \geq 2$, let $s \in I$, $K = I - s$. Then by induction

$$f((\sum_{j \in J_i} r_{ij}m_{ij})_{i \in I}) = f(\sum_{s \in J_s} r_{s_j}m_{s_j})((\sum_{j \in J_i} r_{ij}m_{ij})_{i \in K})$$

$$= \sum_{\alpha \in J_K} (\prod_{i \in K} r_{i\alpha(i)})f(\sum_{s \in J_s} r_{s_j}m_{s_j}, (m_{i\alpha(i)})_{i \in K})$$

$$= \sum_{\alpha \in J_K} (\prod_{i \in K} r_{i\alpha(i)})f(m_{i\alpha(i)})$$

The other direction is obvious. \(\square\)

**Example:** Suppose $f : M_1 \times M_2 \times M_3 \rightarrow W$ is multilinear. Then

$$f(m_{11} + 2m_{12}, 4m_{21}, 3m_{31} + m_{32}) =$$

$$= 12f(m_{11}, m_{21}, m_{31}) + 4f(m_{11}, m_{21}, m_{32}) + 24f(m_{12}, m_{21}, m_{31}) + 8f(m_{12}, m_{21}, m_{32})$$

**Definition 6.1.4** Let $R$ be a ring and $M_i, i \in I$ a family of $R$-modules. A tensor product for $(M_i, i \in I)$ over $R$ is an $R$-multilinear map $f : M_I \rightarrow W$ so that for each multilinear map $g : M_I \rightarrow \tilde{W}$ there exists a unique $R$-linear $\tilde{g} : W \rightarrow \tilde{W}$ with $g = \tilde{g} \circ f$.

**Lemma 6.1.5 [existence of tensor products]** Let $R$ be a ring and $(M_i, i \in I)$ a family of $R$-modules. Then $(M_i, i \in I)$ has a tensor product over $R$. Moreover, it is unique up to isomorphism, that is if $f_i : M_I \rightarrow W_i, i = 1, 2$, are tensor products, than there exists a $R$-linear isomorphism $g : W_1 \rightarrow W_2$ with $f_2 = g \circ f_1$.

**Proof:** Let $F = F_R(M_I)$, the free module on the set $M_I$. So $F$ has a basis $z(m), m \in M_I$. Let $D$ be the $R$-submodule if $F$ generated by the all the elements in $F$ of the form

$$z(ra, b) - rz(a, b)$$
and

\[ z(a, b) + z(\tilde{a}, b) - z(a + \tilde{a}, b) \]

where \( r \in R, a \in M_i, b \in M_{I-i} \) and \( i \in I \).

Let \( W = F/D \) and define \( f : M_I \to W, m \to z(m) + D \).

To check that \( f \) is multilinear we compute

\[ f(ra, b) - rf(a, b) = (z(ra, b) + D) - r(z(a, b) + D) = (z(ra, b) - rz(a, b)) + D = D = 0_W \]

and

\[ f(a+\tilde{a}, b) - f(a, b) - f(\tilde{a}, b) = (z(a+\tilde{a}, b) + D) - (z(a, b) + D) - z(\tilde{a}, b) + D) = (z(a+\tilde{a}, b) - z(a, b) - z(\tilde{a}, b)) + D = D = 0_W \]

So \( f \) is \( R \)-multilinear.

To verify that \( f \) is a tensor product let \( \tilde{f} : M_I \to \tilde{W} \) by \( R \)-multilinear. Since \( F \) is a free with basis \( z(m), m \in M \). There exists a unique \( R \)-linear map \( \tilde{g} : F \to \tilde{W} \) with \( \tilde{g}(z(m)) = \tilde{f}(m) \) for all \( m \in M_I \). We claim that \( D \leq \ker \tilde{g} \). Indeed

\[ \tilde{g}(z(ra, b) - rz(a, b)) = \tilde{g}(z(ra, b) - rf(a, b), \) \]

Here the first equality holds since \( \tilde{g} \) is \( R \)-linear and the second since \( \tilde{f} \) is multilinear.

Similarly \( \tilde{g}(z(a + \tilde{a}) - z(a, b) - z(\tilde{a}, b)) = \tilde{g}(z(a + \tilde{a})) - \tilde{g}(z(a, b)) - \tilde{g}(z(\tilde{a}, b)) = \tilde{f}(a + \tilde{a}) - f(a, b) - f(\tilde{a}, b) = 0. \)

Hence \( \ker \tilde{g} \) contains all the generators of \( D \) and since \( \ker \tilde{g} \) is an \( R \)-submodule of \( F \), \( D \leq \ker \tilde{g} \). Thus the map \( g : W \to \tilde{W}, e + D \to \tilde{g}(e) \) is well defined and \( R \)-linear. Note that \( g(\tilde{f}(m)) = \tilde{g}(\tilde{f}(m)) = \tilde{g}(z(m)) = \tilde{f}(m) \) and so \( \tilde{f} = g \circ f \). To show the uniqueness of \( g \) suppose that \( h : W \to \tilde{W} \) is \( R \)-linear with \( \tilde{f} = h \circ f \). Define \( \tilde{h} : F \to \tilde{W} \) by \( \tilde{h}(e) = h(e + D) \).

Then \( h \) is \( R \) linear and \( \tilde{h}(z(m)) = h(z(m) + D) = h(f(m)) = \tilde{f}(m) = \tilde{g}(z(m)) \). Since \( z(m) \) is a basis for \( F \) this implies \( \tilde{h} = \tilde{g} \). Thus \( g(e + D) = \tilde{g}(e) = \tilde{h}(e) = h(e + D) \) and \( g = h \), as required.

So \( f \) is indeed a tensor product.

Now suppose that \( f_i : M_I \to W_i, i=1,2 \) are tensor products for \( (M_i, i \in I) \) over \( R \). Let \( \{1, 2\} = \{i, j\} \). Since \( f_i \) is a tensor product and \( f_j \) is multilinear, there exists \( g_i : W_i \to W_j \) with \( f_j = g_i f_i \). Then \( (g_j g_i) f_i = g_j (g_i f_i) = g_j f_j = f_j \). Note that also \( \text{id}_{W_i} f_i = f_i \) and so the uniqueness assertion in the definition of the tensor product implies \( g_j g_i = \text{id}_{W_i} \). Hence \( g_1 \) and \( g_2 \) are inverse to each other and \( g_i \) is a \( R \)-linear isomorphism. \( \square \)

Let \( (M_i, i \in I) \) be a family of \( R \)-modules and \( f : M_I \to W \) a tensor product. We denote \( W \) by \( \bigotimes_{i \in I} M_i \). f((m_i)_{i \in I} \) by \( \otimes_{i \in I} m_i \). Also if there is no doubt about the the ring \( R \) and the set \( I \) in question, we just use the notations \( \bigotimes M_i, \otimes m_i \) and \( (m_i) \).

If \( I == \{1, 2 \ldots , n\} \) we also write \( M_1 \otimes M_2 \otimes \ldots \otimes M_n \) for \( \bigotimes M_i \) and \( m_1 \otimes m_2 \otimes \ldots \otimes m_n \) for \( \otimes m_i \).

With this notation we see from the proof of 6.1.5 \( \bigotimes M_i \) is as an \( R \)-module generated by the elements of the form \( \otimes m_i \). But these elements are not linear independent. Indeed we have the following linear dependence relations:
\( (ra) \otimes b = r(a \otimes b) \) and \( (a + \hat{a}) \otimes b = a \otimes b + \hat{a} \otimes b. \)

Here \( r \in R, a \in M_i, b = \otimes_{j \in J} b_j \) with \( b_j \in M_j \) and \( i \in I \).

**Lemma 6.1.6 [tensor powers of \( R \)]** Let \( I \) be finite. Then \( \bigotimes^I R = R \). More precisely, \( f : R^I \to R, (r_i) \to \prod_{i \in I} r_i \) is a tensor product of \((R, i \in I)\).

**Proof:** We need to verify that \( f \) meets the definition of the tensor product. Let \( \tilde{f} : R^I \to \tilde{W} \) be \( R \)-multilinear. Define \( g : R \to \tilde{W}, r \to r \tilde{f}(1) \)), where \((1)\) denotes the element \( r \in R^I \) with \( r_i = 1 \) for all \( i \in I \). Then clearly \( g \) is \( R \)-linear. Moreover,

\[
\tilde{f}(r_i) = \tilde{f}(r_i1) = \left( \prod_{i \in I} r_i \right) \tilde{f}(1) = g(\prod_{i \in I} r_i) = g(f(r_i))
\]

Thus \( \tilde{f} = gf \).

Next let \( \tilde{g} : R \to \tilde{W} \) be linear with \( \tilde{f} = \tilde{g}f \). Then \( \tilde{g}(r) = \tilde{g}(r1) = r\tilde{g}(1) = r\tilde{g}(\prod_{i \in I} 1) = rg(f(1)) = r\tilde{f}(1) = g(r) \) and so \( g \) is unique. \( \square \)

**Lemma 6.1.7 [composition of multilinear maps]** Let \((M_i, i \in I)\) be a family of \( R \)-modules. Suppose that \( I \) is the disjoint union of subsets \( I_j, j \in J \). For \( j \in J \) let \( f_j : M_{I_j} \to W_j \) be \( R \)-multilinear. Also let \( g : W_J \to W \) be \( R \)-multilinear. Then

\[
g \circ (f_j) : M_I \to W, m \to g((f_j(m_j))
\]

is \( R \)-multilinear.

**Proof:** Let \( f = g \circ (f_j) \). Let \( m \in M_I \) and put \( w_j = f_j(m_j) \). Let \( w = (w_j) \in W_J \). Then \( f(m) = g(w) \).

Let \( i \in I \) and pick \( j \in J \) with \( i \in I_j \). Put \( b = (m_k)_{k \in I-i} \) and \( v = (w_k)_{k \in J} \). Then \( w = (w_j, v), m = (m_i, b) \) and \( f_0(m_i) = f(m) = g(w_j, v) = g_v(w_j) \). Let \( d = (m_k)_{k \in I_j-i} \). Then \( m_{I_j} = (m_i, d) \). Thus \( w_j = f_j(m_{I_j}) = f_j(m_i, d) = (f_j)_d(m_i) \).

Hence \( f_b(m_i) = g_v(w_j) = g_v((f_j)_d(m_i)) \). So \( f_b = g_v \circ (f_j)_d \). Since \( g \) is multilinear, \( g_v \) is \( R \) linear. Since \( f_j \) is a multilinear product, \((f_j)_d \) is \( R \)-linear. Since the composition of \( R \)-linear maps are \( R \)-linear, \( f_b \) is \( R \)-linear. So \( f \) is \( R \)-multilinear.

**Lemma 6.1.8 [splitting multilinear maps]** Let \((M_i, i \in I)\) be a family of \( R \)-modules, \( f : M_I \to W \) an \( R \)-multilinear map, \( I = J \sqcup K \) and \( b \in M_K \).

(a) There exists a unique \( R \)-linear map \( \tilde{f}_b : \bigotimes^J \to W \) with \( \tilde{f}_b(\otimes^J m_j) = f_b((m_j)) \).

(c) The function \( f_K : M_K \to \text{Hom}_R(\bigotimes^J M_J, W), b \to \tilde{f}_b \) is \( R \)-multilinear.

(d) There exists a unique \( R \)-linear map \( \tilde{f}_K : \bigotimes^K M_K \to \text{Hom}_R(\bigotimes^J M_J, W) \) with \( \tilde{f}_K(\otimes^K m_k)(\otimes^J m_j) = f((m_i)) \).
6.1. MULTILINEAR FUNCTIONS AND TENSOR PRODUCTS

(e) There exists a unique $R$-bilinear map, $f_{K,J} : \bigotimes K M_k \times \bigotimes J M_j \to W$ with $f_{K,J}(\bigotimes K m_k, \bigotimes J m_j) = f((m_i))$

Proof: (a) Follows from 6.1.2 and the definition of a tensor product.

(b) Let $k \in K$, $a, \tilde{a} \in M_k$, $r \in R$, $b \in M_K - a$ and $d \in M_J$. The $(a, b) \in M_K$ and $(a, b, d) \in M_J$. We compute

$$(rf_{(a,b)})(\bigotimes J d_j) = rf(a, b, d) = f(ra, b, d) = f_{(ra,b)}(\bigotimes J d_j).$$

By the uniqueness assertion in (b), $rf_{(a,b)} = f_{(ra,b)}$. Thus $f_K(ra, b) = rf_K(a, b)$

Similarly

$$(f_{(a,b)} + f_{(\tilde{a},b)})(\bigotimes J d_j) = f(a, b, d) + f(\tilde{a}, b, d) = f(a + \tilde{a}, b, d) = f_{(a+\tilde{a},b)}(\bigotimes J d_j)$$

and $f_{(a,b)} + f_{(\tilde{a},b)} = f_{(a+\tilde{a},b)}$. Hence $f_K(a\tilde{a}, b) = f_K(a + \tilde{a}, b)$ and $f_K$ is $R$-multilinear.

(c) Follows from (b) and the definition of a tensor product.

(d) Define $f_{K,J}(a, b) = \tilde{f}_K(a)(b)$. Since $\tilde{f}_K$ and $\tilde{f}_{K,J}$ are $R$-linear and $f_{K,J}$ is bilinear. Thus (d) follows from (c).

Lemma 6.1.9 [associativity of tensor products] Let $R$ be a ring and $A, B$ and $C$ $R$-modules. Then there exists an $R$-isomorphism

$$A \otimes B \otimes C \to A \otimes (B \otimes C)$$

which sends $a \otimes b \otimes c \to a \otimes (b \otimes c)$ for all $a \in A, b \in B, c \in C$.

Proof: Define $f : A \times B \times C \to A \otimes (B \otimes C), (a, b, c) \to a \otimes (b \otimes c)$. By 6.1.7, $f$ is multilinear. So there exists an $R$-linear map $\tilde{f} : A \otimes B \otimes C \to A \otimes (B \otimes C)$ with $g(a \otimes b \otimes c) = a \otimes (b \otimes c)$.

By 6.1.8 there exists an $R$-linear map $g = \otimes_{\{1, \{2,3\}} : A \otimes (B \otimes C) \to A \otimes B \otimes C$ with $g(a \otimes (b \otimes c)) = a \otimes c$.

Note that $(gf)(a \otimes b \otimes c) = g(a \otimes (b \otimes c)) = a \otimes b \otimes c$. Since $A \otimes B \otimes C$ is generated by the $a \otimes b \otimes c$, we get $gf = id$. Similarly $fg = id$ and so $\tilde{f}$ is an $R$-isomorphism.

Lemma 6.1.10 [tensor product of direct sums] Let $I$ be a finite set and for $i \in I$ let $(M_{ij}, j \in J_i)$ be a family of $R$-modules. Then there exists an $R$-isomorphism,

$$\bigotimes_{i \in I} (\bigoplus_{j \in J_i} M_{ij}) \to \bigoplus_{a \in J_i} (\bigotimes_{i \in I} M_{ia}).$$

with

$$\otimes_{i \in I} (m_{ij})_{j \in J_i} \to (\otimes_{i \in I} m_{ia})_{a \in J_i}.$$
Define $\rho_a$ be the canonical embedding. So for $\alpha \in J_I$, there exists a unique $R$-linear map $f_\alpha : M_I \to \bigotimes_{i \in I} M_{i\alpha(i)}$, $(m_i) \mapsto \otimes_{i \in I} m_{i\alpha(i)}$.

Since $\otimes$ is multilinear and $\pi_{ij}$ is linear, 6.1.7 implies that $f_\alpha$ is multilinear. Hence there exists a unique $R$-linear map

$$\tilde{f}_\alpha : \bigotimes_{i \in I} M_i \to \bigotimes_{i \in I} M_{i\alpha(i)}$$

with $\tilde{f}_\alpha(\otimes m_i) = \otimes m_{i\alpha(i)}$. We claim that for a given $m = (m_i)$ there exists only finitely many $\alpha \in J_I$ with $f_\alpha(m) \neq 0$. Indeed there exists a finite subset $K_i \subseteq J_i$ with $m_{ij} = 0$ for all $j \in J_i \setminus K_i$. Thus $\alpha(m) = 0$ for all $\alpha \in J_I \setminus K_I$. Since $I$ and $K_i$ are finite, $K_I$ is finite. Thus

$$\tilde{f} = (\tilde{f}_\alpha)_{\alpha \in J_I} : \bigotimes_{i \in I} (\bigoplus_{j \in J_i} M_{ij}) \to \bigoplus_{\alpha \in J_I} \bigotimes_{i \in I} M_{i\alpha(i)}.$$

is $R$-linear with

$$(*) \quad \tilde{f}(\otimes_{i \in I} (m_{ij})_{j \in J_i}) = (\otimes_{i \in I} m_{i\alpha(i)})_{\alpha \in J_I}$$

To show that $\tilde{f}$ is an isomorphism, we define its inverse. For $j \in J_i$ let $\rho_{ij} : M_{ij} \to M_i$ be the canonical embedding. So for $a \in M_{ij}$, $\rho_{ij}(a) = (a_k)_{k \in I_j}$, where $a_k = 0$ of $k \neq j$ and $a_j = a$. Let $\alpha \in J_I$ and define

$$\rho_\alpha : \prod_{i \in I} M_{i\alpha(i)} \to \bigotimes_{i \in I} M_i, \quad (m_{i\alpha(i)}) \mapsto \otimes_{i \in I} \rho_{i\alpha(i)}(m_{i\alpha(i)}).$$

Then $\rho_\alpha$ is $R$-multilinear and we obtain an $R$ linear map

$$\tilde{\rho}_\alpha : \bigotimes_{i \in I} M_{i\alpha(i)} \to \bigotimes_{i \in I} M_i$$

with

$$\tilde{\rho}_\alpha(\otimes_{i \in I} m_{i\alpha(i)}) = \otimes_{i \in I} \rho_{i\alpha(i)}(m_{i\alpha(i)}).$$

Define

$$\rho : \bigoplus_{\alpha \in J_I} \bigotimes_{i \in I} M_{i\alpha(i)} \to \bigotimes_{i \in I} M_i, \quad (d_\alpha) \mapsto \sum_{\alpha \in J_I} \rho_\alpha(d_\alpha).$$

Then $\rho$ is $R$ linear. We claim that $\rho \circ \tilde{f} = \text{id}$ and $\tilde{f} \circ \rho = \text{id}$.

