# Contents

1 Introduction

1.1 Unique factorization ........................................... 1
1.2 Some notation .................................................. 2
1.3 Categories ..................................................... 3
1.4 Representation and action ..................................... 5
1.5 Right versus left ............................................... 7

2 Basic group theory

2.1 Cosets and double cosets ....................................... 11
2.2 Quotients and isomorphism .................................... 12
2.3 Subgroups and action .......................................... 13
2.4 Commutator theory ............................................. 15
2.5 Extensions ..................................................... 17
2.6 Solvable groups ............................................... 19
2.7 Nilpotent groups ............................................... 20
2.8 Finite \( p \)-groups and Sylow’s First Theorem ............... 22
2.9 Direct products and sums ...................................... 23
2.10 Problems ..................................................... 26

3 Permutation and Linear Groups

3.1 Permutation groups ............................................. 29
3.1.1 Basics ..................................................... 29
3.1.2 Transitivity ............................................... 30
3.1.3 Primitivity ................................................ 34
3.1.4 Sylow’s Theorems ......................................... 35
3.1.5 Problems .................................................. 37
3.2 Linear groups .................................................. 39
3.2.1 Basics ..................................................... 39
3.2.2 Irreducibility ............................................... 40
3.2.3 Primitivity ................................................ 42
3.2.4 Unipotent linear groups ................................... 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.5 Sylow’s First Theorem (third time)</td>
<td>45</td>
</tr>
<tr>
<td>3.2.6 Problems</td>
<td>45</td>
</tr>
<tr>
<td>4 Finiteness and Reduction</td>
<td>47</td>
</tr>
<tr>
<td>4.1 Finiteness: Sylow’s First Theorem, one last time</td>
<td>47</td>
</tr>
<tr>
<td>4.2 Finite generation and countability</td>
<td>49</td>
</tr>
<tr>
<td>4.3 Limits and finite approximation</td>
<td>51</td>
</tr>
<tr>
<td>4.4 Representational finiteness</td>
<td>54</td>
</tr>
<tr>
<td>4.5 Chain conditions</td>
<td>55</td>
</tr>
<tr>
<td>4.6 Problems</td>
<td>57</td>
</tr>
<tr>
<td>5 Symmetric and alternating groups</td>
<td>59</td>
</tr>
<tr>
<td>5.1 Transpositions</td>
<td>59</td>
</tr>
<tr>
<td>5.2 The Weyl group $W(A_k)$</td>
<td>60</td>
</tr>
<tr>
<td>5.3 The alternating group and simplicity</td>
<td>62</td>
</tr>
<tr>
<td>5.4 Geometry and automorphisms</td>
<td>64</td>
</tr>
<tr>
<td>5.5 Problems</td>
<td>67</td>
</tr>
<tr>
<td>6 Matrices</td>
<td>69</td>
</tr>
<tr>
<td>6.1 Elementary matrices and operations</td>
<td>69</td>
</tr>
<tr>
<td>6.2 Bruhat decomposition</td>
<td>72</td>
</tr>
<tr>
<td>6.3 The Dieudonné determinant</td>
<td>78</td>
</tr>
<tr>
<td>6.4 $(B,N)$-pairs</td>
<td>81</td>
</tr>
<tr>
<td>6.5 Simplicity</td>
<td>86</td>
</tr>
<tr>
<td>6.6 Problems</td>
<td>89</td>
</tr>
<tr>
<td>7 Projective Spaces</td>
<td>91</td>
</tr>
<tr>
<td>7.1 Projective spaces</td>
<td>91</td>
</tr>
<tr>
<td>7.2 The Fundamental Theorem of Projective Geometry</td>
<td>92</td>
</tr>
<tr>
<td>8 Linear transformations</td>
<td>95</td>
</tr>
<tr>
<td>8.1 The dual space</td>
<td>95</td>
</tr>
<tr>
<td>8.2 Matrix representation</td>
<td>97</td>
</tr>
<tr>
<td>8.3 The finite linear groups</td>
<td>97</td>
</tr>
<tr>
<td>8.4 Finitary linear transformations</td>
<td>98</td>
</tr>
<tr>
<td>8.5 Transvections</td>
<td>99</td>
</tr>
<tr>
<td>8.6 Problems</td>
<td>100</td>
</tr>
<tr>
<td>9 Pairings, Isometries, and Automorphisms</td>
<td>103</td>
</tr>
<tr>
<td>9.1 Pairings</td>
<td>103</td>
</tr>
<tr>
<td>9.2 The isometry groups of pairings</td>
<td>107</td>
</tr>
<tr>
<td>9.3 Elations and automorphisms</td>
<td>112</td>
</tr>
<tr>
<td>9.4 Problems</td>
<td>113</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Unique factorization

We are familiar with

(1.1). Theorem. For $n$ a positive integer at least 2, let

$$n = \prod_{i=1}^{k} p_i$$

and

$$n = \prod_{j=1}^{m} q_j$$

where each $p_i$ and $q_j$ is prime. Then $k = m$ and there is a permutation $\pi$ with $p_i = q_{\pi(j)}$, for all $i$. □

Here a prime is a positive integer not 1 and only divisible by 1 and itself.

A group $S$ is simple if it is not 1 and has only 1 and itself as homomorphic images. The appropriate unique factorization theorem for finite groups is then

(1.2). Theorem. (Jordan-Hölder) For $G$ a nontrivial finite group, let

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_k = 1$$

and

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = 1$$

where each $P_i = G_{i-1}/G_i$ and $Q_j = H_{j-1}/H_j$ is simple. Then $k = m$ and there is a permutation $\pi$ with $P_i \simeq Q_{\pi(j)}$, for all $i$. □

A big difference between the two factorization results is that the first admits the natural converse. Two positive integers with the same multiset of prime
divisors are equal, but two groups (even abelian groups) with the same multiset of composition factors might not be isomorphic. So while number theory can focus on properties of the prime numbers, in finite group theory we must not only examine the simple groups but also study in what ways they can be glued together.

A major result identifies the possible factors in a Jordan-Hölder composition series:

(1.3) **Theorem.** (Classification of finite simple groups (CFSG), 1983, 2004) A finite simple group is isomorphic to one of:

1. a cyclic group of prime order \( p \): \( \mathbb{Z}_p \);
2. an alternating group: \( \text{Alt}(n) \);
3. a classical group: \( \text{PSL}_n(q), \text{PSp}_n(q), \text{PSU}_n(q), \text{PO}_n(q) \);
4. an exceptional Lie type group \( 2\text{B}_2(q), 3\text{D}_4(q), \text{E}_6(q), \text{E}_7(q), \text{E}_8(q), \text{F}_4(q), 2\text{F}_4(q), \text{G}_2(q), 2\text{G}_2(q) \);
5. a sporadic simple group, of which there are twenty-six.

Here \( n \) is an integer at least 2 and \( q \) is a prime power. Most choices of these two parameters do in fact give simple groups. The classical groups provide four two-parameter infinite families, so one could say loosely that most finite simple groups are classical. These are the families of groups that will be of greatest interest to us, but there will rarely be any advantage in restricting our attention to those that are finite.

With CFSG in hand, to find all finite groups, we are faced with the problem of gluing things together: extension theory. One of the reasons to study the examples (and especially the classical groups) is that additional knowledge can aid us is solving such questions. For instance Theorem (1.1) can be refined to:

(1.4) **Theorem.** If \( A \) is a finite abelian group, then \( A \) is isomorphic to a direct sum \( \bigoplus_{i=1}^k A_i \), for cyclic subgroups \( A_i \) of order \( p_i^{a_i} \), with \( p_i \) prime and \( a_i \) a positive integer. Furthermore, if \( A \) is also isomorphic to \( \bigoplus_{j=1}^m B_j \), for cyclic subgroups \( B_j \) of order \( q_j^{b_j} \), with \( q_j \) prime and \( b_j \) a positive integer, then \( k = m \) and there is a permutation \( \pi \) with \( p_i = q_{\pi(i)} \) and \( a_i = b_{\pi(i)} \), for all \( i \).

This is clearly a “unique factorization” result, but it is also a Jordan-Hölder theorem. Indeed theorems of Jordan-Hölder type are valid for many lattices, provided certain properties hold and appropriate definitions are made. So, for Theorem (1.4) we require that all factors are indecomposable and that all extensions split.