Let $m = (m_i) = ((m_{ij})) \in M_i$. Then $m_i = \sum_{j \in J_i} \rho_{ij}(m_{ij})$ and by multilinearity of $\otimes$.

$$\otimes_{i \in I} m_i = \sum_{\alpha \in J_I} \otimes_{i \in I} \rho_{i\alpha(i)}(m_{i\alpha(i)})$$
By (*) and the definition of \( \hat{\rho} \).

\[
\hat{\rho}(\hat{f}(\otimes_{i \in I} m_i)) = \sum_{a \in I_J} \hat{\rho}_a(\otimes_{i \in I} m_{i\alpha_i}) = \sum_{a \in I_J} \otimes_{i \in I} \rho_{i\alpha_i}(m_{i\alpha_i}) = \otimes_{i \in I} m_i.
\]

Hence \( \hat{\rho} \hat{f} = \text{id.} \)

Let \( d = (d_\alpha) \in \bigoplus_{\alpha \in I_J} (\otimes_{i \in I} M_{i\alpha_i}). \) To show that \( (\hat{f} \hat{\rho})(d) = d \) we may assume that \( d_\alpha = 0 \) for all \( \alpha \neq \beta \) and that \( d_\beta = \otimes_{i \in I} m_{i\beta_i} \) with \( m_{i\beta_i} \in M_{i\beta_i}. \) Put \( m_{ij} = 0 \) for all \( j \neq \beta_i. \)

Then \( m_i := (m_{i,j}) = \rho_{i\beta_i}(m_{i\beta_i}) \)

Then

\[
\hat{\rho}(d) = \sum_{\alpha \in I_J} \hat{\rho}_\alpha(d_\alpha) = \hat{\rho}_\beta(\otimes_{i \in I} m_{i\beta_i}) = \otimes_{i \in I} \rho_{i\beta_i}(m_{i\beta_i}) = \otimes_{i \in I} m_i
\]

Let \( \alpha \in J_I \) with \( \alpha \neq 0. \) Then \( \alpha_i \neq \beta_i \) for some \( i \in I \) and so \( m_{i\alpha_i} = 0. \) Hence

\[
\hat{f}_\alpha(\hat{\rho}(d)) = 0 = d_\alpha \text{ if } \alpha \neq \beta \text{ and } \hat{f}_\alpha(\hat{\rho}(d)) = \otimes_{i \in I} m_{i\beta_i} = d_\beta \text{ if } \beta = \alpha.
\]

Thus \( \hat{f}(\hat{\rho}(d)) = (\hat{f}_\alpha(\hat{\rho}(d))) = (d_\alpha) = d. \) Hence \( \hat{f} \hat{\rho} = \text{id.} \) and \( \hat{f} \) is an isomorphism with inverse \( \rho. \)

\[
\text{Corollary 6.1.11 [basis for tensor products]} \quad \text{Let } (M_i, i \in I) \text{ be a finite family of } R\text{-modules. Suppose that } M_i \text{ is a free } R\text{-module with basis } A_i, i \in I. \text{ Then } \bigotimes_{i \in I} M_i \text{ is a free } R\text{-module with basis}
\]

\[
(\otimes_{i \in I} a_i \mid a \in A_I)
\]

\[
\text{Proof:} \quad \text{For } j \in A_I \text{ let } M_{ij} = R_j. \text{ Then } M_i = \bigoplus_{j \in A_i} M_{ij}. \text{ For } a \in A_i, \text{ put } T_a = \bigotimes_{i \in I} M_{i\alpha_i}. \text{ Since each } M_{ij} \cong R, \text{ 6.1.6 implies } T_a \cong R. \text{ More precisely, } \bigotimes_{i \in I} a_i \text{ is a basis for } T_a. \text{ By ?? \( \bigotimes_{i \in I} M_i \cong \bigoplus_{a \in A_I} T_a. \text{ Hence } (\otimes_{i \in I} a_i \mid a \in A_I) \text{ is indeed a basis for } \bigotimes_{i \in I} M_i.}
\]

We will denote the basis from the previous theorem by \( \bigotimes_{i \in I} A_i. \) If \( I = \{1, \ldots, n\} \) and \( A_i = \{a_{i1}, a_{i2}, \ldots, a_{im_i}\} \) is finite we see that \( \bigotimes_{i \in I} M_i \) has the basis

\[
a_{1j_1} \otimes a_{2j_2} \otimes \ldots \otimes a_{nj_n}, \quad 1 \leq j_1 \leq m_1, \ldots, 1 \leq j_n \leq m_n.
\]

\[
\text{Lemma 6.1.12 [tensor product of linear maps]} \quad \text{(a) Let } (\alpha_i : A_i \to B_i, i \in I) \text{ a family of } R\text{-linear maps. Then there exists a unique } R\text{-linear map}
\]

\[
\otimes \alpha_i : \bigotimes A_i \to \bigotimes B_i
\]

\[
(\otimes \alpha_i)(\otimes a_i) = \otimes \alpha_i(a_i)
\]

\[
\text{(b) Let } (\alpha_i : A_i \to B_i, i \in I) \text{ and } (\beta_i : B_i \to C_i, i \in I) \text{ families of } R\text{-linear maps. Then}
\]

\[
\otimes (\beta_i \circ \alpha_i) = (\otimes \beta_i) \circ (\otimes \alpha_i).
\]

\[
\text{Proof:} \quad \text{(a) Define } f : A_I \to \bigotimes B_i, \quad (a_i) \to (\otimes \alpha_i(a_i)). \text{ By 6.1.7 } f \text{ is } R\text{-multilinear. So (b) follows from the definition of the tensor product.}
\]

\[
\text{(b) Both these maps send } \otimes a_i \text{ to } \otimes (\beta_i(\alpha_i(a_i))). \quad \square
\]
6.2 Symmetric and Exterior Powers

Let $I$ be a finite set, $R$ a ring and $M$ an $R$-module. Let $M_i = M$ for all $i \in I$. Then $M_I = M^I$. Let $\pi \in \text{Sym}(I)$ and $m = (m_i) \in M^I$. Define $m\pi \in M$ by $(m\pi)_i = m_{\pi(i)}$. (So if we view $m$ as a function from $I \to M$, $mpi = m \circ \pi$) For example if $\pi = (1,2,3)$, then $(m_1,m_2,m_3)\pi = (m_2,m_3,m_1)$. Note that for $\pi,\mu \in \text{Sym}(I)$, $m(\pi\mu) = (m\pi)\mu$.

**Definition 6.2.1** Let $I$ be a finite set, $R$ a ring and $M$ an $R$-modules. Let $f : M^I \to W$ be $R$-multilinear.

(a) $f$ is symmetric if $f(m\pi) = f(m)$ for all $m \in M, \pi \in \text{Sym}(I)$.

(b) $f$ is skew symmetric if $f(m\pi) = (\text{sgn } \pi)f(m)$ for all $m \in M, \pi \in \text{Sym}(I)$.

(c) $f$ is alternating if $f(m) = 0$ for all $m \in M^I$ with $m_i = m_j$ for some $i \neq j \in I$.

**Lemma 6.2.2** [alternating implies skew symmetric]

(a) Let $f : M^I \to W$ be alternating. Then $f$ is skew symmetric.

(b) Suppose that $f : M^I \to W$ is skew symmetric and that $w \neq -w$ for all $0 \neq w \in W$. Then $f$ is alternating.

(c) Let $f : M^n \to W$ be multilinear with $f(m) = 0$ for all $m \in M^n$ with $m_i = m_{i+1}$ for some $1 \leq i < n$. Then $f$ is alternating.

**Proof:** (a) Let $\pi \in \text{Sym}(I)$ and $m \in M$ we need to show that $f(\pi m) = \text{sgn } f(\pi m)$. Since $\pi$ is the product of two cycles we may assume that $\pi$ itself is a 2-cycle. So $\pi = (i,j)$ for some $i \neq j \in I$. Let $a = m_i, b = m_j, d = m_{I\setminus \{i,j\}}$ and $g = f_d$. Then $m = (a,b,d)$, $f(m) = g(a,b)$ and $f(\pi)(m) = f(b,a,d) = g(b,a)$.

Since $f$ and so also $g$ is alternating we compute

$$0 = g(a+b,a+b) = g(a,a) + g(a,b) + g(b,a) + g(b,b) = g(a,b) + g(b,a)$$

Thus $f(\pi m) = g(b,a) = -g(a,b) = (\text{sgn } \pi)f(m)$

(b) Suppose that $m_i = m_j$ for some $i \neq j$ and let $\pi = (i,j)$. Then $m = \pi m$ and so $f(m) = f(\pi m) = (\text{sgn } \pi)f(m) = -f(m)$ Thus by assumption on $W$, $f(m) = 0$ and $f$ is alternating.

(c) By induction on $n$. Let $m \in M$ with $m_i = m_j$ for some $1 \leq i < j \leq n$. Let $m = (a,b)$ with $a \in M^{n-1}$, $b \in M$. Let $g = f_b$, that is $g(d) = f(d,b)$ for $d \in M^{n-1}$. By induction $g$ is alternating. So if $j \neq n$, $f(m) = g(a) = 0$. So suppose $j = n$. Let $\pi = (i,n-1)$. By induction and (b), $f(m\pi) = g(a\pi) = -g(a) = -f(m)$. But $(m\pi)_{n-1} = m_i = m_j = m_n = (m\pi)_n$ and so by assumption $f(m\pi) = 0$. Hence also $f(m) = 0$. \(\square\)

**Definition 6.2.3** Let $R$ be a ring, $M$ an $R$-module, $I$ a finite set and $f : M^I \to W$ an $R$-multilinear function.
(a) \( f \) is called an \( I \)th symmetric power of \( M \) over \( R \) provided that \( f \) is symmetric and for every symmetric function \( g : M^I \to W \), there exists a unique \( R \)-linear map \( \tilde{g} : W \to \tilde{W} \) with \( g = \tilde{g} \circ f \).

(b) \( f \) is called an \( I \)th exterior power of \( M \) over \( R \) provided that \( f \) is alternating and for every alternating function \( g : M^I \to W \), there exists a unique \( R \)-linear map \( \tilde{g} : W \to \tilde{W} \) with \( g = \tilde{g} \circ f \).

**Lemma 6.2.4** [existence of symmetric and alternating powers] Let \( R \) be a ring, \( M \) an \( R \)-module and \( I \) a finite set. Then an \( I \)-th symmetric and an \( I \)-th exterior power of \( M \) over \( R \) exist. Moreover they are unique up to \( R \)-isomorphism.

**Proof:** Let \( A \) be the \( R \)-submodule of \( \bigotimes^I M \) generated by the elements \( \otimes m - \otimes m\pi \), \( m \in M_I, \pi \in \text{Sym}(I) \). Let \( W = (\bigotimes^I M)/A \) and define \( f : M_I \to W \) by \( f(m) = \otimes m + A \).

We claim that \( f \) is an \( I \)-th symmetric power for \( M \) over \( R \). So let \( g : M_I \to \tilde{W} \) be symmetric. Then \( g \) is multilinear and so by the definition of a tensor product there exists a unique \( R \)-linear map \( \tilde{g} : \bigotimes^I M \to \tilde{W} \) with \( \tilde{g}(\otimes m) = g(m) \). Since \( g(m) = g(m\pi) \) for all \( m \in M, \pi \in \text{Sym}(I) \) we have \( \tilde{g}(\otimes m\pi) = g(m\pi) \). Thus \( \otimes m - \otimes m\pi \in \ker \tilde{g} \). Hence also \( A \subseteq \ker \tilde{g} \). So there exists a uniquely determined and well defined \( R \)-linear map \( \tilde{g} : W \to \tilde{W}, d + A \to \tilde{g}(d) \) for all \( d + A \in W \). So \( f \) is an \( I \)-symmetric power of \( M \) over \( R \).

Next let \( B \) be the \( R \)-submodule of \( \bigotimes^I M \) generated by the elements \( \otimes m \) where \( m \in M \) with \( m_i = m_j \) for some \( i \neq j \in I \). Let \( \hat{W} = \bigotimes^I M/B \) and define \( f : M_I \to \hat{W} \) by \( f(m) = \otimes m + B \). As above it is now a routine exercise to verify that \( f \) is an \( R \)-exterior power of \( M \) over \( R \).

Finally the uniqueness of the symmetric and alternating powers are verified in the usual way.

We will denote the \( I \)-th symmetric power of \( M \) over \( R \) by \( M^I \to S^I M, (m_i) \to \prod_{i \in I} m_i \).

The exterior power is denoted by \( M^I \to \Lambda^I M, (m_i) \to \wedge_{i \in I} m_i \).

**Lemma 6.2.5** [symmetric and alternating powers of \( R \)]

(a) \( S^n R \cong R \) for all \( n \geq 1 \)

(b) \( \Lambda^1 R \cong R \) and \( \Lambda^n R = 0 \) for all \( n \geq 2 \).

**Proof:** (a) By 6.1.6 \( R^m \to R, (r_i) \to \prod r_i \) is the \( n \)-th tensor power of \( R \). Since the map is symmetric and is also the \( n \)-th symmetric power.

(b) An alternating map in one variable is just a linear map. So \( \Lambda^R = R \). Now suppose \( n \geq 2, a, b \in R, c \in R^{n-2} \) and \( f : R^n \to W \) is alternating. Then \( f(a, b, c) = abf(1, 1, c) = 0 \). Hence \( \Lambda^n R = 0. \)
Lemma 6.2.6 [tensor products of symmetric and alternating powers] Let \((M_i, i \in I)\) be an \(R\) modules, \(I\) a finite set and suppose that \(I\) is the disjoint unions of the subsets \(I_k \in K\) and \(M_k\) is an \(R\)-module with \(M_i = M_k\) for all \(i \in I_k\). Let \(g : M_I \to W\) be multilinear. Then

(a) Suppose that for all \(k \in K\) and \(b \in I \setminus I_k\), \(g_b : M_{I_k} \to W\) is alternating. Then there exists a unique \(R\)-linear map \(\bar{g} : \bigotimes_{k \in K} (\bigwedge_{i \in I_k} M_i) \to W\) with \(\bar{g}(\otimes_{j \in J} (\bigwedge_{i \in I_k} m_i)) = g((m_i))\) for all \((m_i) \in M^I\).

(b) Suppose that for all \(k \in K\) and \(b \in I \setminus I_k\), \(g_b : M_{I_k} \to W\) is symmetric. Then there exists a unique \(R\)-linear map \(\bar{g} : \bigotimes_{k \in K} (S_{I_k} M) \to W\) with \(\bar{g}(\otimes_{j \in J} (\bigwedge_{i \in I_k} m_i)) = g((m_i))\) for all \((m_i) \in M^I\).

**Proof:** This is easily proved using the methods in ?? and 6.1.9 \(\square\)

Lemma 6.2.7 [symmetric and exterior powers of direct sums] Let \(R\) be a ring, \(I\) a finite set and \((M_j, j \in J)\) a family of \(R\)-modules. Let \(\Delta = \{d \in \mathbb{N}^J \mid \sum_{j \in J} d_j = |I|\}\). For \(j \in J\) let \(\{I^d_j \mid j \in J\}\) be a partition of \(I\) with \(|I^d_j| = d_j\) for all \(j \in J\). For \(d \in \Delta\) put \(A(d) = \{\alpha \in J^n \mid |\alpha^{-1}(j)| = d_j\}\). For \(\alpha \in A(d)\) and \(j \in J\) put \(I^\alpha_j = \alpha^{-1}(j) = \{i \in I \mid \alpha_i = j\}\). Let \(\pi_\alpha \in \text{Sym}(I)\) with \(\pi_\alpha(I^d_j) = I^\alpha_j\). Then

(a) The function 
\[
f : \bigoplus_{j \in J} M_j^I \to \bigoplus_{d \in \Delta} \bigotimes_{j \in J} S^{I^d_j} M_j
\]
\[
((m_{ij})_{j \in J})_{i \in I} \rightarrow \left( \sum_{\alpha \in A(d) \ j \in J \ i \in I^\alpha_j} \bigotimes_{j \in J} m_{\pi_\alpha(i)j} \right)_{d \in \Delta}
\]
is an \(I\)-th symmetric power of \(\bigoplus_{j \in J} M_j\) over \(R\).
(b) The function
\[ f : (\bigoplus_{j \in J} M_j)^I \rightarrow \bigoplus_{d \in \Delta} (\bigotimes_{j \in J} \bigwedge M_j)^{\bar{I}_d} \]

\[(\{m_{ij}\}_{j \in J})_{i \in I} \mapsto (\sum_{\alpha \in A(d)} \text{sgn} \alpha \bigotimes (\bigwedge m_{\alpha(i)j}) )_{d \in \Delta} \]

is an I-th exterior power of \( \bigoplus_{j \in J} M_j \) over \( R \).

**Proof:** (b) View each \( \alpha = (\alpha_i)_{i \in I} \in J^n \) as the function \( I \rightarrow J, i \mapsto \alpha_i \). Since \( \{I_j^d | j \in J \) of \( I \) is a partition of \( I \), each \( I_j^d \) is a subset of \( I \) and each \( i \in I \) is contained \( I_j^d \) for a unique \( j \in J \). Define \( \alpha_d \in J^I \) by \( (\alpha_d)_i = j \) where \( i \in I_j^d \).

Let \( \alpha \in J^I \). Note that \( \{I_j^d | j \in J \} \) is a partition of \( I \). Define \( d = d_{\alpha} \in \Delta \) by \( (d_{\alpha})_j = |I_j^d| \). So \( d \) is unique in \( \Delta \) with \( \alpha \in A(d) \). Note that \( I_{\alpha_d}^d = I_j^d \). We will now verify that there exists a \( \pi_{\alpha} \in \text{Sym}(I) \) with \( \pi_{\alpha}(I_j^d) = I_j^d \). Since \( |I_j^d| = |I_j^d| \), there exists a bijection \( \pi_{\alpha} : I_j^d \rightarrow I_j^d \).

Define \( \pi_{\alpha} \in \text{Sym}(I) \) by \( \pi_{\alpha}(i) = \pi_{\alpha}(i) \), where \( i \in I_j^d \). Since \( \pi_{\alpha}(i) \in I_{\alpha_d}, \alpha(\pi_{\alpha}(i)) = j \). But \( j = \alpha_d(i) \) and so \( \alpha \circ \pi_{\alpha} = \alpha_d \).

Conversely if \( \pi \in \text{Sym}(I) \) with \( \alpha \circ \pi = \alpha_d \) then \( \pi^d : I_j^d \rightarrow I_j^d, i \mapsto \pi(i) \) is a well defined bijection.

Define

\[ f_d^j : M^n \rightarrow \bigwedge_{i \in I_j^d} M_{m_{ij}} \]

and

\[ f_d : M^n \rightarrow \bigotimes_{j \in J} (\bigwedge_{i \in I_j^d} M_{m_{ij}}) \]

We will now show \( \text{sgn} \pi_{\alpha} f_d \circ \pi_{\alpha} \text{alpha} \) does not depend on the particular choice of \( \pi_{\alpha} \). For this let \( \pi \in \text{Sym}(n) \) with \( \alpha_d = \alpha \circ \pi \). Put \( \sigma = \pi - 1 \pi_{\alpha} \) and \( \sigma^j = (\pi^j) - 1 \pi_{\alpha} \). So then \( \sigma^j \in \text{Sym}(I_j^d) \) and and

\[ (f_d^j \circ \pi_{\alpha}(m) = f_d^j (m_{\pi_{\alpha}}) = \bigwedge_{i \in I_j^d} (m_{\pi_{\alpha}})_{ij} = \bigwedge_{i \in I_j^d} (m_{\pi_{\alpha}} (\pi(i))_j = \]

\[ = \text{sgn} \sigma^j \text{sgn} (\bigwedge_{i \in I_j^d} m_{\pi_{\alpha}} (\pi(i))_j) = (\text{sgn} \sigma^j)(f_d^j \circ \pi)(m) \]

Thus \( f_d^j \circ \pi_{\alpha} = (\text{sgn} \sigma^j) f_d^j \circ \pi \). Taking the tensor product over all \( j \in J \) and using \( \text{sgn} \sigma = \prod_{j \in J} \text{sgn} \sigma^j \) we get \( f_d \circ \pi_{\alpha} = \text{sgn} \sigma f_d \circ \pi \). But \( \text{sgn} \sigma = \text{sgn} \pi_{\alpha} \text{sgn} \sigma \text{alpha} \) and so

\[ \text{sgn} \pi_{\alpha} f_d \circ \pi_{\alpha} \text{sgn} \sigma f_d \circ \pi \]
So we can define \( f_\alpha = \text{sgn}_\pi f_d \circ \pi \), where \( \pi \in \text{Sym}(n) \) with \( \alpha_d = \alpha \pi \).

Let \( \mu \in \text{Sym}(n) \) and \( j \in J \). Then \((\alpha \mu)(i) = j\) if and only if \( \alpha(\mu(i)) = j \). Thus \( \mu(I^j) = I^j_\alpha \). Hence \( d_{\alpha \mu} = d_\alpha = d \). Put \( \rho = \pi_{\alpha \mu} \) Then

\[ \alpha_d = (\alpha \mu) \circ \rho = \alpha \circ (\mu \circ \rho) \]

So by definition of \( f_\alpha \)

\[ f_\alpha(m) = (\text{sgn}(\mu \circ \rho))(f_d \circ (\mu \circ \rho)) = (\text{sgn} \mu)(\text{sgn} \rho)(f_d \circ \rho)(m \mu) = \text{sgn} \mu f_{\alpha \mu}(m \mu). \]

So we proved:

\[ (*) \]

For \( d \in \Delta \) define \( \tilde{f}_d = \sum_{\alpha \in A(d)} f_\alpha \). We will show that \( \tilde{f}_d \) is alternating. By 6.1.7, \( f_d = \text{multilinear} \).

Hence also \( \tilde{f}_d \) is multilinear.

Now suppose that \( m_k = m_l \) for some \( k \neq l \in I \). Put \( \mu = (k, l) \in \text{Sym}(I) \).

Let \( \alpha \in A(d) \). Suppose that \( \alpha = \alpha \mu \), that is \( \alpha_k = \alpha_l \). Let \( j = \alpha(i) \). Then \( k, l \in I^j \).

Since \( m_k = m_j, m_l = m_{ij} \) Thus \( \wedge_{i \in I^j} m_{ij} = 0 \), \( f^j_d(m) = 0 \) and so also \( f_\alpha(m) = 0 \).

Suppose next that \( \alpha \neq \alpha \mu \). Since \( m_k = m_l, m = m \mu \). So by \( (*) \)

\[ f_{\alpha \mu}(m) = f_{\alpha \mu}(m \mu) = \text{sgn} \mu f_{\alpha}(m) = -f_{\alpha}(m) \]

Hence \( f_{\alpha \mu}(m) + f_{\alpha}(m) = 0 \). It follows that \( \tilde{f}_d(m) = \sum_{\alpha \in A(d)} f_{\alpha}(m) = 0 \) and \( \tilde{f}_d \) is alternating.

Now define

\[ f = (\tilde{f}_d) : M^n \rightarrow \bigoplus_{d \in \Delta} (\bigotimes_{j \in J} M_j) M \rightarrow (\tilde{f}_d(m))_{d \in \Delta}. \]

To complete the proof of (b) it remains to verify that \( f \) is an \( I \)-th exterior power of \( M \).

Since each \( f_d \) is alternating, \( f \) is alternating. Let \( g : M^n \rightarrow W \) be alternating.

By \( ?? \) there exists a unique \( R \)-linear map

\[ \tilde{g}_d : \bigotimes_{j \in J} M_j \rightarrow W \]

with

\[ \tilde{g}_d \otimes j \in J \wedge_{i \in I^j} m_i = g(m) \]

where \( m \in M^I \) with \( m_i \in M_i \) for all \( i \in I^j \).

Define

\[ \tilde{g} : \bigoplus_{d \in \Delta} (\bigotimes_{j \in J} M_j) \rightarrow W, \quad (u_d)_{d \in \Delta} \rightarrow \sum_{d \in \Delta} \tilde{g}_d(u_d) \]
Let \( m \in M^I \). Since \( g \) is multilinear,

\[
g(m) = \sum_{\alpha \in J^I} w_\alpha
\]

where \( w_\alpha = g(m_{i\alpha(i)}) \).

Let \( \pi = \pi_\alpha \). Since \( g \) is alternating and \( \alpha_d = \alpha \pi \),

\[
w_\alpha = \text{sgn} \pi g(m_{\pi i, \alpha_d(i)})
\]

Note that \( \otimes j \in J \land_{i \in I_d^1} m_i \land_{i \in I_d^1} \pi_{\pi i \alpha_d(i)} = f_d(m \pi) \) and so by definition of \( \check{g}_d \) and the previous equation

\[
w_\alpha = \text{sgn} \pi \check{g}_d(f_d(m \pi)) = \check{g}_d(f_\alpha(m))
\]

Thus

\[
g(m) = \sum_{\alpha \in J^I} w_\alpha = \sum_{d \in \Delta} \sum_{\alpha \in A(d)} \check{g}_d(f_\alpha(m)) = \sum_{d \in \Delta} \check{g}_d(\sum_{\alpha \in A(d)} f_\alpha(m))
\]

Thus \( g = \check{g} \circ f \). So \( f \) is indeed an exterior power and (b) is proved.

(a) To prove (a) we change the proof for (b) as follows: Replace \( \land \) by \( S \). Replace \( \land \) by \( \cdot \). Replace every \( \text{sgn} \lambda \) by 1. Finally the following argument needs to be added:

Let \( \mu \in \text{Sym}(I) \). Then using (***) and \( A(d) = \{\alpha \mu \mid \alpha \in A(d)\} \) we get

\[
\bar{f}_d(m) = \sum_{\alpha \in A_d} f_\alpha(m) = \sum_{\alpha \in A(d)} f_{\alpha \mu}(m \mu) = \sum_{\alpha \in A_d} f_\alpha(m \mu) = \bar{f}_d(m \mu).
\]

Thus \( \bar{f}_d \) is symmetric. \( \square \)

A remark on the preceding theorem. The proof contains an explicit isomorphism. But this isomorphism depends on on the choice of the partitions \( I^k_d \). And the computation of the isomorphism depends on on the choice of the \( \pi_\alpha \). Here is a systematic way to make these choices. Assume \( I = \{1, \ldots, n\} \) and choose some total ordering on \( J \). Let \( d \in \Delta \) and let \( J_d = \{j \in J \mid d_j \neq 0\} \). Note that \( |J_d| \leq |I| \) and so \( J_d \) is finite. Hence \( J_d = \{j_1, \ldots, j_u\} \) with \( j_1 < j_2 < \ldots < j_u \). To simplify notation we write \( k \) for \( j_k \). Choose \( I^1_d = \{1, 2, \ldots, d_1, d_1 + 1, d_1 + 2, \ldots, d_1 + d_2\} \) and so on. Now let \( \alpha \in A(d) \). So \( I^1_d = \{s+1, s+2, \ldots s+d_j\} \), where \( s = \sum_{k<j} d_k \). Define \( \pi_\alpha \) as follows. Send 1 to the smallest \( i \) with \( \alpha(i) = 1 \), 2 to the second smallest element with \( \alpha(i) = 1 \), \( d_1 \) to the largest element with \( \alpha(i) = 2 \), \( d_1 + 1 \) to the smallest element with \( \alpha(i) = 2 \) and so on.

Finally we identify \( \bigwedge^{I^1_d} M_j \) with \( \bigwedge^{d_j} M_j \) by identifying \( \land_{i \in I_d^1} v_i \in \bigwedge^{I^1_d} M_j \) with \( \land_{t=1}^{d_j} v_{s+t} \in \bigwedge^{d_j} M_j \), where \( s = \sum_{k<j} d_k \).
Let \( m = (m_i) \in M^I \) such that for all \( i \in I \) there exists a unique \( j \in J \) with \( m_{ij} \neq 0 \). So \( m_i = m_{ij} \) for a unique \( j \in J \). Denote this \( j \) by \( \alpha(i) \). Then \( \alpha \in J^I \). Note that \( \tilde{f}_d(m) = 0 \) for all \( d \neq d_\alpha \). So suppose that \( \alpha \in A(d) \). Let \( I_i^d = \{i_1^d, i_2^d, \ldots, i_{d_j}^d\} \) with \( i_1^d < i_2^d < \ldots < i_{d_j}^d \). Then since \( \wedge \) is skew symmetric there exists \( \epsilon \in \{1, -1\} \) with

\[
\wedge m = m_{1, \alpha(1)} \wedge m_{2, \alpha(2)} \wedge \ldots \wedge m_{n, \alpha(n)} = \\
= \epsilon m_{i_1^d, 1} \wedge m_{i_2^d, 1} \wedge \ldots \wedge m_{i_{d_1}^d, 1} \wedge m_{i_2^d, 2} \wedge \ldots \wedge m_{i_{d_2}^d, 2} \wedge \ldots \wedge m_{i_{d_1}^d, u} \wedge \ldots \wedge m_{i_{d_u}^d, u}
\]

Then \( \epsilon = \text{sgn} \, \pi_\alpha \) and \( \tilde{f}_d(m) \) is

\[
\epsilon(m_{i_1^d, 1} \wedge m_{i_2^d, 1} \wedge \ldots \wedge m_{i_{d_1}^d, 1}) \otimes (m_{i_2^d, 2} \wedge \ldots \wedge m_{i_{d_2}^d, 2}) \otimes \ldots \otimes (m_{i_{d_1}^d, u} \wedge \ldots \wedge m_{i_{d_u}^d, u})
\]

For example suppose that \( |I| = 3 \) and \( |J| = 2 \). We want to compute \( f(m_{11} + m_{12}, m_{21} + m_{22}, m_{31} + m_{32}) \). Since \( f \) is multilinear we need to compute \( f(m_{1\alpha(1)}, m_{2\alpha(2)}, m_{3\alpha(3)}) \) where \( \alpha(i) \in J = \{1, 2\} \).

If \( \alpha = (1, 1, 1) \) then \( d_\alpha = (3, 0) \) and

\[
\tilde{f}_{(3,0)}(m_{11}, m_{21}, m_{31}) = m_{11} \wedge m_{21} \wedge m_{31}
\]

If \( \alpha = (1, 1, 2) \) then \( d_\alpha = (2, 1) \) and

\[
\tilde{f}_{(2,1)}(m_{11}, m_{21}, m_{32}) = (m_{11} \wedge m_{21}) \otimes m_{32}
\]

If \( \alpha = (1, 2, 1) \) then \( d_\alpha = (2, 1) \) and

\[
\tilde{f}_{(2,1)}(m_{11}, m_{22}, m_{31}) = -(m_{11} \wedge m_{31}) \otimes m_{22}
\]

If \( \alpha = (1, 2, 2) \) then \( d_\alpha = (1, 2) \) and

\[
\tilde{f}_{(1,2)}(m_{11}, m_{22}, m_{32}) = m_{11} \otimes (m_{22} \wedge m_{32})
\]

If \( \alpha = (2, 1, 1) \) then \( d_\alpha = (2, 1) \) and

\[
\tilde{f}_{(2,1)}(m_{11}, m_{21}, m_{32}) = (m_{21} \wedge m_{31}) \otimes m_{12}
\]

If \( \alpha = (2, 1, 2) \) then \( d_\alpha = (1, 2) \) and

\[
\tilde{f}_{(1,2)}(m_{12}, m_{21}, m_{32}) = -m_{21} \wedge (m_{12} \otimes m_{32})
\]

If \( \alpha = (2, 2, 1) \) then \( d_\alpha = (1, 2) \) and

\[
\tilde{f}_{(1,2)}(m_{12}, m_{22}, m_{31}) = m_{31} \otimes (m_{12} \wedge m_{22})
\]

If \( \alpha = (2, 2, 2) \) then \( d_\alpha = (0, 3) \) and

\[
\tilde{f}_{(0,3)}(m_{12}, m_{22}, m_{32}) = m_{12} \wedge m_{22} \wedge m_{32}.
\]
Thus the four coordinates of \( f(m) \) are:

\[
\begin{align*}
  d = (3, 0) : & \quad m_{11} \wedge m_{21} \wedge m_{31} \\
  d = (2, 1) : & \quad (m_{11} \wedge m_{21}) \otimes m_{32} - (m_{11} \wedge m_{31}) \otimes m_{22} + (m_{21} \wedge m_{31}) \otimes m_{12} \\
  d = (1, 2) : & \quad m_{11} \otimes (m_{22} \wedge m_{32}) - m_{21} \wedge (m_{12} \otimes m_{32}) + m_{31} \otimes (m_{12} \wedge m_{22}) \\
  d = (0, 3) : & \quad m_{12} \wedge m_{22} \wedge m_{32}
\end{align*}
\]

Lemma 6.2.8 \[Bases for symmetric and exterior powers\] Let \( R \) be a ring, \( n \) a positive integer and \( M \) a free \( R \)-modules with basis \( \mathcal{B} \). Let \( " \leq " \) be a total ordering on \( \mathcal{B} \).

(a) \((b_1 b_2 \ldots b_n \mid b_1 \leq b_2 \leq \ldots b_n \in \mathcal{B})\) is a basis for \( S^n M \).

(b) \((b_1 \wedge b_2 \wedge \ldots \wedge b_n \mid b_1 < b_2 < \ldots b_n \in \mathcal{B})\) is a basis for \( S^n M \).

**Proof:** For \( b \in \mathcal{B} \) put \( M_b = Rb \). Then \( M_b \cong R \) and \( M = \bigoplus_{b \in \mathcal{B}} M_b \). We will apply \( \boxtimes \) with \( I = \{1, \ldots, n\} \) and \( J = \mathcal{B} \). Let \( \Delta \) be as in the statement of that theorem. Let \( d \in \Delta \).

(a) By \( \boxtimes \), \( \bigotimes_{b \in \mathcal{B}} \left( S^d M_b \right) \cong R \) with basis \( b^d \). By 6.1.6

\[\bigotimes_{b \in \mathcal{B}} (S^d M_b) \cong R\]

and has \( \bigotimes_{b \in \mathcal{B}} b^{d_b} \) has a basis. (a) now follows from \( \boxtimes (a) \)

(b) By \( \boxtimes \), \( \bigwedge^d M_b = 0 \) for all \( d \geq 2 \). So

\[\bigotimes_{b \in \mathcal{B}} \left( \bigwedge^d M_b \right) \cong R = 0\]

if \( d_b \geq 2 \) for some \( b \in \mathcal{B} \) and

\[\bigotimes_{b \in \mathcal{B}} \left( \bigwedge^d M_b \right) \cong R\]

if \( d_b \leq 1 \) for all \( b \in \mathcal{B} \). Moreover, it has basis \( \bigotimes_{b \in \mathcal{B}, d_b=1} b \). (b) now follows from \( \boxtimes (b) \).

**Example:** Suppose \( M \) has basis \( \{a, b, c, d\} \). Then \( S^3 M \) has basis
\[
d^3, cd^2, c^2 d, c^3, bd^2, bcd, be^2, b^2 d, b^3 c, b^3, ad^2, acd, ac^2, abd, abc, ab^2, a^2 d, a^2 c, a^2 b, a^3
\]
and \( \bigwedge^3 M \) has basis
\[
b \wedge c \wedge d, a \wedge c \wedge d, a \wedge b \wedge d, a \wedge b \wedge c
\]
Corollary 6.2.9 [dimension of symmetric and alternating powers] Let $R$ be a ring and $n, m$ positive integer. Then

(a) $S^m R^n \cong R^{\binom{n+m+1}{m}}$

(b) $\bigwedge^m R^n \cong R^{\binom{n}{m}}$.

Proof: This follows from ?? \hfill \Box

Lemma 6.2.10 [uniqueness of dimensions] Let $R$ be a ring and $M$ an free $R$-module with finite basis $\mathcal{A}$ and $\mathcal{B}$. Then $|\mathcal{A}| = |\mathcal{B}|$.