### 1.2 Some notation

Let \( G \) be a group. If \( H \) is a subgroup of \( G \), then we write \( H \leq G \) and \( G \geq H \). We write \( H \trianglelefteq G \) and \( G \trianglerighteq H \) if \( H \) is a normal subgroup of \( G \). For the subset \( X \) of \( G \), \( \langle X \rangle \) is the subgroup of \( G \) generated by \( X \).
1.3. CATEGORIES

For $x, h \in G$ we write $x^h$ for $h^{-1}xh$, the conjugate of $x$ by $h$. More generally, for subsets $X$ and $H$ of $G$, we set $X^H = \{ x^h \mid x \in X, h \in H \}$. Be warned: in some group theory texts [Rob82], $X^H$ is defined to be the subgroup $(X^H)$. That is not our convention.

1.3 Categories

We shall not focus on categories and their role in modern algebra (which is large), but they provide us for a convenient language for setting up our work.

A category $C$ is a class Obj$(C)$ of objects. For each pair $A, B \in$ Obj$(C)$, there is a set Hom$_C(A, B)$, pairwise disjoint, of $C$-morphisms. For each triple of objects $A, B, C$, there is a composition map

$$\circ: \text{Hom}_C(A, B) \times \text{Hom}_C(B, C) \to \text{Hom}_C(A, C),$$

the image $\circ(f, g)$ usually being written $f \circ g$ or just $fg$\(^1\). The following are required:

(i) Always for $a \in \text{Hom}_C(A, B)$, $b \in \text{Hom}_C(B, C)$, and $c \in \text{Hom}_C(C, D)$ we have

$$(a \circ b) \circ c = a \circ (b \circ c) \in \text{Hom}_C(A, D).$$

(ii) For every object $X$ there is a unique morphism $1_X \in \text{Hom}_C(X, X)$, such that always for $a \in \text{Hom}_C(A, B)$ and $b \in \text{Hom}_C(B, C)$ we have

$$a \circ 1_B = a \text{ and } 1_B \circ b = b.$$

The notation $1_A$ can be confusing in those situations where the objects themselves have identity elements; for instance, we use $1_G$ to denote the identity element of the group $G$. Usually the usage will be clear from the context, but for clarity we will at times use Id to denote an identity map.

A motivating model for a category has Obj consisting of all sets with the morphism set Hom$(A, B)$ be all set maps (functions) from $A$ to $B$. Composition is then the usual composition of maps, and (i) observes that composition is associative. Then (ii) records the properties of the identity map $1_X = \text{Id}_X$ from the set $X$ to itself. We will denote this category Set.

Two objects $A$ and $B$ of the category $C$ are isomorphic if there are morphisms $a \in \text{Hom}_C(A, B)$ and $b \in \text{Hom}_C(B, A)$ with $ab = 1_A$ and $ba = 1_B$. For instance, two sets are isomorphic in Set precisely when they are in bijection.

It is crucial to note that the definition of a category does not require Obj$(C)$ to be a set. This is important since, for instance, we know that there is no such thing as the set of all sets. A category in which the class of objects is actually a set is a small category. Our definition is somewhat restrictive. By requiring

\(^1\)An alternative and common convention is to write $g \circ f$ and $gf$ for the composition of $f$ followed by $g$; see Section 1.5.
CHAPTER 1. INTRODUCTION

that each Hom\(_C(A, B)\) actually be a set, we have confined ourselves to those categories that are \textit{locally small}.

A \textit{subcategory} \(D\) of \(C\) is a category for which every object \(D\) of \(D\) is also an object of \(C\) and such that, for \(D, E \in \text{Obj}(D)\), we have \(\text{Hom}_D(D, E) \subseteq \text{Hom}_C(D, E)\). The subcategory \(D\) of \(C\) is \textit{full} if we always have the equality \(\text{Hom}_D(D, E) = \text{Hom}_C(D, E)\). The subcategory \(D\) of \(C\) is \textit{dense} if, for every object \(C\) of \(C\) there is an object \(D\) of \(D\) that is isomorphic to \(C\) in \(C\). For instance, the full subcategory \(FSet\) of finite sets within \(Set\) has, in turn, the full and dense subcategory \(ZFSet\) whose objects are the finite subsets of the integers.

A category \(C\) is \textit{concrete} if it is a subcategory of \(Set\). That is, if the objects of \(C\) are sets, perhaps decorated with additional structure, and the morphisms of \(\text{Hom}_C(A, B)\) are set maps, perhaps with additional, required properties. Our prime example is \(Grp\), the category of all groups in which the morphisms are the group homomorphisms.

We have already introduced the two important categories \(Set\) and \(Grp\). For us the third category of primary interest is \(DVec\), the category of all left vector spaces over the division ring \(D\). (Of course, we should really precede this by discussion of the categories \(Fld\) of fields and \(\text{DivRing}\) of \textit{division rings}—not necessarily commutative fields.) Here the morphisms are the \(D\)-linear transformations from one \(D\)-space to another.

These three main categories have important full subcategories: the category \(FSet\) of finite sets (mentioned above); the category \(FGrp\) of finite groups and the category \(AbGrp\) of abelian groups; and the category \(DFVec\) of finite dimensional left \(D\)-spaces.

Other categories of vector spaces will also be important to us. The categories \(Vec_D\), and \(DFVec_D\) are the right-space counterparts to the left-space categories \(DVec\) and \(DFVec\). A more subtle example is the category \(Vec\) of all left vector spaces. (It has righthanded counterpart \(RVec\).) Here the objects are pairs \((D, V)\) (or \(D V\)) of a division ring \(D\) and a left \(D\)-space \(V\). The morphisms must then also be pairs: \([\sigma, s] \in \text{Hom}_{vec}(D V_E W)\) where \(\sigma\) is a homomorphism from \(D\) to \(E\) (a morphism from \(\text{DivRing}\)) and \(s\) is an abelian group homomorphism (from \(AbGrp\)) that are compatible, in that for \(a, b \in D\) with

\[
\begin{align*}
a & \xrightarrow{\sigma} a' & a' & \xrightarrow{\sigma} b' \\
b & \xrightarrow{\sigma} b'
\end{align*}
\]

and \(u, v \in V\) with

\[
\begin{align*}
u & \xrightarrow{s} u' & u' & \xrightarrow{s} v' \\
v & \xrightarrow{s} v'
\end{align*}
\]

we always have

\[
au + bv \xrightarrow{[\sigma, s]} a'u' + b'v'.
\]

Such maps are \textit{semilinear}. It is important to realize that \(DVec\) is a subcategory of \(Vec\) that is typically not full, since, even for two spaces \(V\) and \(W\) both over \(D = E\), the latter allows \(\sigma\) to be a nontrivial automorphism of the division ring \(D\).
There are other categories we may encounter: rings $\text{Ring}$, modules $R\text{Mod}$ and $\text{Mod}_R$, and associative algebras $\text{Assoc}$. These concrete categories are additionally additive categories. This means that each object set has a natural structure as abelian group and that each morphism is an abelian group homomorphism.

For categories $C$ and $D$ a functor $F$ from $C$ to $D$ associates to each object $C$ of $C$ an object $F(C)$ of $D$ and to each morphism $f \in \text{Hom}_C(A,B)$ a morphism $F(f)$ of $\text{Hom}_D(F(A),F(B))$, such that always

$$F(f)F(g) = F(fg) \quad \text{and} \quad F(1_A) = 1_{F(A)}.$$

An obvious functor from $C$ to itself is the identity functor $1_C$ with $1_C A = A$ and $1_C(f) = f$. The two categories $C$ and $D$ are isomorphic provided there are functors $F: C \rightarrow D$ and $G: D \rightarrow C$ with $FG = 1_D$ and $GF = 1_C$.

Although isomorphism gives us an equivalence relation on the collection of all categories, it is not a terribly helpful one. We have observed above that the category $\text{FSet}$ of finite sets has the full, dense subcategory $\text{ZFSet}$ of finite subsets of the integers. These two categories are certainly not isomorphic, since the second is a small category while the first is not. On the other hand it seems relatively clear that the two categories do not differ in any other substantive way. More useful than isomorphism is category equivalence. Two categories are equivalent provided they have isomorphic full, dense subcategories. In particular $\text{FSet}$ and $\text{ZFSet}$ are equivalent categories.

In the category $C$, the morphisms of $\text{Hom}_C(A,A)$ are the $C$-endomorphisms, and we will write $\text{End}_C(A)$ for $\text{Hom}_C(A,A)$. Those endomorphisms of $A$ that are invertible, that is, are isomorphisms of $A$ with itself, are the $C$-automorphisms, written $\text{Aut}_C(A)$ even $\text{Aut}(A)$. As we see in the next section, these automorphism groups will play a central role for us. For instance $\text{Aut}_{\text{Set}}(A) = \text{Sym}(A)$.

### 1.4 Representation and action

In group theory as in most parts of mathematics, in order to study an object carefully we wish to have a description of it that is easy to work with. For groups, this is done by representing them through their action upon something. Such actions may also be the reasons we are studying the groups in the first place. For instance, Galois was the first to consider finite groups serious, and he encountered these groups as permutations of polynomial roots.