Proof: Let $n = |\mathcal{A}|$. Then $M \cong R^n$. So by 6.2.9(b), $n$ is the smallest non-negative integer with $\bigwedge^{n+1} M = 0$. So $n$ is uniquely determined by $M$ and $n = |\mathcal{B}|$. \hfill \Box

Definition 6.2.11 Let $R$ be a ring and $M$ and free $R$-module with a finite basis $\mathcal{B}$. Then $|\mathcal{B}|$ is called the rank of $M$.

6.3 Determinants and the Cayley-Hamilton Theorem

Lemma 6.3.1 [exterior powers of linear maps] Let $I$ be finite set and $R$ a ring.

(a) Let $\alpha : A \rightarrow B$ be $R$-linear. Then there exists a unique $R$-linear map

$$\bigwedge I \alpha : \bigwedge^I A \rightarrow \bigwedge^I B$$

with

$$\bigwedge^I \alpha(\bigwedge a_i) = \bigwedge \alpha(a_i).$$

(b) Let $\alpha : A \rightarrow B$ and $\beta : B \rightarrow C$ be $R$-linear. Then

$$\bigwedge^I (\beta \circ \alpha) = \bigwedge^I \beta \circ \bigwedge^I \alpha.$$ 

Proof: (a) Define $g : A^I \rightarrow \bigwedge^I B; (a_i) \rightarrow \bigwedge \alpha(a_i)$. If $a_i = a_j$ for some $i \neq j$ then also $\alpha(a_i) = \alpha(b_i)$ and so $g(a) = 0$. Thus $g$ is alternating and (a) follows from the definition of an exterior power.

(b) Both these maps send $\bigwedge a_i$ to $\bigwedge \beta(\alpha(a_i))$.

Theorem 6.3.2 [determinants] Let $R$ be a ring and $n$ a positive integer.

(a) Let $R$ be a ring, $0 \neq M$ a free $R$-module of finite rank $n$, and $\alpha \in \text{End}_R(V)$. Then there exists a unique $r \in R$ with $\bigwedge^n \alpha = \text{rid}_n \bigwedge^n M$. We denote this $r$ by $\det \alpha$. 


6.3. DETERMINANTS AND THE CAYLEY-HAMILTON THEOREM

(b) \( \det : \text{End}_R(V) \to R, \alpha \to \det \alpha \)

is a multiplicative homomorphism.

(c) There exists a unique function \( \det : \mathcal{M}_R(n) \to R \) (called determinant) with the following two properties:

(Det Alt) When viewed as a function in the \( n \) columns, \( \det \) is alternating.

(Det I) Let \( I_n \) be the \( n \times n \) identity matrix. Then \( \det I_n = 1 \).

(d) Let \( A = (a_{ij}) \in \mathcal{M}_R(n) \). Then

\[
\text{det} A = \sum_{\pi \in \text{Sym}(n)} \text{sgn} \pi \prod_{i=1}^{n} a_{i\pi i}
\]

(e) Let \( A = (a_{ij}) \in \mathcal{M}_R(n) \) and \( a_j = (a_{ij}) \) the \( j \)-th column of \( A \). Then \( \wedge a_j = \text{det} A \wedge e_j \), where \( e_j = (\delta_{ij}) \in R^n \).

(f) Let \( R \) be a ring, \( 0 \neq M \) a free \( R \)-module of finite rank \( n \), \( \alpha \in \text{End}_R(V) \), and \( B \) a basis for \( M \). Let \( A = \mathcal{M}^B(\alpha) \) be the matrix for \( \alpha \) with respect to \( B \). Then

\[
\text{det} \alpha = \text{det} A
\]

(g) Let \( A \in \mathcal{M}_R(n) \). Then

\[
\text{det} A = \text{det} A^T
\]

where \( a_{ij}^T = a_{ji} \).

**Proof:**

(a) By ??, \( \Lambda^I M \cong R \). Thus by 4.3.9, \( \text{End}_R(\Lambda^I M) = R_\text{id} \). So (a) holds.

(b) follows from 6.3.1.

(c) Let \( e_i = (\delta_{ij}) \in R^n \). Then by ??, \( e := \wedge_{i=1}^n e_i \) is a basis for \( \Lambda^n R^n \). Define \( \tau : \Lambda^n R^n \to R, re \to r \). Let \( A = (a_{ij}) \in \mathcal{M}_R(n) \) a view \( A \) as \( (a_i)_{1 \leq i \leq n} \) with \( a_i \in R^n \). Define \( \text{det} A = \tau(\wedge_{i \in J} a_i) \). Since \( I_n = (e_i) \), \( \text{det} I_n = 1 \). So \( \text{det} \) fulfills (Det Alt) and Det I. Suppose now \( f : (R^n)^n \to R \) is alternating with \( f((e_i)) = 1 \). Then by definition of an \( I \)-th exterior power there exists an \( R \)-linear map \( \bar{f} : \Lambda^n R^n \to R \) with \( f = \bar{f} \circ \wedge \). Then \( \bar{f}(e) = \bar{e}(\wedge e_i) = f((e_i)) = 1 \) and so \( \bar{f} = \tau \) and \( f = \text{det} \). Thus (c) holds.

(d) We will apply ?? with \( I = J = \{1, \ldots, n\} \) and \( M_j = R e_j \). So \( \bigoplus_{j \in J} = R^n \). Let \( \delta \in \Delta \). If \( d_j \geq 2 \) for some \( j \in J \) then \( \Lambda^{I_j} M_j = 0 \). If \( d_j \leq 1 \) for all \( j \), then \( \sum_{j \in J} d_j = n = |I| \) forces \( d_j = 1 \) for all \( j \in J \). Let \( d \in \Delta \) with \( d_j = 1 \) for all \( j \in J \). Also \( R e_j \to R, re_j \to R \) is an 1-st exterior power. Let \( \alpha \in J^I \). Then \( \alpha \in A(d) \) if and only if \( |\alpha^{-1}(j)| = 1 \) for all \( j \in J \). This is the case if and only of \( \alpha \in \text{Sym}(n) \). Also \( \pi_{\alpha} = \alpha \). Hence ?? implies that

\[
f : (R^n)^n \to R \quad (m_{ij}) \to \sum_{\alpha \in \text{Sym}(n)} \prod_{i=1}^{n} m_{i\alpha i}
\]
is an \( n \)-th exterior power of \( R^n \). Note that \( f((e_i)) = 1 \). So this this choice of \( \bigwedge^n R^n \) we have \( e = 1 \), \( \tau = \text{id}_R \) and \( \det = f \). so (d) holds.

(e) was proved in (c).

(f) For \( A \in \mathcal{M}_R(R) \) let \( \alpha = \alpha_A \) be the corresponding elements of \( \text{End}_R(M) \). So \( \alpha(b) = \sum_{d \in B} a_{db} d \). Let \( a_b = (a_{db}) \), the \( b \)-th column of \( A \). Suppose that \( a_b = a_c \) with \( b \neq c \). Then \( \alpha(b) = \alpha(c) \) and so \( \langle \alpha \rangle \langle \alpha \rangle = \langle \alpha \rangle \langle \alpha \rangle = 0 \). Hence \( \det \alpha = 0 \). Also \( \det I_n = \det \text{id} = 1 \) and so \( A \rightarrow \det(\alpha_A) \) fulfilled (\textbf{Det Alt}) and (\textbf{Det 1}). Thus the uniqueness of \( \det A \) implies \( \det A = \det \alpha \).

(g) Using (d) we compute

\[
\det A^T = \sum_{\pi \in \text{Sym}(n)} \text{sgn} \pi \prod_{i \in I} a_{\pi(i)i} = \sum_{\pi \in \text{Sym}(n)} \text{sgn} \prod_{i \in I} a_{\pi^{-1}(i)} = \sum_{\pi \in \text{Sym}(n)} \text{sgn} \prod_{i \in I} a_{\pi(i)} = \det A
\]

\[\square\]

**Definition 6.3.3** Let \( R \) be a ring and \( s : A \rightarrow B \rightarrow C \) \( R \)-bilinear.

(a) An \( s \)-basis for is a triple \( ((a_d \mid d \in D), (b_d \mid d \in D), c) \) such that \( D \) is a set, \( (a_d \mid d \in D) \) is a basis for \( A \), \( (b_d, d \in D) \) is a basis for \( B \) and \( \{c\} \) is a basis for \( C \) with \( s(a_d, b_e) = \delta_{de} c \) for all \( d, e \in D \).

(b) We say that \( s \) is a pairing if there exists an \( s \)-basis. \( s \) is a finite pairing if \( s \) is pairing and \( \text{rank} A = \text{rank} B \) is finite.

Note that if \( s : A \rightarrow B \rightarrow C \) is a pairing, then \( A, B \) and \( C \) are free \( R \)-modules and \( C \cong R \) as an \( R \)-module. Also \( s \) is non-degenerate, that is \( s(a, b) = 0 \) for all \( b \in B \) implies \( a = 0 \), and \( s(a, b) = 0 \) for all \( a \in A \) implies \( b = 0 \).

The converse is only true in some special circumstances. For example if \( R \) is a field, \( s : A \rightarrow B \rightarrow C \) is bilinear, \( \dim_R C = 1 \) and \( \dim_R A \) is finite, then it is not to difficult to see that \( s \) is a pairing.

But if \( \dim_R A \) is not finite this is no longer true in general. For example let \( B = A^* = \text{Hom}_R(A, R) \) and \( s(a, b) = b(a) \). Then \( \dim_R B > \dim_R A \) and so \( s \) is not a pairing.

For another example define \( s : \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}, (a, b) \rightarrow \mathbb{Z}, (a, b) \rightarrow 2ab \). The \( s \) is not a pairing. Indeed suppose \( \{1\}, \{2\}, \{c\} \) is an \( s \)-basis. Then \( c = s(a, b) = 2ab \), a contradiction to \( \mathbb{Z} = \mathbb{Z}c \).

**Lemma 6.3.4** [duality and alternating powers] Let \( R \) be a ring, \( I, J, K \) finite sets with \( K = I \uplus J \) and let \( s : A \times B \rightarrow R \) be \( R \)-bilinear. Let \( \Delta = \{E \subseteq K \mid |E| = |J|\} \) and for \( E \in \Delta \) choose \( \pi_E \in \text{Sym}(K) \) with \( \pi_E(J) = E \).
(a) There exists a unique $R$-bilinear map

$$s^J_K : \bigwedge^K A \times \bigwedge^J B \to \bigwedge^I A$$

with

$$s^J_K(\wedge a_k, \wedge b_j) = \sum_{E \in \Delta} \det(s(a_{\pi_E(j)}, b_{j'})_{j,j' \in J}) \bigwedge_{i \in I} a_{\pi_E(i)}$$

(b) $s^J_K$ is independent from the choice of the $\pi_E$.

(c) Let $\alpha \in \text{End}_R(A)$ and $\beta \in \text{End}_R(B)$ with $s(\alpha(a), b) = s(a, \beta(b))$ for all $a \in A, b \in B$. Then

$$(\wedge^J \alpha)(s^J_K( u, (\wedge^J \beta)(v)) = s^J_K((\wedge^K \alpha)(u), v)$$

for all $u \in \bigwedge^K A$ and $v \in \bigwedge^J B$.

(d) Suppose there exists a basis $E = (e_d, d \in D)$ for $A$ and a basis $F = (f_d, d \in D)$ for $B$ such that $s(e_d, f_{d'}) = \delta_{dd'}$. Let $\alpha \in D^K$ and $\beta \in D^J$ be one to one. Then

$$s^J_K(\bigwedge_{k \in K} e_{\alpha(k)}, \bigwedge_{j \in J} f_{\beta(j)}) = \begin{cases} \pm \bigwedge_{k \in K \setminus \alpha^{-1}(\beta(J))} e_{\alpha(k)} & \text{if } \beta(J) \subseteq \alpha(K) \\ 0 & \text{if } \beta(J) \not\subseteq \alpha(K) \end{cases}$$

Proof: (a) and (b) We first show that

$$f_E(a, b) := \text{sgn } \pi_E \det(s(a_{\pi_E(j)}, b_{j'})_{j,j' \in J}) \bigwedge_{i \in I} a_{\pi_E(i)}$$

is independent from the choice of $\pi_E$. Indeed let $\pi \in \text{Sym}(K)$ with $\pi(J) = E$. Let $\sigma = \pi^{-1}\pi_E$. Let $\sigma_J \in \text{Sym}(J)$ be defined by $\sigma_J(j) = \sigma(j)$. Similarly define $\sigma_I$. Then

$$\det(s(a_{\pi_E(j)}, b_{j'})) = \det(s(a_{(\pi\sigma_J)(j)}, b_{j'})) = \text{sgn } \sigma_J \det(s(a_{\pi_i}, b_{j'}))$$

and

$$\bigwedge_{i \in I} a_{\pi_E(i)} = \bigwedge_{i \in I} a_{\pi_{\sigma_I}(i)} = \text{sgn } \sigma_I \bigwedge_{i \in I} a_{\pi(i)}.$$

Using that $\text{sgn } \pi = \text{sgn } \sigma \text{sgn } \pi_E = \text{sgn } \sigma_I \text{sgn } \sigma_J \text{sgn } \pi_E$ and multiplying the last two equations together we obtain the claimed independence from the choice of $\pi_E$.

Define

$$f : A^K \times B^J \to \bigwedge^J A, \quad (a, b) \mapsto \sum_{E \in \Delta} f_E(a, b)$$

In view of 6.2.6 it remains to show that $f_b$ and $f_a$ are alternating for all $a \in A^K$ and $b \in B^J$. That $f_a$ is alternating is obvious. So suppose $b \in B^J$ and $a \in A^K$ with $a_k = a_l$ for distinct
$k, l \in K$. Let $E \in \Delta$ and put $\pi = \pi_E$. If $k$ and $l$ are both in $\pi(J)$ then $\det(s(a_{\pi(j)}, b_{\pi(j)})) = 0$. If $k, l$ are both in $I$ then $\bigwedge_{i \in I} a_{\pi(i)} = 0$. So in both these cases $f_E(a, b) = 0$. Suppose now that $k \in \pi(I)$ and $l \in \pi(J)$. Let $\sigma = (k, l) \in \text{Sym}(K)$ and $E' = \sigma(E) \neq E$. We may choose $\pi_{E'} = \sigma \pi$. $a_k = a_l$ now implies $f_{E'}(a, b) = \text{sgn} \sigma f_E(a, b)$ and so $f_{E'}(a, b) + f_E(a, b) = 0$. If follows that $f_b(a) = f(a, b) = 0$ and $f_b$ is alternating.

(c) Let $a \in A^K, b \in B^J$. Note that $\beta \circ b = (\beta(b_j))$. Let $E \in \Delta$. Then

$$
\left( \bigwedge_{i \in I} \alpha \right)(f_E(a, \beta \circ b)) = \left( \bigwedge_{i \in I} \alpha \right)(\text{sgn} \pi_E \det(s(a_{\pi_E(j)}, b_{\pi_{E'}(j)}))) = \\
= \text{sgn} \pi_E \det(s(\alpha(a_{\pi_E(j)}), b_{\pi_{E'}(j)})) = \left. f_E(\alpha \circ a, b) \right|_{\alpha} = (\alpha \circ a, b)
$$

Thus (c) holds.

(d) Suppose $E \in \Delta$ and $f_E(a, b) \neq 0$ where $a = (e_{\alpha(i)})$ and $b = (f_{\beta(j)})$. Let $A = s(e_{\alpha}(\pi_E(j)), f_{\beta_{J'}}(j'))$. Then $\det A \neq 0$. Let $t \in E$. Then $t = \pi_E(j)$ for some $j \in J$ and so $s(e_{\alpha}(t), t, \alpha_{f_{\beta_{J'}}}(j'))$ is a row of $A$. This row cannot be zero and $s(e_{\alpha}(t), t, \alpha_{f_{\beta_{J'}}}(j')) \neq 0$ for some $t' \in J$. But then $\alpha(t) = \beta(t')$. It follows that $\beta(I) \subseteq \alpha(I)$ and $E = \alpha^{-1}\beta(I)$. Also $\det A = \pm 1$ and so (ca) holds.

**Proposition 6.3.5 [The exterior algebra]** Let $R$ be a ring and $M$ an $R$-module.

(a) Let $I, J$ and $K$ finite sets with $K = I \uplus J$ Then there exists a unique bilinear map

$$
\wedge : \bigwedge^I M \times \bigwedge^J M \to \bigwedge^K M, (a, b) \to a \wedge b
$$

with

$$
(\bigwedge_{i \in I} m_i) \wedge (\bigwedge_{j \in J} m_j) = \bigwedge_{k \in K} m_i
$$

for all $(m_i) \in M^{i}.$

(b) Define

$$
\bigwedge M = \bigoplus_{i=0}^{\infty} \bigwedge^i M
$$

and

$$
\wedge : \bigwedge^I M \times \bigwedge^J M \to \bigwedge^K M, \ (a_j)_{j=0}^{\infty} \wedge (b_j)_{j=0}^{\infty} = (\sum_{i=0}^{k} a_i \wedge b_{k-i})_{k=0}^{\infty}.
$$

Then $(\bigwedge^I M, +, \wedge)$ is a (non)-commutative ring with $R = \bigwedge^0 M \leq Z(\bigwedge M)$. 
Lemma 6.3.6  

**Proof:**  
(a) Define \( f : M^I \times M^J \to \bigwedge^K M, ((a_i), (a_j)) \to \bigwedge_{k=1}^{K} a_k \). Clearly \( f(a_i) \) and \( f(a_j) \) is alternating and so (a) follows from 6.2.6.  

(b) First of all \( (\bigwedge M, +) \) is an abelian group. By (a) \( \wedge \) is bilinear. So the distributive laws hold. Let \( l, m, n \) be non-negative integers and \( m_k \in M \) for \( 1 \leq k \leq l + m + n \). Then

\[
(l \wedge \bigwedge_{i=1}^{l} m_i) \wedge \bigwedge_{i=l+1}^{l+m} m_i = \bigwedge_{i=1}^{l} m_i = \bigwedge_{i=l+1}^{l+m} m_i = (l \wedge \bigwedge_{i=1}^{l} m_i) \wedge \bigwedge_{i=l+1}^{l+m+n} m_i
\]

and so \( \wedge \) is associative.