Let $A$ be an object of the category $C$. Then a $C$-representation of the group $G$ on $A$ is a homomorphism $\rho: G \rightarrow \text{Aut}_C(A)$. In this case we say that $G$ is a group of operators on $A$ and that $G$ acts on $A$ via $\rho$. This action of $G$ on $A$ is faithful if the kernel of $\rho$ is the identity.

Three types of categories $C$ and the associated representations within $\text{Aut}_C(\cdot)$ will be of particular interest to us:

\[2\text{Hooray for the Oxford comma.}\]
(1) In $\text{Set}$ each object $A$ is a set (with no further structure). Its automorphism group $\text{Aut}_C(A) = \text{Aut}_{\text{Set}}(A)$ is then $\text{Sym}(A)$, the \textit{symmetric group} of all permutations on the set $A$. The associated representations are \textit{permutation representations}.

(2) For the category $C = D\text{Vec}$ of vector spaces $V$ over the division ring $D$, the automorphism group is the \textit{general linear group} $\text{GL}_D(V)$, also written $\text{GL}(D,V)$ or $\text{GL}(V)$. The associated representations are the $D$-\textit{linear representations}. If instead we take the vector space $D V$ as an object in the category $\text{Vec}$ (with no uniformly specified coefficient ring) then we have $\text{Aut}_{\text{vec}}(D V) = \Gamma L_D(V)$ or $\Gamma L_D(V)$ or (with some abuse) $\Gamma L(V)$. The representations are now \textit{semilinear}, since they may involve nontrivial automorphisms of $D$.

(3) If $C = \text{Grp}$, the category of groups, then we are concerned with \textit{group automorphisms}.

In concrete categories, such as these, if $G$ acts on the object $A$ and $B$ is a subset of $A$ with $B^g \subseteq B$ for all $g \in G$, then we say that $B$ is $G$-\textit{invariant}. If $B$ is actually a subobject of $A$, then $G$ acts on $B$ via the restriction of $g$ to $B$, which we write as $g|_B$.

If the object $B$ of $C$ is isomorphic to $A$ via the morphism $f: A \rightarrow B$, then the commutative diagram:

\[
\begin{array}{ccc}
A & \xrightarrow{h} & A \\
\downarrow f & & \downarrow f \\
B & \xrightarrow{h^*} & B
\end{array}
\]

provides an isomorphism $f^*: \text{Aut}_C(A) \rightarrow \text{Aut}_C(B)$ given by

\[
h f^* h^* = f^{-1} h f.
\]

Any representation $\rho_A$ of $G$ on $A$ then has a naturally associated representation $\rho_B = \rho_A f^*$ on $B$; the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{\rho_A} & \text{Aut}_C(A) \\
\gamma \downarrow & & \downarrow f^* \\
H & \xrightarrow{\rho_B} & \text{Aut}_C(B)
\end{array}
\]

In this case $\rho_A$ and $\rho_B$ are said to be \textit{equivalent} representations. If $G$ is isomorphic to the group $H$ via the map $\gamma: G \rightarrow H$, and the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{\rho_A} & \text{Aut}_C(A) \\
\gamma \downarrow & & \downarrow f^* \\
H & \xrightarrow{\rho_B} & \text{Aut}_C(B)
\end{array}
\]

\footnote{In many places, a linear representation is required to be acting on a finite dimensional space from $D\text{FVec}$. This restriction will not be made here.}
then the two representations $\rho_A$ and $\rho_B$ are said to be *semiequivalent* with $\rho_B = \rho_A^{[\gamma, f]}$.

The equivalence $f^*$ is just the semiequivalence $(\text{Id}_G, f)$:

\[
\begin{array}{c|c}
G & \text{Aut}_C(A) \\
\hline
\text{Id}_G & \downarrow f^* \\
G & \text{Aut}_C(B)
\end{array}
\]

where we have used $\text{Id}_G$ to denote the identity endomorphism of $G$ in $\text{Grp}$.

If $C$ is an additive category, then the set of $C$-endomorphisms $\text{End}_C(A) = \text{Hom}_C(A, A)$ has a natural structure as a ring under composition and (pointwise) addition. In this case, we may also define a $C$-representation of a ring $R$ as a ring homomorphism $\varphi : R \rightarrow \text{End}_C(A)$ for $A$ and object of $C$, where we must require the identity of the ring $R$ to map to $1_A$. The group $\text{Aut}_C(A)$ is the group of units of $\text{End}_C(A)$, so for additive categories a representation of the group $G$ leads to a representation of the group ring $\mathbb{Z}G$. This can provide a powerful tool for study of $G$. We have concepts of equivalence and semiequivalence similar to those above.

### 1.5 Right versus left

Action on the left is exhibited by function composition,

\[ f(g(x)) = (fg)(x), \]

while action on the right is modeled by exponentiation,

\[ (x^f)^g = x^{fg}. \]

The distinction is largely a matter of convention. Analysts almost always favor left action, since they are regularly dealing with functions and their properties. Algebraists often prefer right action, and that is usually the case here. This is evidenced by our composition map for morphisms; our definitions $h^* = f^{-1}hf$ in the previous section and of conjugation by $x^g = g^{-1}xg$; and our chosen convention for permutation multiplication:

\[ (1, 2, 3, 4, 5)(2, 4, 6, 8) = (1, 4, 5)(2, 3, 6, 8). \]

We do not demand right action always. For instance, above we have written functors as functions and compose them as functions. And even when our action is on the right, we sometimes use function notation, for instance in characterizing a group homomorphism $\varphi : G \rightarrow H$ by $\varphi(g)\varphi(h) = \varphi(gh)$ (but here we must be careful to avoid casual composition).

Our preferred notation for right action is exponentiation

\[ a \xrightarrow{f} a^f, \]
but there may be times when it is helpful to use $af$ or even $a.f$ rather than $a^f$.
(In particular, nested exponentiation can look very confusing.)

In any event, there are situations where the correct thing is to use both right and left action. For instance our preferences for right action of morphisms and left scalar action on vector spaces go hand in hand:

**1.5. Proposition.** Let $V$ and $W$ be left vector spaces over the division ring $D$, and let $g$ be a $D$-endomorphism (linear transformation) from $V$ to $W$. That is, for $u,v \in V$ and $x,w \in W$ with

$$u \xrightarrow{g} x \text{ and } v \xrightarrow{g} w,$$

and, for $\alpha, \beta \in D$, we have

$$\alpha u + \beta v \xrightarrow{g} \alpha x + \beta w.$$

Let $e_1, \ldots, e_i, \ldots, e_m$ be a basis of $V$, so that $v = \sum_{i=1}^{m} v_i e_i$ of $V$ is represented in the left $D$-space of row vectors $D^m$ by

$$\vec{v} = (v_1, \ldots, v_i, \ldots, v_m).$$

Similarly let $f_1, \ldots, f_j, \ldots, f_n$ be a basis of $W$ with $w = \sum_{j=1}^{n} w_j f_j$ of $W$ represented in $D^n$ by

$$\vec{w} = (w_1, \ldots, w_j, \ldots, w_n).$$

Define the scalars $g_{ij}$ from $D$ by

$$e_i \xrightarrow{g} \sum_{j=1}^{n} g_{ij} f_j,$$

and then let $G = (g_{ij})_{ij}$ be the matrix of $D^{m,n}$ with $(i,j)$-entry $g_{ij}$. Then

$$\vec{v} G = \vec{w}.$$ 

The point here is the action of the morphism $g$ taking the left $D$-space $V$ to the left $D$-space $W$ is naturally represented via right multiplication by the matrix $G$.

Let $V$ and $W$ be left $D$-spaces with $\text{Hom}(V,W)$ the set of abelian group homomorphisms from $V$ to $W$ and $\text{Hom}_D(V,W) (= \text{Hom}_{D\text{Vec}}(V,W))$ the corresponding set of linear transformations—homomorphisms as left $D$-spaces. In this situation one often says that the $f$ of $\text{Hom}_D(V,W)$ are those homomorphisms whose group action “commutes” with the scalar action of $D$. Instead it might be better to say that these actions “associate,” since the condition that $f$ of $\text{Hom}(V,W)$ belongs to $\text{Hom}_D(V,W)$ is

$$(\alpha x)f = \alpha(xf),$$

for all $\alpha \in D$ and $x \in V$. 