So \( (\bigwedge M, +, \wedge) \) is indeed a (non)-commutative ring. That \( R \subseteq Z(\bigwedge M) \) follows from the fact that \( \wedge \) is \( R \)-linear. \( \square \)

**Lemma 6.3.6**  

**Finite pairings** Let \( R \) be a ring and \( s : A \times B \to C \) a finite pairing.

(a) The functions

\[
s_A : A \to \text{Hom}_R(B, C), a \to s_a
\]

and

\[
s_B : B \to \text{Hom}_R(A, C), b \to s_b
\]

are \( R \)-linear isomorphisms.

(b) Let \( f \in \text{End}_R(B) \). Then there exists a unique \( f^s \in \text{End}_R(A) \) with \( s(f^s(a), b) = s(a, f(b)) \) for all \( a \in A, b \in B \).

(c) Suppose \( (a_d, d \in D), (b_d, d \in D) \) and (c) are \( s \)-basis for \( (A, B, C) \). Let \( M_D(f^s) = M_D(f)^T \)

**Proof:**  
Let \( ((a_d \mid d \in D), (b_d \mid d \in D), c) \) be an \( s \)-basis. (a) For \( e \in D \) define \( \phi_e \in \text{Hom}_R(B, C) \) by \( \phi_e(\sum_{e \neq d} b_d) = r_{ec} \). Then \( (\phi_d, d \in D) \) is a basis for \( \text{Hom}_R(B, C) \). Since \( s(a_e, b_d) = \delta_{edc} \), \( s_A(c) = \phi_e \). Hence (a) holds.

(b) Define \( \tilde{f} \in \text{End}_R(\text{Hom}_R(B, C)) \) by \( \tilde{f}(\phi) = \phi \circ f \). Let \( g \in \text{End}_R(A), a \in A \) and \( b \in B \). Then

\[
s(a, f(b)) = s_A(a)(f(b)) = ((\tilde{f})(s_A))(a)(b)
\]

and

\[
s(g(a), b) = s_A(g(a))(b)
\]

Hence \( s(a, f(b)) = s(g(a), b) \) for all \( a \in A, b \in B \) if and only if \( \tilde{f} \circ s_A = s_A \circ g \). By (a), \( s_A \) has an inverse so \( f^s = s_A^{-1} \tilde{f} s_A \) is the unique element fulfilling (c).

(c) Let \( g \in \text{End}_R(B) \). Put \( U = M_f(D) \) and \( V = M_g(D) \). So \( g(a_d) = \sum_{h \in D} v_{hd} a_h \) and \( f(b_d) = \sum_{h \in D} u_{hd} b_h \). Thus
Let \( \bigwedge \) denote the exterior algebra. For a \( \bigwedge \) of finite rank, let \( s(a_e,f(b_d)) = \sum_{h \in D} u_{hd}s(a_e,b_h) = u_{ed}c \)

and
\[
s(g(a_e),b_d) = \sum_{h \in D} v_{he}s(a_h,b_d) = v_{de}c
\]

Hence \( s(a,f(b)) = s(g(a),f) \) for all \( a \in A, b \in B \) if and only if \( v_{de} = u_{ed} \) for all \( d, e \in D \).
So (c) holds (and we have a second proof for (b)). \( \square \)

Recall that for an \( R \)-module \( M, M^* \) denote the dual module, so \( M^* = \text{Hom}_R(M,R) \).

**Lemma 6.3.7 [dual of the exterior algebra]** Let \( R \) be a ring, \( M \) a free module of finite rank over \( R \) and \( I \) a finite set

(a) There exists a unique \( R \)-bilinear function \( s_I : \bigwedge^I M^* \times \bigwedge^I M \to R \) with \( s_I(\bigwedge \phi_i, \bigwedge m_i) = \det(\phi_i(m_j))_{i,j \in I} \).

(b) \( s_I \) is a finite pairing.

(c) \( \bigwedge^I M^* \cong (\bigwedge^I M)^* \) as \( R \)-modules.

**Proof:** Define \( s : M^* \times M \to R, (\phi,m) \to \phi(m) \). (a) follows from 6.3.4(a) applied with \( A = M^*, B = M, K = I, J = I \) and "\( I = \emptyset \)". And (b) follows from part (d) of the same lemma. Finally (c) is a consequence of (b) and ??(a). \( \square \)

**Proposition 6.3.8 [adjoint of a linear map]** Let \( R \) be a ring and \( M \) a \( R \)-module of finite rank. Let \( f \in \text{End}_R(M) \). Then there exists \( f^{\text{ad}} \in \text{End}_R(M) \) with \( f \circ f^{\text{ad}} = f^{\text{ad}} \circ f = \det f \text{id}_M \).

**Proof:** Consider \( t : M \times \bigwedge^n M \to \bigwedge^n M, (m,b) \to m \wedge b \). We claim that \( t \) is a finite pairing. For this let \( (a_i, 1 \leq i \leq n) \) be a basis for \( M \). Put \( b_i = a_1 \wedge a_2 \wedge a_{i-1} \wedge a_{i+1} \wedge a_n \).

Let \( c = a_1 \wedge \ldots \wedge a_n \). By ??, \( (b_i, 1 \leq i \leq n) \) is a basis for \( \bigwedge^n M \) and \( \{c\} \) is a basis for \( \bigwedge^n M \). Also \( a_i \wedge b_j = 0 \) for \( i \neq j \) and \( a_i \wedge b_i = (-1)^i c \). \((a_i), \((-1)^{i-1} b_i), c \) is a \( t \) basis. Let \( f^a d = (\text{bigwedge}^{n-1} f)^t \) be given by ??(b). So \( f^{\text{ad}} \in \text{End}_R(M) \) is uniquely determined by

\[
f^{\text{ad}}(m) \wedge b = m \wedge (\bigwedge f)(b)
\]

for all \( m \in M, b \in \bigwedge^{n-1} M \).

In particular,
\[
(f^{\text{ad}}(f(m) \wedge b) = f(m) \wedge (\bigwedge f)(b) = (\bigwedge f)(m \wedge b) = (\det f)(m \wedge b) = m \wedge (\det f)b
\]
6.3. DETERMINANTS AND THE CAYLEY-HAMILTON THEOREM

Note that also \((\det f)m \wedge b = m \wedge (\det f)b\) and so by \(\Box\)

\[
\text{ad} \circ f = ((\det f)\text{id}_{\Lambda^{n-1}M})^t = (\det f)\text{id}_M
\]

To show that also \(f \circ \text{ad} = \text{id}_M\) we use the dual \(M^*\) of \(M\). Recall that \(f^* \in \text{End}_R(M^*)\) is define by \(f^*(\phi) = \phi \circ f\). It might be interesting to note that \(f^* = f^*\), where \(s\) is the pairing \(s : M^* \rightarrow M, (\phi, m) \rightarrow \phi(m)\).

Applying the above results to \(f\) in place of \(f^*\) we have

\[
f^* \circ \text{ad}^* = (\det f^*)\text{id}_{M^*}
\]

By \(\Box\) we have \(\det f^* = \det f\). So dualizing the previous statement we get

\[
f \circ (f^* \circ \text{ad}^*) = \det f \text{id}_M
\]

So the proposition will be proved once we show that \(f^* \circ \text{ad}^* = \text{ad}^*\) or \(f^* = f^*\).

To do this we will compute that matrix of \(f^* \circ \text{ad}^*\) with respect to the basis \((a_i)\). Let \(D\) be the matrix of \(f\) with respect to \((a_i)^t\) and \(E\) the matrix of \(\Lambda^{n-1} f\) with respect to \((-1)^i b_i\).

Let \(D_{ij}\) be the matrix \((d_{kl})_{k \neq i, l \neq j}\). Then the coefficient of \(b_j\) in \(\Lambda^{n-1} \sum_{k=1}^n d_{hk}a_k\) is readily seen to be \(\det D_{ij}\).

It follows that

\[
E_{ij} = (-1)^{i-1-1} \det D_{ij} = (-1)^{i+j} \det D_{ij}
\]

Let \((\phi_i)\) be the basis of \(M^*\) dual to \((a_i)\). So \(\phi_i(a_j) = \delta_{ij}\). Then the matrix for \(f^*\) with respect to \((\phi_i)\) is \(D^T\). Note that \((D^T)_{ij} = (D_{ji})^T\) and so the \((i, j)\) coefficient of the matrix of \(f^*\) is

\[
(-1)^{i+j} \det(D^T)_{ij} = (-1)^{i+j} \det(D_{ji})^T = (-1)^{i+j} \det D_{ji}
\]

Thus \(f^*\) has the matrix \(E^T\) with respect to \((\phi_i)\). So does \((f^*)^T\). Hence \(f^* = f^*\) and the proposition is proved. \(\Box\)

**Lemma 6.3.9** [extending scalars] Let \(R\) and \(S\) be rings with \(R \leq S\). Let \(M\) be an \(R\) module. Then there exists bilinear function

\[
\cdot : S \times S \otimes_R M \rightarrow S \otimes M, (s, \tilde{m}) \rightarrow s\tilde{m}
\]

with

\[
s(t \otimes m) = st \otimes m
\]

for all \(s, t \in S\) and \(m \in M\). Moreover, \((S \otimes_R M, c \cdot 0\) is an \(S\)-module.
**Proof:** Let \( s \in S \). By 6.1.12 there exists a unique \( \text{id}_S \otimes \text{id}_M \in \text{End}_R(S \otimes_R M) \) which sends \( t \otimes m \) to \( st \otimes m \). We will write \( s \otimes 1 \) for \( \text{id}_S \otimes \text{id}_M \). It is readily verified that \( s \to s \otimes 1 \) is a ring homomorphism. So the lemma is proved. \( \square \)

**Lemma 6.3.10** [extending scalars for free modules] Let \( R \) and \( S \) be rings with \( R \subseteq S \). Let \( M \) be a free \( R \)-module with basis \( B \).

(a) \( S \otimes_R M \) is a free \( S \)-module with basis \( 1 \otimes A := \{ 1 \otimes b \mid b \in B \} \).

(b) Let \( \alpha \in \text{End}_R(M) \), \( A \) the matrix of \( \alpha \) with respect to \( B \) and \( s \in S \). Then \( sA \) is the matrix of \( s \otimes \alpha \) with respect to \( 1 \otimes B \).

**Proof:** (a) Note that \( M = \bigoplus_{b \in B} Rb \) and \( Rb \cong R \). By ?? \( S \otimes_R M \cong \bigoplus_{b \in B} S \otimes_R Rb \). Also by ?? \( S \otimes_R b \cong S \).

(b) Let \( d \in B \) Then

\[
(s \otimes \alpha)(1 \otimes d) = s \otimes \alpha(d) = s \otimes \left( \sum_{e \in B} b_{ed} e \right) = \sum_{e \in B} (sb_{ed})(1 \otimes e)
\]

So (b) holds. \( \square \)

**Definition 6.3.11** Let \( R \) be a ring, \( M \) a free \( R \)-module of finite rank and \( \alpha \in \text{End}_R(M) \).

(a) Let \( S \) be a ring with \( R \) as a subring. Let \( s \in S \). Then \( s \otimes \alpha \) denotes the unique \( R \)-endomorphism of \( S \otimes_R M \) with

\[
(s \otimes 1)(t \otimes m) = (st \otimes \alpha(m)
\]

for all \( t \in S, m \in M \).

(b) Consider \( x \otimes 1 - 1 \otimes \alpha \in \text{End}_{R[x]}(R[x] \otimes_R M) \). Then

\[
\chi_\alpha = \det(x \otimes 1 - 1 \otimes \alpha) \in R[x]
\]

is called the characteristic polynomial of \( \alpha \).

(c) Let \( n \) be positive integer and \( A \in \mathcal{M}_R(n) \). Consider the matrix \( xI_n - A \in \mathcal{M}_{R[x]}(n) \). Then \( \chi_A = \det(xI_n - A) \) is called the characteristic polynomial of \( A \).

**Lemma 6.3.12** [properties of the characteristic polynomial] Let \( R \) be a ring, \( M \) an \( R \)-module with finite basis \( I \), \( n = |I| \), \( \alpha \in \text{End}_R(M) \) and \( A \) the matrix of \( \alpha \) with respect to \( A \).

(a) \( \chi_\alpha = \chi_A \).
(b) For $J \subset I$ let $A_J = (a_{ij})_{i,j \in J}$. The coefficient of $x^m$ in $\chi_A$ is

$$(-1)^{n-m} \sum_{J \subset I, |J| = n-m} \det A_J$$

(c) $\chi_\alpha$ is monic of degree $n$.

**Proof:**

(a) By 6.3.10(b) the matrix for $x \otimes 1 - 1 \otimes \alpha$ with respect to $xI_n - A$. Thus (a) follows from 6.3.2(f).

(b) Let $D = xI_n - A$. Let $a_i$ be the $i$ column of $A_i$. Let $e_i = (\delta_{ij})$. The $D = (xe_i - a_i)$. For $J \subset I$ let $A_J^*$ be the matrix with whose $k$-column is $a_k$ if $k \in J$ and $e_k$ if $k \notin J$. Then since det is multilinear

$$\det D = \sum_{J \subseteq I} x^{||I|-|J||} (-1)^{|J|} \det A^*J$$

Let $T(J)$ be the matrix with

$$t(J)_{ij} = \begin{cases} a_{ij} & \text{if } i,j \in J \\ 1 & \text{if } i = j \notin J \\ 0 & \text{otherwise} \end{cases}$$

Then it is easy to see that $\det A^*(J) = \det T(J) = \det A(J)$ and (b) follows.

(c) Follows from (b). \qed

**Theorem 6.3.13 [Cayley-Hamilton]**

Let $R$ be a ring, $M$ be a free $R$-module of finite rank. Let $\alpha \in \text{End}_R(M)$. Then

$$\chi_\alpha(\alpha) = 0.$$ 

**Proof:** Define

$$\phi : R[x] \times M \to M, \quad (f,m) \to f(\alpha)(m).$$

Since $\phi$ is bilinear there exists a unique $R$-linear map

$$\Phi : R[x] \otimes_R M \to M \text{ with } \Phi(f \otimes m) = f(\alpha)(m).$$

Let $\beta = x \otimes 1 - 1 \otimes \alpha \in \text{End}_{R[x]}(R[x] \otimes_R M)$.

Let $f \in R[x]$ and $m \in M$. Then

$$\beta(f \otimes m) = xf \otimes m - f \otimes \alpha(m) = fx \otimes m - f \otimes \alpha(m)$$

and so

$$\Phi(\beta(f \otimes m)) = (f(\alpha)\alpha)(m) - (f(\alpha)(\alpha(m)) = 0$$

Hence $\Phi \beta = 0$. 

By 6.3.8 there exists $\beta^{ad} \in \text{End}_{R[x]}(R[x] \otimes_R M)$ with $\beta \circ \beta^{ad} = \det \beta \otimes 1$.

It follows that

$$0 = (\Phi \circ \beta) \circ \beta^{ad} = \phi \circ (\beta \circ \beta^{ad}) = \Phi \circ (\det \beta \otimes 1)$$

So

$$0 = \phi((\det \beta \otimes 1))(1 \otimes m) = \phi(\det \beta \otimes m) = (\det \beta)(\alpha)(m)$$

By definition $\chi_{\alpha} = \det \beta$ and so the Cayley Hamilton Theorem is proved. \(\square\)

**Theorem 6.3.14** [Cayley Hamilton for finitely generated modules] Let $M$ be a finitely generated $R$-module and $\alpha \in \text{End}_R(M)$. Then there exists a monic polynomial $f \in R[x]$ with

$$f(A) = 0.$$

**Proof:** Let $I$ be a finite subset of $M$ with $M = RI$. Let $F = F_R(I)$ be the free $R$-module on $I$. So $F$ has a basis $(a_i, i \in I)$. Let $\pi$ be the unique $R$-linear map from $F$ to $M$ with $a_i \to i$ for all $i \in I$. Since $M = RI, M = \pi(F)$. By 4.3.3 there exists $\beta \in \text{End}_R(F)$ with

$$\pi \circ \beta = \alpha \circ \pi$$

We claim that (*) $\pi \circ f(\beta) = f(\alpha) \circ \pi$ for all $f \in R[x]$

For this let $S = \{f \in R[x] \mid \pi \circ f(\beta) = f(\alpha) \circ \pi\}$. Let $f, g \in S$. Then

$$\pi \circ (fg)(\alpha) = \pi \circ (f(\alpha) \circ g(\alpha)) = (\pi \circ f(\alpha) \circ g(\alpha)) = (f(\alpha) \circ \pi) \circ g(\alpha) =$$

$$= f(\alpha) \circ (\pi \circ g(\alpha)) = f(\alpha) \circ (g(\alpha) \circ \pi) = (f(\alpha) \circ g(\alpha)) \circ \pi = (fg)(\alpha) \circ \pi$$

Since $\pi$ is $\mathbb{Z}$-linear, also $f - g \in S$. Thus $S$ is a subring of $R[x]$. Since $R$ and $x$ are in $S, S = R[x]$ and (*) is proved. Let $f = \chi_{\beta}$. The $f$ is monic and by 6.3.13 $f(\beta) = 0$. By (*)

$$f(\alpha) \circ \pi = \pi \circ f(\beta) = 0$$

Since $\pi$ is onto this implies $f(\alpha) = 0$. \(\square\)
Chapter 7

Hilbert’s Nullstellensatz

Throughout this chapter ring means commutative ring with identity.

7.1 Ring Extensions

Definition 7.1.1 Let $R$ and $S$ be rings with $R \subseteq S$ and $1_S = 1_R$. Then $S$ is called a ring extension of $R$. Such a ring extension is denoted by $S : R$.

Definition 7.1.2 Let $S : R$ be a ring extension.

(a) Let $s \in S$. $s$ is called integral over $R$ if $f(s) = 0$ for some monic polynomial $f \in R[x]$.

(b) $S : R$ is called integral if all $s \in S$ are integral over $R$.

(c) $S : R$ is called finite if $S$ is finitely generated as an $R$-module (by left multiplication).