1.5. RIGHT VERSUS LEFT

Of course, the matrix spaces
\[ D^m (= D^{1,m} = \text{Mat}_{1,m}(D)) \quad \text{and} \quad D^{m,n} (= \text{Mat}_{m,n}(D)) \]
have natural structure as both left and right \( D \)-spaces. But if \( D \) is a noncommutative division ring, care must be taken since, in general, \( \alpha \vec{x} \) and \( \vec{x} \alpha \) are different as are \( \gamma G \) and \( G \gamma \). The identity (from Proposition (1.5))

\[ (\alpha \vec{v}) (G \gamma) = \alpha (\vec{v} G) \gamma \]
tells us that \( D^{m,n} = \text{Hom}_{D\text{-Vec}}(D^m, D^n) \), taking left \( D \)-space \( D^m \) to left \( D \)-space \( D^n \), has its natural structure as a right \( D \)-space. (This is particularly important in discussion of dual spaces \( V^* = \text{Hom}_{D\text{-Vec}}(V, D) \).)

(1.6). Problem.
(a) Verify Proposition (1.5).
(b) In the situation of Proposition (1.5), let \( h \) be a second \( D \)-endomorphism from \( V \) to \( W \) and \( H \) the corresponding matrix representing \( h \) with respect to the bases \( e_1, \ldots, e_i, \ldots, e_m \) and \( f_1, \ldots, f_j, \ldots, f_n \). Prove that the \( D \)-endomorphism \( g + h \) is represented by the matrix \( G + H \) and so that, as abelian groups, \( \text{Hom}_D(V, W) \) and \( \text{Mat}_{m,n}(D) \) are isomorphic.
(c) Consider the special case \( V = W \) and \( e_i = f_i \), for all \( i \). Prove that \( \text{End}_D(V) \) and \( \text{Mat}_n(D) \) are isomorphic as rings.

Remark. When rephrased appropriately, these remarks remain valid for arbitrary rings \( R \) with identity where \( V \) and \( W \) are free \( R \)-modules.
CHAPTER 1. INTRODUCTION
Chapter 2

Basic group theory

2.1 Cosets and double cosets

If $X$ and $Y$ are subsets of $G$, then

$$XY = \{ xy \mid x \in X, y \in Y \}.$$ 

In particular, if $X \leq G$ and $Y = \{y\}$ then $XY$ is a coset of $X$ in $G$ (as is $yX$).\footnote{These days $HY$ is usually called a right coset and $yH$ a left coset \cite{Asc00}, but in the past \cite{Hil59} it was often the other way around.} The number of distinct cosets $XY$ in $G$ is the index of $X$ in $G$, written $[G:X]$. (It is equal to the number of distinct cosets $yX$ in $G$; see Problem \cite{Pro2.36}).

The basic result on cosets is:

(2.1). Lemma. Let $H \leq G$ and $x, y \in G$.

(a) $Hx \cap Hy$ is either $Hx = Hy$ or is empty.

(b) $xH \cap yH$ is either $xH = yH$ or is empty.

(c) $|Hx| = |Hy| = |xH| = |yH|$.

(d) For $H \leq G$, $Hx = Hy$ if and only if $yx^{-1} \in H$; and $xH = yH$ if and only if $xy^{-1} \in H$.

We immediately have the central result of finite group theory.

(2.2). Theorem. (Lagrange's Theorem) If $G \geq H$ then $|G| = [G:H]|H|$.

Also of interest are double cosets $HxK$ for subgroups $H, K \leq G$. The double coset $HxK$ is a union of various cosets $Hxk$ of $H$ and of various cosets $hxK$ of $K$. As with cosets, two double cosets are either equal or disjoint, but unlike...
cosets, double cosets can have varying orders. For instance \( H \triangleleft H = H \) but other double cosets \( H \times H \) will likely contain more than one coset of \( H \).

The set \( \{ Hx \mid x \in G \} \) is often denoted \( H \backslash G \) and correspondingly we write \( \{ xH \mid x \in G \} = G \backslash H \) . Similarly \( \{ HxK \mid x \in G \} = H \backslash G/K \).

The product of cosets \( HxHy \) is the disjoint union of the cosets \( Hxhy \) and always contains the coset \( Hxy \). The identity \( HxHy = Hxy \) characterizes \( H \) as a normal subgroup of \( H \), as discussed below.

Double coset multiplication will also be of interest. Especially \( HxH \cdot HyH \) is always the union of the double cosets \( HxhyH \) and contains the double coset \( HxyH \).

### 2.2 Quotients and isomorphism

Two groups \( A \) and \( B \) are isomorphic provided they are the same group only with names changed. That is, there is a bijection \( \varphi: A \rightarrow B \) with \( a_1 \cdot a_2 = a_3 \) if and only if \( \varphi(a_1) \cdot \varphi(a_2) = \varphi(a_3) \).

If we are not concerned about the specific map \( \varphi \), we write \( A \simeq B \) to indicate that \( A \) and \( B \) are isomorphic.

Homomorphisms are more complicated. They are maps \( \varphi: A \rightarrow B \) still satisfying \( \varphi(a_1) \varphi(a_2) = \varphi(a_1a_2) \), but they need no longer be injective or surjective. Surjectivity can be forced by replacing \( B \) with the image \( \varphi(A) \). Still, we are not just renaming elements; we may be ignoring the distinctions between certain elements and identifying them with each other.

An arbitrary subgroup \( K \) of the group \( G \) is a normal subgroup of \( G \) if it is the kernel of some homomorphism. This is a qualitative definition. There are equivalent quantitative statements. In particular the subgroup \( K \) is normal if, for every \( x \in G \), \( Kx = xK \). Thus \( K \) is normal in \( G \) precisely when \( K^x = K \), for all \( x \in G \).

It is helpful to realize that the subgroup \( K \) is normal in \( G \) precisely when \( SK = KS \), for every subset \( S \) of \( G \). In particular, when \( K \) is normal, the cosets \( G/K = \{ Kx \mid x \in G \} \) do multiply naturally as sets:

\[ KxKy = Kxy. \]

The group \( G/K \) (with this multiplication) is the factor group or quotient group of \( G \) by \( K \).

For any homomorphism \( \varphi: G \rightarrow H \), the subgroup \( \{ g \in G \mid \varphi(g) = 1_H \} \) is the kernel of \( \varphi \), written \( \ker \varphi \), and is normal in \( \varphi(G) \).

### (2.3). Theorem. (First Isomorphism Theorem) Let \( \varphi: G \rightarrow H \) be a homomorphism of groups. Then the image \( \varphi(H) \) is isomorphic to the factor group \( G/K \), where \( K = \ker \varphi = \{ g \in G \mid \varphi(g) = 1_H \} \). The isomorphism is given by \( \varphi(g) \mapsto Kg \). \[ \square \] 

\(^2\)Care must be taken with this, since for many it implies that \( H \) is a normal subgroup.
The First Isomorphism Theorem is critical in all group theory. It says that every homomorphism has a canonical model.

2.4. Theorem. (Second Isomorphism Theorem) Let \( H \subseteq G \) and \( K \subseteq G \). Then \( HK = KH \subseteq G \), and \( HK/K \simeq H/H \cap K \) via the map \( Kh \mapsto (H \cap K)h \).

2.5. Theorem. (Third Isomorphism Theorem) Let \( G \supseteq N \) and \( G \geq K \geq N \). Then \( K \) is normal in \( G \) if and only if \( K/N \) is normal in \( G/N \). In that case, \( G/K \simeq (G/N)/(K/N) \).

The Second and Third Isomorphism Theorems discuss the lattices of subgroups and normal subgroups of a group. In particular the First and Third Isomorphism Theorems tell us that, for any surjective homomorphism \( \varphi : G \rightarrow H \), there is a natural bijection between the lattice of normal subgroups of \( H \) and the lattice of normal subgroups of \( G \) that contain \( \ker \varphi \).

The First and Third Isomorphism Theorems are often invoked without mention, while use the Second often occasions remark.

The isomorphism theorems together allow us to do a great deal of group theory. If in a category \( \mathbf{C} \) we have some counterpart to them, then \( \mathbf{C} \) becomes a much more manageable place to work. In particular, concepts like simplicity and results of Jordan-Hölder type are more approachable. Concrete categories like \( \mathbf{RMod} \) and \( \mathbf{Mod}_R \) have them, and the definition of abelian categories is designed to guarantee them in an appropriate form.