Let $S : R$ be a ring extension and $I \subseteq S$. Then $R[I]$ denotes the subring of $S$ generated by $R$ and $I$, that is $R[I]$ is the intersection of all subrings of $S$ containing $R$ and $I$. Note that $R[I]$ is the image of $R[x_i, i \in I]$ under unique ring homomorphism $R[x_i, i \in I] \to S$ with $r \to r \forall r \in R$ and $x_i \to i, \forall i \in I$. So

$$ R[I] = \{ f(I) \mid f \in R[x_i, i \in I] \}. $$

Examples:

Suppose $S : R$ is a ring extension with $R$ a field and $S$ a integral domain. Let $s \in S$. Then $s$ is integral over $R$ if and only if $s$ is algebraic over $R$. $S : R$ is integral if and only if its algebraic. Note that then by 5.1.6 $S$ is a field. $S : R$ is a finite ring extension if and only if its a finite field extension.

Let $R = \mathbb{Z}$ and $S = \mathbb{C}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$. $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

Theorem 7.1.3 [equivalent conditions for integral] Let $S : R$ be a ring extension and $s \in S$. Then the following are equivalent:

197
(a) \( s \) is integral over \( R \).

(b) \( R[s] : R \) is finite.

(c) There exists a subring \( T \) of \( S \) containing \( R[s] \) so that \( T : R \) is finite.

(d) \( R[s] \) has a faithful module \( M \) which is finitely generated as an \( R \)-module.

**Proof:**
(a) \( \Rightarrow \) (b): Let \( f(s) = 0 \) for a monic \( f \in R[x] \). Let \( J = \{ g \in R[x] \mid g(s) = 0 \} \). Then \( R[s] \cong R[x]/J \) and \( R[x]f \leq J \). By \( ?? \) \( R[x]/(f) \) is finitely generated as an \( R \)-module. Since \( R[x]/J \) is isomorphic to a quotient of \( R[x]/(f) \), also \( R[s] \) is a (b) \( \Rightarrow \) (c): Just choose \( T = R[x] \).

(c) \( \Rightarrow \) (d): Let \( B = T \). As \( 1 \in T \), \( aT \neq 0 \) for all \( 0 \neq a \in R[s] \). So \( T \) is a faithful \( R[s] \)-module.

(d) \( \Rightarrow \) (a): By 6.3.13 there exists a monic \( f \in R[x] \) with \( f(s)M = 0 \). Since \( M \) is faithful for \( R[s] \), \( f(s) = 0 \).

**Corollary 7.1.4** [finite ring extensions are integral] Let \( S : R \) be a finite ring extension. Then \( S : R \) is integral.

**Proof:** This follows immediately from 7.1.3(c) applied with \( T = S \).

**Lemma 7.1.5** [finite over finite ring extension] Let \( S : E \) and \( E : R \) be finite ring extensions. Then \( S : R \) is a finite ring extension.

**Proof:** This follows immediately from 5.1.3(aa).

**Lemma 7.1.6** [finite covers for rings]

(a) Let \( S \) be a ring and \( \{E_j \mid j \in J\} \) be a family of subrings of \( S \). Suppose that for each \( j, k \in J \) there exists an \( l \in J \) with \( E_j \cup E_k \subseteq E_l \). Then \( \bigcup_{j \in J} E_j \) is a subring of \( S \).

(b) \( S : R \) be a ring extension and \( I \subseteq S \). Then
\[
R[I] = \bigcup\{ R[J] \mid J \subseteq I, |J| < \infty \}.
\]

(a) Let \( s, t \in \bigcup_{j \in J} E_j \). Then \( s \in E_j \) and \( t \in E_k \) for some \( j, k \in J \). By assumption there exists \( l \in J \) with \( E_j \cup E_k \subseteq E_l \). As \( E_l \) is a subring of \( S \), \( st \) and \( s - t \) are in \( E_l \) and so in \( \bigcup_{j \in J} E_j \).

(b) Follows from (a) applied to the family of subrings \( \{ R[J] \mid J \subseteq I, |J| < \infty \} \).

**Proposition 7.1.7** [rings generated by integral elements] Let \( S : R \) be a ring extension and \( I \subseteq S \) so that each \( b \in I \) is integral over \( R \).
7.2 GOING UP AND DOWN

(a) If $I$ is finite, $R[I] : R$ is finite and integral.

(b) $R[I] : R$ is integral.

(c) The set $\hat{R}$ of the elements in $S$ which are integral over $R$ form a subring of $S$. $\hat{R} : R$ is integral.

Proof: (a) By induction on $|I|$. If $|I| = 0$ there is nothing to prove. So suppose there exists $i \in I$ and let $J = I - i$. Put $E = R[J]$. By induction $E : R$ is finite. Since $i$ is integral over $R$, $f$ is integral over $E$. Thus by 7.1.3(b), $E[i] : E$ is finite. Note that $E[I] = R[I][i] = R[I]$ and so (a) follows from ??.

(b) By ?? $RI = \bigcup\{R[J] \mid J \subseteq I, |J| < \infty\}$. By (a) each of the $R[J] : R$ are integral. So (b) holds.

(c) Follows from (b) applied to $I = \hat{R}$.

Let $R, S$ and $\hat{R}$ be as in the preceding proposition. $\hat{R}$ is called to integral closure of $R$ in $S$. If $\hat{R} = R$, $R$ is called integrally closed in $S$.

If $R$ is an integral domain and $R$ is integrally closed in $\frac{R}{x^4}$ (the field of fraction of $R$), then $R$ is called integrally closed. The concept of integrally closed is much weaker than algebraically closed. For example $\mathbb{Z}$ is integrally closed (since its easy to see that it is integrally closed in $\mathbb{F}_a = mb\mathbb{Q}$). But $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$, since $\sqrt{2}$ is in the integral closure.

Lemma 7.1.8 [integral over integral] Let $S : E$ and $E : R$ be integral ring extensions. Then $S : R$ is integral.

Let $s \in S$ and let $f \in E[x]$ be the monic with $f(s) = 0$. Let $I$ be the set of non-zero coefficients $f$. Then $I$ is a finite subset of $E$ and so by 7.1.7(a), $R[I] : R$ is finite. Since $f \in R[I][x]$, 7.1.3 implies that $R[I][s] : R[I]$ is finite. So by 7.1.5, $R[I][s] : R$ is finite. So by 7.1.3, $s$ is integral over $R$.

7.2 Going Up and Down

Definition 7.2.1 Let $R$ be ring and $I$ an ideal in $R$. Then $\text{rad} I = \text{rad}_R I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}^+\}$. $\text{rad}_R I$ is called the radical of $I$ in $R$. If $I = \text{rad}_R I$, $I$ is called a radical ideal in $R$.

Lemma 7.2.2 [prime ideals are radical] Let $R$ be a ring and $P$ an ideal in $R$.

(a) $\text{rad} P$ is an ideal in $R$ and $P \leq \text{rad} P$.

(b) All primes ideals in $R$ are radical ideals.
**Proof:** (a) follows from the Binomial Theorem.
(b) Obvious. \(\square\)

**Lemma 7.2.3 [intersecting principal ideals]** Let \( S : R \) be an integral extension.

(a) Let \( P \) be an ideal in \( R \) and \( p \in P \).
    (aa) \( Sp \cap R \subseteq \text{rad} \, P \).
    (ab) If \( P \) is a prime ideal or an radical ideal,
    \( Sp \cap R \subseteq P \).

(b) Suppose \( S \) is an integral domain
    (ba) Let \( 0 \neq b \in S \), then \( Sb \cap R \neq 0 \).
    (bb) Let \( Q \) be a non-zero ideal in \( S \), then \( Q \cap R \neq 0 \).

**Proof:** (aa) Let \( s \in S \) so that \( r := sp \in R \). Since \( S : R \) is integral there exists \( r_0, r_1 \ldots r_{n-1} \in R \) with
\[
s^n = r_{n-1}s^{n-1} + \ldots + r_1 s + r_0
\]
Multiplying this equation with \( p^n \) we obtain:
\[
(sp)^n = (r_{n-1}p)(sp)^{n-1} + \ldots + r_1 p^{n-1}(sp) + r_0 p^n
\]
Hence
\[
r^n = (r_{n-1}p)p^{n-1} + \ldots + (r_1 p^{n-1})r + r_0 p^n
\]
As \( P \) is an ideal and \( r_i r^i \in R \) we have \( r_i r^i p^{n-i} \in P \) for all \( 0 \leq i < n \). So the right side of the last equation lies in \( P \). Thus \( r^n \in P \) and \( r \in \text{rad} \, P \).
    (ab) Follows from (aa) and 7.2.2.
    (ba) Let \( f \in R[x] \) be a monic polynomial of minimal degree with \( f(b) = 0 \) Let \( f = xg + r \) where \( r \in R \) and \( g \in R[x] \) is monic of degree one less than \( f \).
\[
0 = f(b) = bg(b) + r
\]
and so \( r = -g(b)b \)
If \( r = 0 \), we get \( g(b)b = 0 \). Since \( b \neq 0 \) and \( S \) is an integral domain, \( g(b) = 0 \). But this contradicts the minimal choice of \( \deg f \).
Hence \( 0 \neq r = -g(b)b \in R \cap Sb \).
    (bb) Let \( 0 \neq b \in Q \). Then by (ba) \( 0 \neq R \cap Sb \leq R \cap Q \). \(\square\)
Theorem 7.2.4 [going up and down, abstract] Let $S : R$ be an integral extension and $P$ a prime ideal in $R$. Let

$$
\mathcal{M} := \{I \mid I \text{ is an ideal in } R, R \cap I \subseteq P\}
$$

Order $\mathcal{M}$ by inclusion. Let $Q \in \mathcal{M}$.

(a) $Q$ is contained in a maximal member of $\mathcal{M}$

(b) The following are equivalent:

(ba) $Q$ is maximal in $\mathcal{M}$.

(bb) $Q$ is a prime ideal and $R \cap Q = P$.

Proof: Let $\mathcal{M}_Q = \{I \in \mathcal{M} \mid Q \leq I\}$. Then a maximal element of $\mathcal{M}_Q$ is also a maximal element of $\mathcal{M}$.

(a) Since $Q \in \mathcal{M}_Q$, $\mathcal{M}_Q \neq \emptyset$. So by Zorn’s Lemma it remains to show that every non-empty chain $D$ in $\mathcal{M}_Q$ has an upper bound in $\mathcal{M}_Q$. Put $D = \bigcup D$. By 3.3.9(a) $D$ is an ideal in $S$. Let $E \in D$. Then $Q \leq E \leq D$. Moreover,

$$R \cap D = \bigcup_{E \in D} R \cap E \leq P$$

Thus $D \in \mathcal{M}_Q$ and $D$ is an upper bound for $D$.

(b) For $E \subseteq S$ put $\bar{E} = E + Q/Q \subseteq S/Q$. Note that $\bar{R} \cong R/R \cap Q$. Since $R \cap Q \leq P$, it is readily verified that $\bar{P}$ is a prime ideal in $\bar{R}$. Let $I$ be an ideal in $S$ with $Q \leq I$. Then $(R + Q) \cap I = Q + (R \cap I)$ and so $\bar{R} \cap \bar{I} \leq \bar{P}$ if and only if $R \cap I \leq P$. So replacing $S$ by $S/Q$ we may assume that $Q = 0$.

(ba) $\Rightarrow$ (bb). Suppose that $Q$ is not a prime ideal. As $Q = 0$, this means $S$ is not an integral domain. Hence there exists $b_1, b_2 \in S - 0$ with $b_1 b_2 = 0$. Since $Q = 0$ is maximal in $\mathcal{M}$, $Sb_i \notin \mathcal{M}$ and so $R \cap Sb_i \notin P$. Hence there exist $s_i \in S$ with $0 \neq r_i := s_i b_i \in R \setminus P$. But then $r_1 r_2 = (s_1 b_1)(s_2 b_2) = (s_1 s_2)(b_1 b_2) = 0 \in P$. But this contradicts the fact that $P$ is a prime ideal in $R$.

So Thus $Q$ is a prime ideal. Suppose that $P \neq R \cap Q$, that is $P \neq 0$. Let $0 \neq p \in P$. The by ??(a), $Sp \cap R \leq P$. Hence $Sp \in \mathcal{M}$, contradiction the maximality of $Q = 0$. So (ba) implies (bb).

(bb) $\Rightarrow$ (ba) Suppose now that $Q$ is a prime ideal and $P = R \cap Q$. Then $S$ is an integral domain and $P = 0$. Let $I$ be any non-zero ideal in $S$. Then by ??(bb), $R \cap I \neq O$ and so $R \cap I \leq P$ and $I \notin \mathcal{M}$. Thus $\mathcal{M} = \{0\}$ and $Q$ is maximal. \qed

Corollary 7.2.5 [going up and down, concrete] Let $S : R$ be an integral extension.

(a) Let $P$ be a prime ideal in $R$ and $Q$ an ideal in $S$ with $R \cap Q \leq P$. Then there exists a prime ideal $Q$ in $S$ with $R \cap Q = P$ and $Q \leq M$. 


(a) Let \( P \) be a prime ideal in \( R \). Then there exists a prime ideal \( M \) in \( S \) with \( R \cap Q = P \).

(c) Let \( Q_1 \) and \( Q_2 \) be prime ideals in \( S \) with \( R \cap Q_1 = R \cap Q_2 \) and \( Q_1 \leq Q_2 \). Then \( Q_1 = Q_2 \).

(d) Let \( M \) be a maximal ideal in \( S \). Then \( M \cap R \) is a maximal ideal in \( R \).

(e) Let \( P \) be maximal ideal in \( S \). The there exists a maximal ideal \( M \) of \( S \) with \( R \cap M = P \).

Proof:
(a) Let \( \mathcal{M} \) be defined as in 7.2.4. By part (a) there exists a maximal element \( M \) of \( \mathcal{M} \) containing \( Q \). By part (b) \( M \) is a prime ideal and \( R \cap M = P \).

(b) Follows from (a) applied with \( Q = 0 \).

(c) By 7.2.4, applied with \( P = R \cap Q_1 \) and \( Q = Q_1 \) we get that \( Q_1 \) is maximal in \( \mathcal{M} \). As \( Q_2 \in \mathcal{M} \) and \( Q_1 \leq Q_2 \), \( Q_1 = Q_2 \).

(d) Since \( 1 \notin M \), \( R \cap M \neq R \). So by 3.2.8, \( M \cap R \) is contained in a maximal ideal of \( P \) of \( R \). By (b) there exists an ideal \( Q \) in \( S \) with \( P = R \cap Q \) and \( M \leq Q \). Since \( M \) is maximal, \( M = Q \). Thus \( R \cap M = R \cap Q = P \) is maximal in \( R \).

(e) By 3.2.9, \( P \) is a prime ideal in \( R \). So by (b) there exists an ideal \( Q \) of \( S \) with \( R \cap Q = P \). Let \( M \) be a maximal ideal in \( S \) with \( Q \leq M \). Then \( P = R \cap Q \leq R \cap M < R \) and has \( P \) is a maximal ideal in \( R \), \( P = R \cap M \).

\[ \square \]

### 7.3 Noether’s Normalization Lemma

**Definition 7.3.1** Let \( \mathbb{K} \) be a field. A \( \mathbb{K} \)-algebra is a ring extension \( R : \mathbb{K} \). A \( \mathbb{K} \)-algebra \( R : \mathbb{K} \) is called finitely generated if \( R = \mathbb{K}[I] \) for some finite subset \( I \) of \( K \)

**Theorem 7.3.2** [Noether’s Normalization Lemma] Let \( \mathbb{K} \) be a field and \( R : \mathbb{K} \) a ring extension. Suppose that there exists a finite subset \( I \) of \( R \) so that \( R : \mathbb{K}[I] \) is integral. Then there exists a finite subset \( J \) of \( R \) so that \( J \) is transcendental over \( \mathbb{K} \) and \( R : \mathbb{K}[J] \) is integral.

**Proof:** Choose \( J \subseteq R \) with \( |J| \) minimal with respect to \( J \) finite and \( R : \mathbb{K}[J] \) being integral. Suppose that \( J \) is not algebraic independent over \( \mathbb{K} \) and pick \( 0 \neq f \in K[x_j, j \in J] \) with \( f(J) = 0 \). Let \( I = \mathbb{N}^J \) then \( f = \sum_{\alpha \in I} k\alpha x^\alpha \), where \( k\alpha \in K \). Let \( I^* = \{ \alpha \in I \mid k\alpha \neq 0 \} \) and pick \( c \in \mathbb{Z}^+ \) with \( \alpha_j < c \) for all \( \alpha \in I^* \) and \( j \in J \). Let \( \tau : J \to \mathbb{N} \) be one to one with \( \tau(l) = 0 \) for some \( l \in J \). Define

\[ \rho : I^* \to \mathbb{Z}^+, \quad \alpha \to \sum_{j \in J} c^{\tau(j)} \alpha_j \]

We claim that \( \rho \) is one to one. Indeed suppose that \( \rho(\alpha) = \rho(\beta) \) for \( \alpha \neq \beta \in I^* \). Let \( J^* = \{ j \in J \mid \alpha(j) \neq \beta(j) \} \) and \( j \in J^* \) with \( \tau(j) \) is minimal

\[ 0 = \rho(\alpha) - \rho(\beta) = c^{\tau(j)}(\alpha(j) - \beta(j)) + \sum_{k \in J^* - j} c^{\tau(k)-\tau(j)}(\alpha(k) - \beta(k)) \]
7.3. NOETHER’S NORMALIZATION LEMMA

But this implies that \( c \) divides \( \alpha(j) - \beta(j) \) a contradiction to \( c > \alpha(j) \) and \( c > \beta(j) \).

Since \( \rho \) is one to one, \( \rho(\mathbb{I}^*) \) has a unique maximal element \( \rho(\alpha) \).

For \( l \neq j \in J \) define \( v_j = j - \tau \). We will show that \( l \) is integral over \( S := \mathbb{K}[v_j, j \in J - l] \).

Note that \( j = v_j + l \tau \). Let \( \beta \in \mathbb{I}^* \). Then \( J \beta = l \beta \prod_{j \in J - k} (v_j + l \tau)^{\beta_j} \).