2.3. Subgroups and action

Each \( g \) of the group \( G \) acts on \( G \) via conjugation:

\[(xy)^g = g^{-1}xyg = g^{-1}xgg^{-1}yg = x^gy^g.\]

Our conjugacy definition \( x^g = g^{-1}xg \) makes conjugacy into a right action:

\[(x^g)^h = h^{-1}(g^{-1}xg)h = (gh)^{-1}x(gh) = x^{gh}.\]

The induced automorphism \( \iota_g \) is called an inner automorphism of \( G \). The image of the representation \( \iota : G \rightarrow \text{Aut}(G) (= \text{Aut}_{\text{Grp}}(G)) \) is the inner automorphism group \( \text{Inn}(G) \) and is normal in \( \text{Aut}(G) \). The kernel of the representation \( \iota \) consists of everything fixed by conjugation. That is the center \( Z(G) \) of \( G \):

\[Z(G) = \{ z \in G \mid zg = gz \text{ for all } g \in G \};\]

so \( \text{Inn}(G) \) is isomorphic to \( G/Z(G) \). The quotient \( \text{Aut}(G)/\text{Inn}(G) \) is the outer automorphism group of \( G \), denoted \( \text{Out}(G) \).

\[\text{Those who prefer left action will define the conjugate of } x \text{ by } g \text{ to be } gxg^{-1}, \text{ which can be denoted } ^g x \text{ giving } ^h( ^g x ) = ^{hg} x.\]
CHAPTER 2. BASIC GROUP THEORY

For any subset \( H \) of \( G \), the normalizer of \( H \) in \( G \) denoted \( N_G(H) \), is

\[
N_G(H) = \{ g \in G \mid H^g = H \}.
\]

This is the largest subgroup of \( G \) within which \( H \) is a normal subset. Therefore a subgroup \( H \) is normal in \( G \) precisely when \( G = N_G(H) \).

The group \( N_G(H) \) acts on \( H \) by conjugation, and the kernel of this action \( C_G(H) \) is the centralizer of \( H \) in \( G \):

\[
C_G(H) = \{ g \in G \mid gh = hg \text{ for all } h \in H \}.
\]

The normalizer of a subgroup \( H \) always contains \( H \) itself, but the centralizer of \( H \) can be very small even if \( H \) is large. In any event, \( C_G(H) \subseteq N_G(H) \).

If the set \( H \) contains the single element \( h \), then \( N_G(H) = C_G(h) \) (which we write in place of \( C_G(\{h\}) \)).

(2.6). Lemma. Let \( H \) be a subset of group \( G \). Then the number of distinct conjugates of \( H \) in \( G \) is \( [G:N_G(H)] \).

Proof. Let \( g_i \), for \( i \in I \) be a complete set of representatives for distinct cosets of \( N_G(H) \) in \( G \). Then for every \( g \in G \) there are unique \( n \in N \) and \( i \in I \) with \( g = ng_i \). Then \( H^g = H^{ng_i} = H_{g_i} \), so the \( H^{g_i} \) give all conjugates. On the other hand \( H^{g_i} = H^{g_j} \) gives \( g_i(g_j)^{-1} \in N_G(H) \), hence \( i = j \).

(2.7). Proposition. (The Class Equation) Let \( g_i \), for \( 1 \leq i \leq n \), be representatives for the conjugacy classes of noncentral elements in the finite group \( G \). Then

\[
|G| = |Z(G)| + \sum_{i=1}^{n} [G:C_G(g_i)].
\]

Proof. The group \( G \) is the disjoint union of its distinct conjugacy classes. A class contains one element if and only if it is in the center of \( G \); that is, the union of the classes of size 1 has cardinality \( |Z(G)| \). The noncentral class containing each \( g_i \) has cardinality \( [G:C_G(g_i)] \) by Lemma (2.6).

If \( A \) acts on \( G \) and \( H \) is a subset of \( G \) with \( H^a = H \) for all \( a \in A \) then \( H \) is \( A \)-invariant. (See Section 1.4.) For instance \( N \) is normal in \( G \) precisely when it is \( \text{Inn}(G) \)-invariant. The nonidentity group \( G \) is a simple group provided \( 1 \) and \( G \) are the only normal subgroups of \( G \), that is, the only \( \text{Inn}(G) \)-invariant subgroups of \( G \).

A subgroup of \( G \) is characteristic in \( G \) when it is \( \text{Aut}(G) \)-invariant. Clearly this is a stronger requirement than normality. A group \( G \) that is \( \text{Aut}(G) \)-simple is characteristicaly simple. That is, its only characteristic subgroups are \( 1 \) and \( G \) itself.

(2.8). Proposition.

(a) If \( P \) char \( Q \) char \( R \), then \( P \) char \( R \).

(b) If \( P \) char \( R \) and \( Q/P \) char \( R/P \), then \( Q \) char \( R \).
2.4. COMMUTATOR THEORY

(c) If $P \text{ char } Q \trianglelefteq R$, then $P \trianglelefteq R$. \hfill $\Box$

If $M$ and $N$ be subgroups of $G$ with $N \trianglelefteq M$, then the quotient group $M/N$ is called a section of $G$. Sections form the basis of an important group theoretical technique called internal representation theory.

(2.9). Lemma. Let $M$ and $N$ be $A$-invariant subgroups of $G$ with $N \trianglelefteq M$. (This happens, for instance, if $A \leq N_G(M)$ and $N$ char $M$.) Then $A$ acts on the section $M/N$ by $(Nm)^a = Nm^a$ for $m \in M$ and $a \in A$. \hfill $\Box$

2.4 Commutator theory

We have $gh = hg.g^{-1}h^{-1}gh$; so we define the commutator

$$[g, h] = g^{-1}h^{-1}gh$$

to gauge the extent to which $g$ and $h$ commute.\footnote{In places where left action is preferred to right action, the opposite notation $[g, h] = ghg^{-1}h^{-1}$ is often used.}

Obviously, they commute if and only if $[g, h] = 1$. We iterate by defining $[[g, h], k] = [g^{-1}h^{-1}gh, k]$. For $H, K \leq G$, we set $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle (= [K, H]$ by Lemma (2.11)(b)). Furthermore $[H, K, L] = [[[H, K], L] = \langle [H, K], L \rangle$.

(2.10). Lemma. If $\varphi$ is a homomorphism from $G$ to $M$ then $[x, y]^{\varphi} = [x^{\varphi}, y^{\varphi}]$. Thus if $I \leq H \leq G$ and $J \leq K \leq G$, then $[I, J] \leq [H, K]$ and $\varphi([H, K]) = [\varphi(H), \varphi(K)]$. In particular, if $H$ and $K$ are characteristic subgroups of $G$, then $[H, K]$ is also characteristic in $G$. \hfill $\Box$

(2.11). Lemma. Let $x, y, z \in G$.

(a) $[x, y] = [y, x]^{-1}$.
(b) $[x, y] = (y^{-1})^x y$; $[x, y] = x^{-1}x^y$.
(c) $[xy, z] = [x, z]^y[y, z]$; $[x, yz] = [x, z][x, y]^z$.
(d) $[x, y^{-1}, z]^y[y, z^{-1}, x]^y [z, x^{-1}, y]^z = 1$. \hfill $\Box$

(2.12). Corollary. Let $H, K \leq G$.

(a) $N_G(H) \geq K$ if and only if $H \geq [H, K]$.
(b) $[K, H] = [H, K] \trianglelefteq (H, K)$.
(c) $\langle H^G \rangle = H[H, G]$.

Proof. (a) We have $N_G(H) \geq K$ if and only if $h^k \in H$, for all $h \in H$ and $k \in K$. This happens precisely when, for all $h \in H$ and $k \in K$, we have (using Lemma (2.11)(b)) $h^{-1}h^k = [h, k] \in H$, which is the case if and only if $H \geq [H, K]$.
b) From Lemma (2.11) (a) we find $[K, H] = [H, K]$. For all $g, h \in H$ and $k \in K$, we have

$$[h, k]^g = [hg, k][g, k]^{-1} \in [H, K]$$

by Lemma (2.11) (e). Hence $H \leq N_G([H, K])$, and similarly for $K$.

(c) By (b) the subgroup $[H, G]$ is normal in $G$. In particular, $H[H, G]$ is a subgroup. As $h^g = h[h, g]$, we have

$$\langle H[G] \rangle \leq H[H, G] \leq \langle h, h^g | h \in H, g \in G \rangle = \langle H^G \rangle.$$  


Proof. By Lemma (2.11) (e), for all $x \in X, y \in Y, z \in Z$, we have

$$[x, y^{-1}, z][y, z^{-1}, x][z, x^{-1}, y]^z = 1.$$  

Since by hypothesis $[x, y^{-1}, z][y, z^{-1}, x][z, x^{-1}, y]^z = 1$, we have

$$[z, x^{-1}, y][z, x^{-1}, y]^z = 1,$$

for all appropriate $x, y, z$. That is, every $y \in Y$ commutes with all $[z, x^{-1}] \in [Z, X]$. As these constitute a generating set for $[Z, X]$, in fact $[Z, X, Y] = 1$, as desired.

The proof of the next corollary makes use of a very standard group theoretic practice: a bar convention. In these situations, the image $\varphi(H)$ of the homomorphism $\varphi$ from the group $H$ is denoted $\bar{H}$ (or $\tilde{H}$ or $\hat{H}$, and so forth); then for each subset $A$ of $H$, the subset $\varphi(A)$ of $\bar{H}$ is denoted $\bar{A}$ (respectively, $\tilde{A}$, $\hat{A}$).


Proof. We make use of the bar convention $\bar{G} = G/N$. By hypothesis, $[\bar{X}, \bar{Y}, \bar{Z}] = 1$ and $[\bar{Y}, \bar{Z}, \bar{X}] = 1$. Therefore by the Three Subgroups Lemma (2.13) we have $[\bar{Z}, \bar{X}, \bar{Y}] = 1$. That is, $[Z, X, Y] \leq N$.


Proof. We have, by assumption, $[X, Y, X] = [Y, X, X] = 1$; so from the Three Subgroups Lemma (2.13) we get $1 = [X, X, Y] = [[X, X], Y] = [X, Y] = [Y, X]$.

The subgroup $[G, G] = G'$ is the derived subgroup of $G$, a normal, indeed characteristic, subgroup of $G$ (see Lemma (2.10)).

(2.16). Theorem. If $N$ is normal in $G$ with $G/N$ abelian, then $N \geq G'$. Conversely if $N \geq G'$, then $N$ is normal in $G$ and $G/N$ is abelian.
2.5. EXTENSIONS

Proof. Let $\overline{G} = G/N$. Thus $\overline{G}$ is abelian if and only if $[\overline{g}, \overline{h}] = \overline{1}$ (for all $\overline{g}, \overline{h} \in \overline{G}$) if and only if $[g, h] \in N$ (for all $g, h \in G$) if and only if $G' \leq N$. In the abelian group $\overline{G} = G/G'$, the subgroup $\overline{N}$ is certainly normal; therefore $N$ is normal in $G$. □

(2.17). Proposition. If $G = \langle H^G \rangle$, then $G/G'$ is isomorphic to $H/G' \cap H$. In particular, $G/G'$ is a quotient of $H/H'$.

Proof. We have $G = \langle H^G \rangle = H[H, G]$ by Corollary (2.12). Thus $[H, G]$ is a normal subgroup of $G$ with $H' = [H, H] \leq [H, G] \leq [G, G] = G'$. By the Dedekind modular law we have $G' = (H \cap G')[H, G]$, so the result follows from the isomorphism theorems. □

A group $G$ with $G = G'$ is a perfect group. By the theorem, $G$ is perfect if and only if its only abelian quotient is 1. A group $G$ is quasisimple if it is perfect and $G/Z(G)$ is simple.

(2.18). Proposition. A simple group is either perfect or cyclic of prime order.

Proof. If $G$ is not perfect, then $G > G'$. For simple $G$, this forces $G' = 1$; so $G$ is abelian. Let $1 \neq g \in G$. Then $\langle g \rangle$ is normal in abelian $G = \langle g \rangle$. If $|g| = |G|$ was not prime then some $\langle g^e \rangle$ would be a nontrivial proper subgroup of $G$, also normal; so $G$ is cyclic of prime order. □

2.5 Extensions

An arbitrary group $G$ with $N \trianglelefteq G$ and $G/N \simeq H$ is an extension of $N$ by $H$. Returning to unique factorization, we investigate the extent to which knowledge of $N$ and $H$ determines $G$ in the extension

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

There are two basic issues:

(a) What is the action of $H$ on $N$; that is, the homomorphism $\varphi : H \longrightarrow \text{Aut}(N)$?

(b) Given an action of $H$ on $N$, what are the possible extension types $G$?

Here is an important observation: given any action of a group $H$ on a group $N$, there is always at least one solution $G$ to the extension problem described above.

Let $\varphi : H \longrightarrow \text{Aut}(N)$ be a homomorphism, and define on the set $H \times N$ the multiplication

$$(h_1, n_1)(h_2, n_2) = (h_1h_2, n_1^{\varphi(h_2)}n_2)$$

5a first bar convention
6a second bar convention
We write $H \ltimes_{\varphi} N$ for this set endowed with this multiplication. It is called the semidirect product of $N$ by $H$ or the split extension of $N$ by $H$.

**Theorem.**

(a) The semidirect product $M = H \ltimes_{\varphi} N$ is a group. The inverse of $(h, n)$ is $(h^{-1}, (n^{-1})_{\varphi(h^{-1})})$.

(b) $H_0 = \{(h, 1) \mid h \in H\}$ is a subgroup of $M$ isomorphic to $H$.

(c) $N_0 = \{(1, n) \mid n \in N\}$ is a normal subgroup of $M$ isomorphic to $N$.

(d) $H_0 \cap N_0 = 1$, $M = H_0 N_0$, and $M/N_0 \cong H_0$.

This is the “external” semidirect product. The corresponding “internal” semidirect product motivates the external definition.

**Corollary.** Let $G$ have subgroups $H$ and $N$ with $H \leq N_G(N)$ and $H \cap N = 1$. Then $\langle H, N \rangle = HN \cong H \ltimes_{\varphi} N$, where $\varphi : H \to \text{Aut}(N)$ is conjugation, given by $n^{\varphi(h)} = n^h = h^{-1}nh$.

**Proof.** $h_1n_1 \cdot h_2n_2 = h_1(h_2h_2^{-1})n_1h_2n_2 = h_1h_2n_1^h \cdot n_2$, \qed

Thus the semidirect product is a tool for realizing automorphisms of groups via inner automorphisms in larger groups. In it, the action of $H$ on $N$ is always given by conjugation. Generally if $A$ acts on $K$, then we often write $[a, x]$ for $xa^{-1}$ and $[x, a]$ for $x^{-1}xa$, since these are the natural commutators in the semidirect product $A \ltimes K$. Also when we write $[A, K]$ and $[K, A]$, the calculations are done within $A \ltimes K$.

As just done, we often drop the subscript and write

$$\langle H, N \rangle = HN \cong H \ltimes N$$

when the intended action is understood. Since $N$ is normal in $HN$, we have $HN = NH$. This suggests that we can also write internal semidirect products as $NH = N \rtimes H$. The multiplication is

$$n_1h_1 \cdot n_2h_2 = n_1n_2^{h_1^{-1}h_1}h_2.$$ 

This, in turn, suggests the definition for another external semidirect product: $N \ltimes_{\varphi} H$ is defined on the set $N \times H$ with multiplication given by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1n_2^{\varphi(h_1)^{-1}}, h_1h_2),$$

where, as before $\varphi : H \to \text{Aut}(N)$ is a homomorphism.

**Lemma.** The subgroup isomorphisms $(h, 1) \mapsto (1, h)$, for $h \in H$, and $(1, n) \mapsto (n, 1)$, for $n \in N$, extend to an isomorphism of $H \ltimes_{\varphi} N$ and $N \ltimes_{\varphi} H$. \qed
2.6 Solvable groups

Subnormality is the transitive extension of normality. The finite series
\[ G = G_0 \geq G_1 \geq \cdots \geq G_i \geq \cdots \geq G_n = 1 \]
is a finite subnormal series if each \( G_{i+1} \) is normal in \( G_i \). Similarly it is a normal series or characteristic series if all its members are normal and then characteristic in \( G \). A finite subnormal series is more frequently called finite series. (We refrain from defining general series.) A subgroup \( H \) is subnormal in \( G \) if it is a member of some subnormal series starting at \( G \). In that case we write \( H \leq G \) and \( G \triangleright H \). The defect of subnormal \( H \) is the length of the shortest subnormal series from \( G \) and finishing at \( H \). For instance \( G \) has defect 0 in \( G \) while any normal subgroup \( N \) has defect 1.

The group \( G \) is solvable if it has a finite subnormal series
\[ G = G_0 \geq G_1 \geq \cdots \geq G_i \geq \cdots \geq G_n = 1 \]
in which all the factors \( G_i/G_{i+1} \) are abelian. It is important that we not assume the series to be a composition series; an abelian group is always solvable, but only finite abelian groups have finite composition series.

Set \( G = G^{(0)} \) and, for \( i \geq 1 \),
\[ G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \]
Then \( \{ G^{(i)} \mid i \geq 0 \} \) is the derived series of \( G \). This is a characteristic series by Lemma (2.10). We set \( G^{(\infty)} = \bigcup_{i \geq 0} G^{(i)} \), a characteristic and perfect subgroup of \( G \).