Thus \( k_{\beta}J^{\beta} = k_{\beta} l^{\rho(\beta)} + f_{\beta}(l) \) where \( g_{\beta} \in \mathbb{K}[x] \) with \( \deg f_{\beta} < \rho(\beta) \).

By the maximality of \( \rho(\alpha) \) and \( f(J) = 0 \) we conclude

\[
\frac{k_{\alpha}l^{\rho(\alpha)}}{\rho(\alpha)} + g(l) = 0
\]

where \( g \in \mathbb{K}[x] \) with \( \deg g < \rho(\alpha) \). Hence

\[
l^{\rho(\alpha)} + \frac{k_{\alpha}^{-1}g(l)}{\rho(\alpha)} = 0
\]

and \( l \) is integral over \( S \). Note that \( j = v_k + k \tau \) \( \in S[l] \) and \( \mathbb{K}[J] = S[l] \). Since \( R : \mathbb{K}[J] \) is integral we conclude from 7.1.8 that \( R : S \) is integral. But this contradicts the minimal choice of \( |J| \).

\[\square\]

**Proposition 7.3.3 [Integral Extension of Fields]** Let \( S : R \) be an integral extension so that \( S \) and \( R \) are integral domains. Then \( S \) is a field if and only if \( R \) is a field.

**Proof:** Suppose first that \( R \) is a field. Then \( S : R \) is algebraic and so by 5.1.6(c), \( S \) is a field.

Suppose next that \( S \) is a field and let \( 0 \neq r \in R \). Since \( S \) is a field, \( 1 \in Sr \cap R \). Hence by 5.1.6 applied with \( P = Rr \), \( 1 = 1^n \in Rr \) for some \( n \in \mathbb{Z}^+ \). Thus \( r \) is invertible in \( R \), and \( R \) is a field. \[\square\]

**Proposition 7.3.4 [Finitely generated field extensions]**

(a) Let \( F : \mathbb{K} \) be a field extensions so that \( F \) is finitely generated over \( \mathbb{K} \). Then \( F : \mathbb{K} \) is finite. In particular, if \( \mathbb{K} \) is algebraically closed \( F = \mathbb{K} \).

(b) Let \( \mathbb{K} \) be an algebraically closed field, \( A \) a finitely generated \( \mathbb{K} \)-algebra and \( M \) a maximal ideal in \( A \). Then \( A = \mathbb{K} + M \).

**Proof:** (a) By 7.3.2 there exists a finite subset \( J \) of \( \mathbb{K} \) so that \( F : \mathbb{K}[J] \) is integral and \( J \) is algebraically independent over \( \mathbb{K} \). By 5.1.6, \( \mathbb{K}[J] \) is a field. Since the units in \( \mathbb{K}[J] \) are \( \mathbb{K} \) we get \( J = \emptyset \). Hence \( F : \mathbb{K} \) is integral and so algebraic. Thus by 5.1.6 \( F : \mathbb{K} \) is algebraic.

(b) Note that \( A/M \) is a field. So by (a), \( A/M = K + M/M \) and thus \( A = K + M \). \[\square\]
7.4 Affine Varieties

Throughout this section let $\mathbb{F} : \mathbb{K}$ be a field extension with $\mathbb{F}$ algebraically closed. Also $D$ is a finite set, $A = \mathbb{K}[x_d, d \in D]$ and $B = \mathbb{F}[x_d, d \in D]$. For $S \subseteq A$ define $V(S) = V_{\mathbb{F}^D}(S) = \{v \in \mathbb{F}^D \mid f(v) = 0 \forall f \in S\}$. $V(S)$ is called an affine variety in $\mathbb{F}^D$ defined over $\mathbb{K}$. For $U \subseteq \mathbb{F}^D$ let $J(U) = J_A(U) = \{f \in A \mid f(u) = 0 \forall u \in U\}$. $U$ is called closed if $U = V(J(U))$ and $S$ is called closed if $S = J(V(S))$.

Lemma 7.4.1 [Basic Properties of V and J] Let $U \subseteq \tilde{U} \subseteq \mathbb{F}^D$ and $S \subseteq \tilde{S} \subseteq A$.

(a) $J(U)$ is an ideal in $R$.
(b) $J(\tilde{U}) \subseteq J(U)$.
(c) $V(\tilde{S}) \subseteq V(S)$.
(d) $U \subseteq V(J(U))$.
(e) $S \subseteq J(V(S))$.
(f) $U$ is closed if and only if $U = V(S)$ for some $S \subseteq A$.
(g) $S$ is closed if and only if $S = J(U)$ for some $U \subseteq \mathbb{F}^D$.

Proof: (a) Clearly $0 \in J(U)$. Let $f, g \in J(U)$, $h \in A$ and $u \in U$. Then $(f - g)(u) = f(g) - g(u) = 0$ and $(hf)(u) = h(u)f(u) = 0$. So $f - g \in J(U)$ and $hf \in J(U)$.
(b) and (c) are obvious.
(d) Let $u \in U$. Then for all $f \in J(U)$, $f(u) = 0$. So (d) holds.
(e) Similar to (d).
(f) If $S$ is closed, $U = V(S)$ where $S = J(U)$. So suppose $U = J(S)$. Then by (d), $S \subseteq V(U)$ and so by (b) $J(V(U)) \subseteq J(S) = U$. By (e), $U \subseteq J(V(U))$ and hence $U = J(V(U))$. Thus (f) holds.
(g) Similar to (f).

Lemma 7.4.2 [Annihilators of points are maximal] Let $u \in \mathbb{F}^D$.

(a) $J(u)$ is the kernel of the evaluation map: $\Phi : A \to \mathbb{F}, f \to f(u)$.

(b) If $\mathbb{F} : \mathbb{K}$ is algebraic, $J(u)$ is a maximal ideal in $A$.

Proof: (a) is obvious.
(b) Note that $\mathbb{K} \leq \Phi(\mathbb{K}) \leq \mathbb{F}$. So $\Phi(\mathbb{K})$ is an integral domain which is algebraic over $\mathbb{K}$. So by 5.1.6 $\Phi(\mathbb{K})$ is an field. Hence $J(u) = \ker \Phi$ is a maximal ideal.

Lemma 7.4.3 [Maximal Ideals in B] Let $M$ be maximal ideal in $B$. 


Proposition 7.4.4

(a) There exists \( u \in \mathbb{F}^D \) with \( M = J_B(u) \).
(b) \( M \) is the ideal in \( B \) generated by \( (x_d - u_d, d \in D) \).
(c) \( V(M) = \{ u \} \).

**Proof:** (a) and (b) By 7.3.4, \( B = \mathbb{F} + M \). Hence for each \( d \in D \) there exists \( u_d \in \mathbb{F} \) with \( x_d - u_d \in M \). Let \( u = (u_d)_{d \in D} \) and let \( I \) be the ideal generated by \( (x_d, d \in D) \). Then \( x_d \in \mathbb{F} + I \) and so \( \mathbb{F} + I \) is a subring of \( B \) containing \( \mathbb{F} \) and all \( x_d \). Hence \( B = \mathbb{F} + I \) and \( B/I \) is a field. So \( I \) is a maximal ideal. Since \( I \subseteq M \) and \( I \subseteq J_B(u) \) we get \( M = I = J_B(u) \).

(c) Let \( a \in V(M) \). Since \( x_d - u_d \in M \), \( 0 = (x_d - u_d)(a) = a_d - u_d \). Hence \( a_d = u_d \) and \( a = d \).

**Proposition 7.4.4** [varieties are not empty] Let \( I \) be an ideal in \( A \) with \( I \neq \emptyset \). Then \( V(I) \neq \emptyset \).

By 3.2.8 \( I \) is contained in a maximal ideal \( P \) of \( A \). Let \( \mathbb{A} \) be the set of elements in \( \mathbb{F} \) algebraic over \( \mathbb{K} \). Then

\[ V_{\mathbb{A}}(M) \subseteq V(M) \subseteq V(P) \]

and so we may assume that \( \mathbb{F} = \mathbb{A} \) and \( I \) is maximal in \( A \). Then \( \mathbb{F} : \mathbb{K} \) is algebraic. Since \( B = A[\mathbb{F}] \) we conclude from 7.1.7, \( B : A \) is integral. Hence by 7.2.5, there exists a maximal ideal \( M \) of \( B \) with \( I = A \cap M \). By 7.4.3, \( V(M) \neq \emptyset \). As \( V(M) \subseteq V(I) \) the proposition is proved.

**Theorem 7.4.5** [Hilbert’s Nullstellensatz] Let \( I \) be an ideal in \( A \). Then \( J(V(I)) = \text{rad} I \).

**Proof:** Let \( f \in \text{rad} I \) and \( u \in V(I) \). Then \( f^n \in I \) for some \( n \in \mathbb{Z} \). Thus \( f^n(u) = (f(u))^n \) and since \( \mathbb{F} \) is an integral domain, \( f(u) = 0 \). Thus \( f \in J(V(I)) \) and \( \text{rad} I \subseteq J(V(I)) \).

Next let \( 0 \neq f \in J(V(I)) \). It remains to show that \( f \in \text{rad} I \). Let \( E = D + f \) and put \( y = x_f \). Then \( \mathbb{K}[x_e, e \in E] = A[y] \). Let \( L \) be the ideal in \( A[y] \) generated by \( I \) and \( yf - 1 \). We claim that \( V_{\mathbb{F}}(L) = \emptyset \). Suppose \( c \in V_{\mathbb{F}}(L) \). Then \( c = (a, b) \) with \( a \in \mathbb{F}^D \) and \( b \in \mathbb{F} \). Let \( g \in I \). Then \( 0 = g(a, b) = g(a) \) and so \( a \in V(I) \). Since \( f \in J(V(I)) \) we get \( f(a) = 0 \). Hence \( 0 = (yf - 1)(a, b) = bf(a) - 1 = -1 \neq 0 \).

Thus indeed \( V_{\mathbb{F}}(L) = \emptyset \). \( \emptyset \) implies \( L = A[y] \). So there exists \( g_s(y) \in A[y], 0 \leq s \leq m \) and \( f_s, 1 \leq s \leq m \in I \) with

\[ 1 = g_0(y)(yf - 1) + \sum_{s=1}^{m} g_s(y)f_s \]

Let \( \mathbb{A} = A(x_d, d \in D) \) be the field of fractions of \( A \). Let \( \phi : A[y] \to \mathbb{A} \) be the unique ring homomorphism with \( \phi(a) = a \) for all \( a \in A \) and \( \phi(y) = f^{-1} \). Applying \( \phi \) to the previous equation we obtain:
\[ 1 = g_0(f^{-1})(f^{-1}f - 1) + \sum_{s=1}^{m} g_s(f^{-1})f_i = \sum_{s=1}^{m} g_i(f^{-1})f_i \]

Let \( t \in \mathbb{Z}^+ \) with \( t \geq \deg_y g_i(y) \) for all \( 1 \leq i \leq m \). Then \( g_i(f^{-1})f^m \in A \) and so \( g_i(f^{-1})f^mf_i \in AI = I \). So multiplying the previous displayed equation with \( f^m \) we get \( f^m \in I \) and so \( f \in \text{rad} \, I \) \( \square \)
Appendix A

Zorn’s Lemma

This chapter is devoted to prove Zorn’s lemma. To be able to do this we assume throughout this lecture notes that the axiom of choice holds. The axiom of choice states that if \((A_i, i \in I)\) is a nonempty family of nonempty sets then also \(\prod_{i \in I} A_i\) is not empty. That is there exists a function \(f : I \to \bigcup_{i \in I} A_i\) with \(f(i) \in A_i\). Naively this just means that we can pick an element from each of the sets \(A_i\).

A partial ordered set is a set \(M\) together with a reflexive, anti-symmetric and transitive relation \(\leq\). That is for all \(a, b, c \in M\)

\[
\begin{align*}
(a) & \quad a \leq a \quad \text{(reflexive)} \\
(b) & \quad a \leq b \text{ and } b \leq a \implies a = a \quad \text{(anti-symmetric)} \\
(c) & \quad a \leq b \text{ and } b \leq c \implies a \leq c \quad \text{(transitive)}
\end{align*}
\]

We say that \(a\) and \(b\) are comparable if \(a \leq b\) or \(b \leq a\). \((M, \leq)\) is called linear ordered if any two elements are comparable. Let \(C\) be a subset of \(M\), then \(C\) is also a partially ordered set with respect to \(\leq\). \(C\) is called a chain if any two elements in \(C\) are comparable, that is if \(C\) is linear ordered.

An upper bound \(m\) for \(C\) is an element \(M\) in \(M\) so that \(c \leq m\) for all \(c \in C\).

An least upper bound for \(C\) is an upper bound \(m\) so that \(m \leq d\) for all upper bounds \(d\) of \(C\). A function \(f : M \to M\) is called increasing if \(a \leq f(a)\) for all \(a \in M\).

An element \(m \in M\) is called a maximal element if \(a \leq m\) for all \(a \in M\) comparable to \(M\), i.e if \(a = m\) for all \(a \in M\) with \(M \leq a\). We are now able to state Zorn’s Lemma

**Theorem A.1 (Zorn) [Zorn]** Let \(M\) be a nonempty partially ordered set in which every chain has an upper bound. Then \(M\) has a maximal element.

As the main steps toward a proof of Zorn’s lemma we show:

**Lemma A.2 [fixedpoint]** Let \(M\) be a non-empty partially ordered set in which every non-empty chain has a least upper bound. Let \(f : M \to M\) be an increasing function. Then \(f(m_0) = m_0\) for some \(m_0 \in M\).
Proof: To use that $M$ is not empty pick $a \in M$. Replacing $M$ by $\{m \in M \mid a \leq m\}$ we may assume that $a \leq m$ for all $m \in M$. We aim is to find a subset of $M$ which is a chain and whose upper bound necessarily a fixed-point for $f$. We will not be able to reach both these properties in one shot and we first focus on the second part. For this we define a subset $A$ of $M$ to be closed if:

(L a) $a \in A$

(L b) $f(b) \in A$ for all $b \in A$.

(L c) If $C$ is a non-empty chain in $A$ then its least upper bound is in $A$.

Since $M$ is closed, there do exists closed subsets. Suppose that there exists an closed subset which is a chain. By (L a), $A$ is not empty. Let $m_0$ be its least upper bound. By (L c), $m_0 \in A$ and by (L b), $f(m_0) \in A$. Thus $f(m_0) \leq m_0$ and as $\leq$ is anti symmetric $f(m_0) = m_0$.

So all what remains to do is to find a closed chain. There is an obvious candidate: It is immediate from the three conditions of closed that the intersection closed sets is still closed. So let $A$ be the intersection of all the closed sets.

Define $e \in A$ to be extreme if

$$f(b) \leq e \text{ for all } b \in A \text{ with } b < e$$

Note that $a$ extreme, so the set $E$ of extreme elements in $A$ is not empty.

Here comes the main point of the proof

Claim 1: Let $e$ be extreme and $b \in A$. Then $b \leq e$ or $f(e) \leq b$. In particular, $e$ and $b$ are comparable.

To prove Claim 1 put

$$A_e = \{b \in A \mid b \leq e \text{ or } f(e) \leq b\}$$

We need to show that $A_e = A$. As $A$ is the unique minimal closed set we just need to show that $A_e$ is closed.

Clearly $a \in A_e$. Let $b \in A_e$. If $b < e$, then as $e$ is extreme, $f(b) \leq e$ and so $f(b) \in A_e$. If $e = b$, then $f(e) = f(b)$ and again $f(b) \in A_e$. If $f(e) \leq b$. Then $f(e) \leq b \leq f(b)$ and $f(e) \leq f(b)$ by transitivity. So again $f(b) \in A_e$.

Finally, Let $D$ be a non-empty chain in $A_e$ and $m$ its least upper bound. If $d \leq e$ for all $d \in D$, then $e$ is an upper bound for $D$ and so $m \leq e$ and $m \in A_e$. So suppose that $d \not\leq e$ for some $d \in D$. As $d \in A_e$, $f(e) \leq d \leq m$ and again $m \in A_e$.

We proved that $A_e$ is closed. Thus $A_e = A$ and the claim holds.

Claim 2: $E$ is closed.

Indeed, $a \in E$. Let $e \in E$ and $b \in A$ with $b < f(e)$. We need to show that $f(b) \leq f(e)$. By Claim 1,$b \leq e$ or $f(e) \leq b$.The latter case is impossible by anti-symmetry. If $b < e$, then
since $e$ is extreme, $f(b) \leq e \leq f(e)$. If $e = b$, then $f(b) = f(e) \leq f(e)$. So $f(e)$ is extreme. Finally let $D$ be a non-empty chain in $E$ and $m$ its least upper bound. We need to show that $m$ is extreme. Let $b \in A$ with $b < m$. As $m$ is a least upper bound of $D$, $b$ is not an upper bound and there exits $e \in D$ with $e \not\leq b$. By claim 1, $e$ and $b$ are comparable and so $b < e$. As $e$ is extreme, $f(b) \leq e \leq f(e)$ and so $m$ is extreme. So $E$ is closed.

As $E$ is closed and $E \subseteq A$, $A = E$. Hence by Claim 2, any two elements in $A$ are comparable. So $A$ is a chain. As remarked above, the least upper bound for $A$ is a fixed point of $f$.

As an immediate consequence we get:

**Corollary A.3 [weakzorn]** Let $M$ be a non-empty partially ordered set in which every non-empty chain has a least upper bound. Then $M$ has a maximal element.

**Proof:** Suppose not. Then for each $m \in M$ there exists $f(m)$ with $m < f(m)$. (The axiom of choice is used here). But then $f$ is a strictly increasing function, a contradiction to A.2

**Lemma A.4 [maxchain]** Let $M$ be any partial ordered set. Order the set of chains in $M$ by inclusion. Then $M$ has a maximal chain.

**Proof:** Let $\cal M$ be the set of chains in $M$. The union of a chain in $M$ is clearly a chain in $M$ and is an lower bound for the chain. Thus A.3 applied to $\cal M$ yields a maximal member of $\cal M$. That is a maximal chain in $M$.