We encountered \( G^{(1)} = [G, G] = G' \), the derived subgroup of \( G \) earlier. By Theorem (2.16) each factor \( G^{(i)}/G^{(i+1)} \) is abelian. Therefore, if \( G^{(n)} = 1 \), for some \( n \), then \( G \) is solvable. Indeed we see next that a group is solvable if and only if there is an \( n \) with \( G^{(n)} = 1 \).

(2.22). **Theorem.** Let \( G = G_0 \geq G_1 \geq \cdots \geq G_k \) with all factors \( G_{i-1}/G_i \) abelian. Then \( G_i \geq G^{(i)} \) for all \( i \).

**Proof.** The case \( k = 1 \) is contained in Theorem (2.16). The general case follows by induction. \( \square \)

(2.23). **Corollary.** \( G \) is solvable if and only if \( G^{(k)} = 1 \) for some \( k \). \( \square \)

Calculation of the derived series can thus be thought of as a “greedy algorithm” for verifying solvability. One consequence is that, if \( n \) is chosen minimal subject to \( G^{(n)} = 1 \), then any subnormal series testifying to the solvability of \( G \) must have length at least \( n \); and there is such a series of length exactly \( n \) (namely, the derived series). This \( n \) is called the derived length of the solvable group \( G \).

\(^7\)We are actually describing chains rather than series, but the terminology is standard.
(2.24). Theorem. 
(a) Subgroups and quotient groups of solvable groups are solvable.
(b) For \( N \leq G \), if \( N \) and \( G/N \) are solvable then \( G \) is solvable.
(c) If \( A \) and \( B \) are normal and solvable in \( G \), then \( AB \) is normal and solvable in \( G \).

Proof. If \( H \leq G \), then \( H^{(k)} \leq G^{(k)} \); so subgroups of solvable groups are solvable. Also, for any homomorphism, \( \varphi(G') = \varphi(G)' \) (by Lemma (2.10)); so quotients of solvable groups are solvable.

We can stick together series with abelian factors for \( G/N \) and \( N \) to produce one for \( G \). In particular this is possible when \( G = AB \) and \( N = A \).

(2.25). Corollary. If \( G \) is a finite group, then it has a unique maximal normal solvable subgroup.

Proof. By the last part of the theorem, in a finite group all normal solvable subgroups generate a solvable normal subgroup, clearly the largest.

The normal subgroup of the corollary is the solvable radical of \( G \) and is, in fact, characteristic in \( G \).

2.7 Nilpotent groups

Let \( L_0(G) = G \) and, for \( i \geq 1 \),

\[
L_i(G) = [L_{i-1}(G), G].
\]

By Lemma (2.10) this gives a characteristic series \( \{ L_i(G) \mid i \geq 0 \} \), which is called the lower central series for \( G \). By design each \( L_{i-1}(G)/L_i(G) \) is central in \( G/L_i(G) \), but again it is not certain that there is some \( n \) with \( L_n(G) = 1 \).

The lower central series is initially the same as the derived series. Indeed \( L_0(G) = G = G^{(0)} \) and \( L_1(G) = [G,G] = G^{(1)} \); but then they can diverge, since \( L_2(G) = [[G,G],G] \) will generically have \( G^{(2)} = [[G,G],[G,G]] \) as a proper subgroup.

Again, let \( Z_0(G) = 1 \), \( Z_1(G) = Z(G) \), and, for \( i \geq 1 \),

\[
Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G));
\]

that is, \( Z_{i+1}(G) \) is the preimage in \( G \) of the center of \( G/Z_i(G) \). The series \( \{ Z_i(G) \mid i \geq 0 \} \) is the upper central series for \( G \). By Proposition (2.8)(b) each \( Z_{i+1}(G) \) is characteristic in \( G \). In this case the subgroup 1 belongs to the series, but \( G \) might not.

(2.26). Theorem. Let \( G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq \cdots \supseteq G_n = 1 \) be a normal series in the group \( G \) with, for each \( i \geq 0 \),

\[
G_i/G_{i+1} \leq Z(G/G_{i+1}).
\]
2.7. NILPOTENT GROUPS

(a) $L_i(G) \leq G_i$, hence $L_n(G) = 1$.

(b) $Z_i(G) \geq G_{n-i}$, hence $Z_n(G) = G$.

**Proof.** (a) Induct on $i$, with the case $i = 0$ being clear. If $L_i(G) \leq G_i$ then

$$L_{i+1}(G) = [L_i(G), G] \leq [G_i, G] \leq G_{i+1}.$$  

(b) Induct on $i$, with the case $i = 0$ clear. Set $\bar{G} = G/Z(G)$. Then by the definition of the upper central series,

$$Z_i(\bar{G}) = \overline{Z_{i+1}(G)} = Z_{i+1}(G)/Z(G).$$

By the Third Isomorphism Theorem [2.5] we have $\bar{G}_i \leq \bar{G}$ with

$$\bar{G}_i/\bar{G}_{i+1} \leq Z(\bar{G}/\bar{G}_{i+1}).$$

In particular, $\bar{G}_{n-1} = 1$ as $G_{n-1} \leq Z(G)$. By induction $\bar{G}_{(n-1)-1} \leq Z_i(\bar{G})$. Taking preimages in $G$, we find $G_{n-(i+1)} \leq Z_{i+1}(G)$, as desired. □

A normal series as in the theorem is a central series for $G$. Thus $G$ has a central series if and only if its lower central series reaches 1 in a finite number $n$ of steps if and only if its upper central series reaches $G$ in a finite number $m$ of steps. In this case, the group $G$ is nilpotent. The theorem goes on to tell us that the smallest such $n$ and $m$ are equal. This number $n = m$ is the nilpotence class of the group $G$.

We next have a nilpotent counterpart to Theorem [2.24], although part (b) should really be viewed as the failure within nilpotent groups of a basic property of solvable groups: an extension of a solvable group by a solvable group by a solvable group is solvable, while a (noncentral) extension of a nilpotent group by a nilpotent group is rarely nilpotent, as Sym(3) and Alt(4) testify. This also means that extracting (c) from (b) is more complicated.

**Theorem.**

(a) Subgroups and quotient groups of nilpotent groups are nilpotent.

(b) For $N \trianglelefteq G$, if $N \leq Z(G)$ and $G/N$ is nilpotent then $G$ is nilpotent.

(c) If $A$ and $B$ are normal and nilpotent in $G$, then $AB$ is normal and nilpotent in $G$.

(d) Let $G$ be nilpotent and $1 \neq N \trianglelefteq G$. Then $Z(G) \cap N \neq 1$.

**Proof.** (a) By Lemma [2.10] always $L_i(H) \leq L_i(G)$ and $\varphi(L_i(G)) = L_i(\varphi(G))$.

(b) By (a) we may assume $N = Z(G)$. But then the preimage of the upper central series for $G/N$ is the upper central series for $G$.

(c) By induction on nilpotence class in $G/Z(G)$, we have $ABZ(G)/Z(G)$ nilpotent. Then by (b) the preimage $AGZ(G)$ is nilpotent as is its subgroup $AB$ (by (a)).
(d) Choose the smallest $i$ with $N \cap Z_i(G) \neq 1$. As $N$ is normal

$$[G, N \cap Z_i(G)] \leq N \cap Z_{i-1}(G) = 1,$$

and $1 \neq N \cap Z_i(G) \leq Z(G)$. \hfill \Box

We are used to doing induction in finite groups on order. Nilpotent groups allow induction on class even when infinite. Similarly solvable groups allow induction on derived length even when infinite.

**2.28. Proposition.** Let $G$ be a nilpotent group.

(a) $U < N_G(U)$ for all $U < G$.

(b) $U$ is subnormal in $G$ for all $U \leq G$.

(c) $[N, G] < N$ for all nonidentity normal $N$.

(d) $Z(G/N)$ is nontrivial for all proper normal $N$.

**Proof.** Part (d) follows from Theorem (2.27)(a).

(a) Choose the largest $i$ with $Z_i(G) \leq U$. Then

$$[U, Z_{i+1}(G)] \leq [Z_{i+1}(G), G] \leq Z_i(G) \leq U.$$ 

Thus $Z_{i+1}(G) \leq N_G(U)$ by Corollary (2.12), but $Z_{i+1}(G)$ is not in $U$.

(b) By our proof of (a), the subnormal series

$$U < N_G(U) < N_G(N_G(U)) < \cdots$$

reaches $G$ in a number of steps at most the nilpotence class of $G$.

(c) Choose the largest $i$ with $N \leq L_i(G)$. Then

$$[N, G] \leq [L_i(G), G] = L_{i+1}(G).$$

As $N$ is not contained in $L_{i+1}(G)$, we must have $[N, G] < N$. \hfill \Box

For finite groups $G$, each of these properties actually characterizes $G$ as being nilpotent. (See Problem (2.41)).