**Proof of Zorn’s Lemma** By A.4 there exists a maximal chain $C$ in $M$. By assumption $C$ has an upper bound $m$. Suppose that $m \leq a$ for some $a \in M$. Then $C \cup \{m, l\}$ is a chain in $M$ and the maximality of $C$ implies $l \in C$. Thus $l \leq m$ and $m = l$. Thus $m$ is maximal element.

As an application of Zorn’s lemma we prove the well-ordering principal. A partially ordered set $M$ is called well ordered if it is a chain and if every non-empty subset $I$ of $M$ has a least element, that is there exists an lower bound $i$ of $I$ with $i \in I$. We say that a set can be well ordered if the exists a relation " $\leq$ " on $M$ so that $(M, " \leq " )$ is well ordered.

**Theorem A.5 (Well-ordering principal) [wellorder]** Every set $M$ can be well ordered.

**Proof:** Let $\cal M$ be the set of well ordered sets $\alpha = (M_\alpha, \leq_\alpha)$ with $M_\alpha \leq M$. As the empty set can be well ordered, $\cal M$ is not empty. For $\alpha, \beta \in \cal M$ define $\alpha \leq \beta$ if

< 1. $M_\alpha \leq M_\beta$
<2. \( \leq_\beta |M_\alpha \times M_\alpha| \leq_\alpha \).

<3. \( a \leq_\beta b \) for all \( a \in M_\alpha, b \in M_\beta \setminus M_\alpha \)

It is easy to see that \( \leq \) is a partial ordering on \( M \). We would like to apply Zorn’s lemma to obtain a member in \( M \). For this let \( \mathcal{A} \) be a chain in \( M \). Put \( M_\alpha = \bigcup_{\alpha \in \mathcal{A}} M_\alpha \) and for \( a, b \in M_\alpha \) define \( a \leq_\alpha b \) if there exists \( \alpha \in \mathcal{A} \) with \( a, b \in M_\alpha \) and \( a \leq_\alpha b \). Again it is readily verified that \( \leq_\alpha \) is a well define partial ordering on \( M_\alpha \). Is it well ordered? Let \( I \) be any non-empty subset of \( M^* \) and pick \( \alpha \in \mathcal{A} \) so that \( I \cap M_\alpha \neq \emptyset \). Let \( m \) be the least element of \( I \cap M_\alpha \) with respect to \( \leq_\alpha \). We claim that \( m \) is also the least element of \( I \) with respect to \( \leq_\ast \). Indeed let \( i \in I \). If \( i \in M_\alpha \), then \( m \leq_\alpha i \) by choice of \( m \). So also \( m \leq_\ast i \). If \( i \not\in M_\alpha \), pick \( \beta \in \mathcal{A} \) with \( i \in M_\beta \). As \( \mathcal{A} \) is a chain, \( \alpha \) and \( \beta \) are comparable. As \( i \in M_\beta \setminus M_\alpha \) we get \( \alpha < \beta \) and (3) implies \( m \leq_\beta i \). Again \( m \leq_\ast i \) and we conclude that \( (M_\alpha, \leq_\alpha) \) is well ordered. Clearly it is also an upper bound for \( \mathcal{A} \).

So by Zorn’s lemma there exists a maximal element \( \alpha \in \mathcal{M} \). Suppose that \( M_\alpha \neq M \) and pick \( m \in M \setminus M_\alpha \). Define the partially ordered set \( (M_\alpha, \leq_\ast) \) by \( M_\ast = M_\alpha \cup \{m\} \), \( \leq_\ast |M_\alpha \times M_\ast = \leq_\alpha \) and \( i \leq_\ast m \) for all \( i \in M_\alpha \). Then clearly \( (M_\ast, \leq_\ast) \) is a well-ordered set and \( \alpha < (M_\ast, \leq_\ast) \), a contradiction to the maximality of \( \alpha \).

Thus \( M_\alpha = M \) and \( \leq_\alpha \) is a well ordering on \( M \).

The well ordering principal allows to prove statement about the elements in an arbitrary set by induction. This works as follows. Suppose we like to show that a statement \( P(m) \) is true for all elements \( m \) in a set \( M \). Endow \( M \) with a well ordering \( \leq \) a suppose that we can show

\[
P(a) \text{ is true for all } a < m \implies P(m)
\]
then the statement is true for all \( m \in M \). Indeed suppose not and put \( I = \{i \in M \mid P(i) \text{ is false }\} \). Then \( I \) has a least element \( m \). Put then \( P(a) \) is true for all \( a < i \) and so \( P(i) \) is true by the induction conclusion.

A well-ordering can also be used to define objects by induction:

**Lemma A.6 [defind]** Let \( I \) be a well ordered set and \( S \) a set. For \( a \in I \) let \( I^a = \{i \in I \mid i \leq a \} \) and \( I_a = \{i \in I \mid i < a \} \). Suppose that for each \( a \in I \), \( F_a \) is a set of functions from \( I^a \rightarrow S \).

Also suppose that if \( f : I_a \rightarrow S \) is a function with \( f |_{I_b} \in F_b \) for all \( b \in I_a \), then there exists \( f \in F_a \) with \( \overline{f} |_{I_a} = f \).

Then there exists \( f : I \rightarrow S \) with \( f |_{I_a} \in F_a \) for all \( a \in A \).

**Proof:** Let \( I \) be the set of all subsets \( J \) of \( I \) so \( a \leq b \in J \) implies \( a \in J \). Note that either \( J = R \) or \( J = I_a \) where \( a \) is the least element of \( R \setminus I \). Put

\[
\mathcal{M} = \{ f : J_f \rightarrow S \mid J_f \in I, f |_{I_a} \in F_a, \forall a \in J \}
\]

Order \( \mathcal{M} \) by \( f \leq g \) if \( J_f \subset J_g \) and \( g |_{J_f} \). Let \( C \) be a chain in \( \mathcal{M} \). Put \( J = \bigcup_{f \in C} J_f \). Clearly \( J \in I \).

Define \( f : J \rightarrow S \) by \( f(j) = g(j) \) where \( g \in C \) with \( j \in J_g \). Then also \( f |_{I} = g |_{I} \).
and so $f \in \mathcal{M}$. Thus $f$ is an upper bound for $\mathcal{M}$. By Zorn’s lemma, $\mathcal{M}$ has a maximal member $f$. If $J_f = R$ we are done. So suppose $J_f \neq R$. Then $J_f = I_a$ for some $a \in I$. Buy assumptions there exists $\tilde{f} \in \mathcal{F}_a$ with $\tilde{f} |_{I_a} = f$. But then $\tilde{F} \in \mathcal{M}$ and $f < \tilde{f}$, a contradiction to the maximal choice of $f$. \qed
Appendix B

Categories

In this chapter we give a brief introduction to categories.

Definition B.1 A category is a class of objects \( C \) together with

(i) for each pair \( A \) and \( B \) of objects a set

\[ \text{Hom}(A, B), \]

an element \( f \) of \( \text{Hom}(A, B) \) is called a morphism from \( A \) to \( B \) and denoted by \( f : A \rightarrow B \);

(ii) for each triple \( A, B, C \) of objects a function

\[ \text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C), \]

for \( f : A \rightarrow B \) and \( g : B \rightarrow C \) we denote the image of \( (g, f) \) under this function by \( g \circ f \), \( g \circ f : A \rightarrow C \) is called the composite of \( f \) and \( g \);

so that the following rules hold:

(I) [Associative] If \( f : A \rightarrow B \), \( g : B \rightarrow C \) and \( h : C \rightarrow D \) are morphisms then

\[ h \circ (g \circ f) = (h \circ g) \circ f \]

(II) [Identity] For each object \( A \) there exists a morphism \( \text{id}_A : A \rightarrow A \) such that for all \( f : A \rightarrow B \) and \( g : B \rightarrow A \)

\[ f \circ \text{id}_A = f \text{ and } \text{id}_A \circ g = g \]

A morphism \( f : A \rightarrow B \) in the category \( C \) is called an equivalence if there exists \( g : B \rightarrow A \) with

\[ f \circ g = \text{id}_B \text{ and } g \circ f = \text{id}_A \]
Two objects $A$ and $B$ are called \textit{equivalent} if there exists an equivalence $f : A \rightarrow B$. Note that associativity implies that the composite of two equivalences is again an equivalence.

\textbf{Examples}

Let $\mathcal{S}$ be the class of all sets. For $A, B \in \mathcal{S}$, let $\text{Hom}(A, B)$ be the set of all functions from $A \rightarrow B$. Also let the composites be defined as usual. Note that a morphism is an equivalence if and only if it is a bijection.

The class of all groups with morphisms the group homomorphisms forms category $\mathcal{G}$.

Let $\mathcal{C}$ be a category with a single object $A$. Let $G = \text{Hom}(A, A)$. The composite

$$G \times G \rightarrow G$$

is a binary operation on $G$. (I) and (II) now just mean that $G$ is a monoid. Conversely every monoid gives rise to a category with one object which we will denoted by $\mathcal{C}_G$. An object in $\mathcal{C}_G$ is equivalent to $e_G = \text{id}_A$ if and only if it has an has inverse.

Let $\mathcal{G}$ be a monoid. For $a, b \in \mathcal{G}$ define $\text{Hom}(a, b) = \{x \mid xa = b\}$. If $x : a \rightarrow b$ and $y : b \rightarrow c$. Then $(yx)a = y(xa) = yb = c$ so $yx : a \rightarrow c$. So composition can be defined as multiplication. The resulting category is denoted by $\mathcal{C}(\mathcal{G})$.

The class of all partially ordered sets with morphisms the increasing functions is a category.

Let $I$ be a partially ordered set. Let $a, b \in I$. If $a \leq b$ define $\text{Hom}(a, b) = \emptyset$. If $a \leq b$ then $\text{Hom}(a, b)$ has a single element, which we denote by "$a \rightarrow b$". Define the composite by

$$(b \rightarrow c) \circ (a \rightarrow b) = (a \rightarrow c)$$

this is well defined as partial orders are transitive. Associativity is obvious and $a \rightarrow a$ is an identity for $A$. We denote this category by $\mathcal{C}_I$.

Let $\mathcal{C}$ be any category. Let $\mathcal{D}$ be the class of all morphisms in $\mathcal{C}$. Given morphisms $f : A \rightarrow B$ and $g : C \rightarrow D$ in $\mathcal{C}$ define $\text{Hom}(f, g)$ to be the sets of all pairs $(\alpha, \beta)$ with $\alpha : A \rightarrow C$ and $\beta : B \rightarrow D$ so that $g \circ \alpha = \beta \circ f$, that is the diagram:

$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{\alpha} & & \downarrow{\beta} \\
C & \xrightarrow{g} & D
\end{array}$

commutes.

Let $\mathcal{C}$ be a category. The \textit{opposite} category $\mathcal{C}^{\text{op}}$ is defined as follows:

The objects of $\mathcal{C}^{\text{op}}$ are the objects of $\mathcal{C}$.

$\text{Hom}^{\text{op}}(A, B) = \text{Hom}(B, A)$ for all objects $A, B$. $f \in \text{Hom}^{\text{op}}(A, B)$ will be denoted by

$$f : A \xleftarrow{\text{op}} B \quad \text{or} \quad f : A \leftarrow B$$
The opposite category is often also called the dual or arrow reversing category. Note that two objects are equivalent in \( C \) if and only if they are equivalent in \( C^{\text{op}} \).

**Definition B.2** (a) An object \( I \) in a category is called universal (or initial) if for each object \( C \) of \( C \) there exists a unique morphism \( I \to C \).

(b) An object \( I \) in a category is called couniversal (or terminal) if for each object \( C \) of \( C \) there exists a unique morphism \( C \to I \).

Note that \( I \) is initial in \( C \) if and only if its terminal in \( C^{\text{op}} \).

The initial and the terminal objects in the category of groups are the trivial groups. Let \( I \) be a partially ordered set. A object in \( C_I \) is initial if an only if its a least element. Its terminal if and only if its a greatest element.

Let \( G \) be a monoid and consider the category \( C(G) \). Since \( g : e \to g \) is the unique morphism form \( e \) to \( G \), \( e \) is a initial object. \( e \) is a terminal object if and only if \( G \) is a group.

**Theorem B.3** [uniuni] Any two initial (resp. terminal) objects in a category \( I \) are equivalent.

**Proof:** Let \( A \) and \( B \) be initial objects. In particular, there exists \( f : A \to B \) and \( g : B \to A \). Then \( \text{id}_A \) and \( g \circ f \) both are morphisms \( A \to A \). So by the uniqueness claim in the definition of an initial object, \( \text{id}_A = g \circ f \), by symmetry \( \text{id}_B = f \circ g \).

Let \( A \) and \( B \) be terminal objects. Then \( A \) and \( B \) are initial objects in \( C^{\text{op}} \) and so equivalent in \( C^{\text{op}} \). Hence also in \( C \). \( \square \)

**Definition B.4** Let \( C \) be a category and \( (A_i, i \in I) \) a family of objects in \( C \). A product for \( (A_i, i \in I) \) is an object \( P \) in \( C \) together with a family of morphisms \( \pi_i : P \to A_i \) such that any object \( B \) and family of homomorphisms \( (\phi_i : B \to A_i, i \in I) \) there exists a unique morphism \( \phi : B \to P \) so that \( \pi_i \circ \phi = \phi_i \) for all \( i \in I \). That is the diagram commutes:

\[
P \xrightarrow{\phi} B \\
\downarrow \pi_i \downarrow \phi_i \\
A_i
\]

commutes for all \( i \in I \).

Any two products of \( (G_i, i \in I) \) are equivalent in \( C \). Indeed they are the terminal object in the following category \( E \)
The objects in $\mathcal{E}$ are pairs $(B, (\phi_i, i \in I))$ there $B$ is an object and $(\phi_i : B \to A_i, i \in I)$ is a family of morphism. A morphism in $\mathcal{E}$ from $(B, (\phi_i, i \in I))$ to $(D, (\psi_i, i \in I))$ is a morphism $\phi : B \to D$ with $\phi_i = \psi_i \circ \phi$ for all $i \in I$.

A coproduct of a family of objects $(G_i, i \in I)$ in a category $\mathcal{C}$ is its product in $\mathcal{C}^{\text{op}}$. So it is an initial object in the category $\mathcal{E}$. This spells out to:

**Definition B.5** Let $\mathcal{C}$ be a category and $(A_i, i \in I)$ a family of objects in $\mathcal{C}$. A coproduct for $(A_i, i \in I)$ is an object $P$ in $\mathcal{C}$ together with a family of morphisms $\pi_i : A_i \to P$ such that for any object $B$ and family of homomorphisms $(\phi_i : A_i \to B, i \in I)$ there exists a unique morphism $\phi : P \to B$ so that $\phi \circ \pi_i = \phi_i$ for all $i \in I$. 

Bibliography


Index

\begin{itemize}
\item \textit{FA(I)}, 32
\item \textit{(A)}, 61
\item \textit{J(U)}, 204
\item \textit{N_G(H)}, 21
\item \textit{R[G]}, 55
\item \textit{R[I]}, 81
\item \textit{R[[G]]}, 83
\item \textit{R^e[G]}, 61
\item \textit{R^a_p}, 57
\item \textit{R^p}, 79
\item \textit{S^{-1}R}, 75
\item \textit{V(S)}, 204
\item \textit{Z(G)}, 44
\item \textit{\tau}, 75
\item \textit{\text{F}_{R}}, 76
\item \textit{Syl_p(G)}, 47
\item \textit{Fix_S(G)}, 44
\item \textit{\text{rad}_R I}, 199
\item \textit{p-group}, 44
\item \textit{p-subgroup}, 47
\item \textit{\mathcal{P}(G)}, 16
\item \textit{[L:K]}, 143
\end{itemize}

 skew symmetric, 178

 abelian, 10
 action, 41
 affine variety, 204
 algebraic, 144
 algebraic closure, 147
 algebraically closed, 147
 algebraically dependent, 164
 algebraically independent, 164
 alternating, 178
 annihilator, 95

 anti homomorphism, 8
 anti-homomorphism, 57
 anti-symmetric, 207
 arrow reversing, 215
 associate, 66
 Associative, 213
 associative, 9
 augmentation ideal, 61
 automorphism, 7

 basis, 120
 bilinear, 113
 bimodule, 111
 binary operation, 7

 category, 213
 center, 44
 chain, 207
 characteristic, 58
 characteristic polynomial, 142, 194
 Chinese Remainder Theorem, 65
 closed, 204
 common divisor, 72
 commutative, 10
 commuting homomorphism, 29
 comparable, 207
 complete ring of fraction, 76
 composite, 213
 composition series, 128
 coproduct, 216
 cosets, 16
 couniversal, 215
 cut, 130
 cyclic, 112

 degree, 81, 143
multilinear, 171
multiple root, 89
multiplication table, 7
multiplicative subset, 74
multiplicity, 89

norm, 73
normal, 17, 149
normal closure, 160
normalizer, 21
normalizes, 21

opposite, 8, 214
opposite ring, 57
orbits, 42
order, 7

pairing, 188
perfect, 168
PID, 67
polynomial ring, 81
polynomials, 81
power semigroup ring, 83
power set, 16, 43
pre-group, 7
prime, 67
prime ideal, 63
primitive, 90
principal ideal, 67
principal ideal domain, 67
principal ideal ring, 67
product, 215
purely inseparable, 152

radical, 199
reflexive, 207
relation, 37, 39
relatively prime, 72
representatives, 44
right evaluation, 87
ring, 53
ring extension, 197
ring homomorphism, 57
root, 88
self-dual, 113
semigroup, 9
semigroup ring, 55
separable, 150
sequence, 97
series, 128
similar, 138
simple, 124
simple ring, 60
split, 99
splits, 145
splitting field, 148
stable, 159
stable, 149
submodule, 94
subring, 60
support, 30
Sylow p-subgroup, 47
symmetric, 178
symmetric power, 179
tensor product, 172
terminal, 215
torsion element, 122
torsion free, 122
torsion module, 122
transcendence basis, 166
transcendental, 144
transitive, 42, 207

UFD, 69
unique factorization domain, 69
unitary, 94
universal, 215
upper bound, 207

well ordered, 209
word, 33

zero divisor, 56