**2.29. Corollary.** If $G$ is a finite group, then it has a unique maximal normal nilpotent subgroup. \hfill \Box

This subgroup, called the *Fitting subgroup* of $G$, is then clearly characteristic in $G$.

### 2.8 Finite $p$-groups and Sylow’s First Theorem

Let $p$ be a prime. The finite group $G$ is a *$p$-group* if it has order a power of the prime $p$.\footnote{Sylow’s First Theorem and Lagrange’s Theorem imply that this is equivalent to requiring all elements to have order a power of $p$. This second version is a better definition in that it has content for infinite groups as well.}
2.9. DIRECT PRODUCTS AND SUMS

(2.30). Lemma. Let $G$ be a finite $p$-group. Then $G$ is nilpotent. Let $P \leq G$ with $|P| = p^a$ and $|G| = p^b$. Then for each integer $c$ with $a \leq c \leq b$ there is a subgroup $Q$ with $P \leq Q \leq G$ and $|Q| = p^c$.

Proof. Recall the Class Equation of Proposition (2.7):

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G:C_G(g_i)],$$

where the $g_i$ are representatives for the distinct conjugacy classes of noncentral elements in $G$. Each $[G:C_G(g_i)]$ is a multiple of $p$, as is $|G|$. Therefore $|Z(G)|$ is also a multiple of $p$, which is to say that $Z(G)$ is nontrivial. Therefore $P$ is nilpotent by Theorem (2.27) (b) and induction. The rest then follows by Proposition (2.28) (a) since, for proper $Q$, the $p$-group $N_G(Q)/Q$ has a nontrivial center. 

(2.31). Theorem. (Sylow’s First Theorem) If the finite group $G$ has order $|G| = p^a m$ with $p$ prime, $a \in \mathbb{N}$, and $\gcd(p,m) = 1$, then $G$ contains subgroups of order $p^a$ and index $m$.

Proof. Consider again the Class Equation or Proposition (2.7):

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G:C_G(g_i)].$$

If any of the indices $[G:C_G(g_i)]$ is not a multiple of $p$, then $C_G(g_i)$ is a proper subgroup of $G$ whose order is a multiple of $p^a$, and we are done by induction.

Thus we can assume that $\sum_{i=1}^{n} [G:C_G(g_i)]$ is a multiple of $p$, and hence (as in the previous lemma) $Z(G)$ has order a multiple of $p$. By the structure theory of finite abelian groups (see Theorem (1.4)) $Z(G)$ contains a subgroup $Z$ of order $p$. Now we are done by induction in $G/Z$. 

2.9 Direct products and sums

For any two groups $H$ and $N$ there is always the trivial map $\varphi: H \to \text{Aut}(N)$ that sends each element of $H$ to the trivial automorphism of $N$. In that case the semidirect product is actually the direct product

$$H \ltimes_{\varphi} N = H \times N.$$
In this case $[H, N] = 1$, and $N$ also acts trivially on the normal subgroup $H$:

$$H \times N \cong N \times H = N \times H.$$ 

Once we have defined the direct product of two groups, we immediately have the direct product of any finite set of groups via

$$H_1 \times H_2 \times H_3 = (H_1 \times H_2) \times H_3 \cong H_1 \times (H_2 \times H_3).$$

More generally, let $G_i, i \in I$, be a set of groups. The direct product of the $G_i$, written $\bigotimes_{i \in I} G_i$ is the group consisting of those sequences $(g_i)_{i \in I}$ with multiplication defined pointwise:

$$(g_i)_{i \in I}(h_i)_{i \in I} = (g_i h_i)_{i \in I}.$$ 

For $|I| = 2$, indeed for finite $I$, this is just the direct product defined above.

The direct product is sometimes referred to as the external direct product since it is a group constructed from the collection of groups $G_i$, initially external to the product. The next result produces a direct product from inside a group:

**Theorem. (Chinese Remainder Theorem)** Let $N_i$, for $i \in I$, be normal subgroups of the group $G$ with $G = \langle N_i \mid i \in I \rangle$, and set $G_i = G/N_i$. Then the map

$$g \mapsto (N_i g)_{i \in I}$$

is a homomorphism of $G$ into the direct product $\bigotimes_{i \in I} G_i$ with kernel $\bigcap_{i \in I} N_i$.

**Proof.** The map $g \mapsto (N_i g)_{i \in I}$ is certainly a homomorphism, since each of its projections $\pi_i: g \mapsto N_i g$ is the natural factor map $\pi_i: G \to G/N_i = G_i$. The kernel is then

$$\{ g \in G \mid N_i g = N_i, \text{ for all } i \in I \} = \bigcap_{i \in I} N_i. \quad \square$$

Indeed, more is true. For each $j$, the described coordinate projection $\pi_j: g \mapsto (N_i g)_{i \in I} \mapsto N_j g$ is onto $G_j$. In general, a subgroup of $H \leq \bigotimes_{i \in I} G_i$ for which each projection $\pi_i(H)$ is onto $G_i$, is a subdirect product of the $G_i$. An important example of a subdirect product is the the embedding of the group $G$ on the diagonal of $G \times G$ via $g \mapsto (g, g)$.

The Chinese Remainder Theorem reveals the direct product as the categorical product in $\text{Grp}$ relative to the various projections $\pi_i$. The categorical coproduct in $\text{Grp}$ is the free product. This shall not be of much direct interest to us, but it does have a quotient that is important.

For each $i$ we have the natural injection $\iota_i$ of $G_i$ into $\bigotimes_{i \in I} G_i$ that takes $g \in G_j$ to the $I$-tuple $(g_i)_{i \in I}$ with $g_j = g$ and $g_i = 1_{G_i}$ for $i \neq j$. The group $\bigoplus_{i \in I} G_i$ is the subgroup $\langle \iota_i(G_i) \mid i \in I \rangle$ of $\bigotimes_{i \in I} G_i$. This is then the normal subgroup of $\bigotimes_{i \in I} G_i$ consisting of those $(g_i)_{i \in I}$ with $g_i = 1_{G_i}$ for all but a finite
2.9. DIRECT PRODUCTS AND SUMS

number of $i$. In particular if $I$ is finite, then $\bigoplus_{i \in I} G_i = \bigotimes_{i \in I} G_i$, but if $I$ is infinite then the containment is proper.

The group $\bigoplus_{i \in I} G_i$ is a kind of coproduct in $\text{Grp}$ in that is the natural quotient of the coproduct subject to the additional relations

\[ [i_i(G_i), i_j(G_j)] = 1 \text{ for all } i \neq j. \]

In particular, in the category of abelian groups $\text{AbGrp}$ this is the coproduct. For this reason, we call $\bigoplus_{i \in I} G_i$ the direct sum of the $G_i$.

The reason we make these distinctions here is that, just as with the Chinese Remainder Theorem and direct products, there is a natural context in which we encounter direct sums.

(2.34). Theorem. If, in the group $G$, the subgroups $G_i$, for $i \in I$, normalize each other and, for all $i \in I$ satisfy

\[ G_i \cap \langle G_j \mid j \neq i \rangle = 1, \]

then the subgroup $\langle G_i \mid i \in I \rangle$ is isomorphic to the direct sum $\bigoplus_{i \in I} G_i$.

Proof. The isomorphism from $\bigoplus_{i \in I} G_i$ to $G$ is given by

\[ (g_i)_{i \in I} \mapsto \prod_{i \in I} g_i. \]

This is well-defined since all but a finite number of the $g_i$ are $1_G$ and for $i \neq j$ the elements $g_i$ and $g_j$ of $G$ commute.

This theorem explains why the direct sum is often called the internal direct product. There are various different terms for these two products, and that can be confusing. The (external) direct product is also the Cartesian product and the unrestricted direct product while the direct sum (internal direct product) is also the restricted direct product and sometimes, even, the direct product. We shall only refer to the direct sum as the direct product when $I$ is finite so they are equal, as in the next theorem.

(2.35). Theorem. A finite group is nilpotent if and only if it is the direct product of its Sylow subgroups.

Proof. A finite group that is the direct product of $p$-groups is nilpotent by Theorem [2.27] and Lemma [2.30].

Now let $G$ be finite and nilpotent. For each Sylow subgroup $P$, we have $N_G(N_G(P)) = N_G(P)$ by Lemma [2.32]. As $G$ is nilpotent, this forces $N_G(P) = P$ by Proposition [2.28](a). That is, every Sylow subgroup of $G$ is normal. Let $P_i$, for $1 \leq i \leq n$, be the (unique) Sylow $p_i$-subgroup (with $p_i \neq p_j$, for $i \neq j$). For each $i$ the subgroup $\langle P_j \mid j \neq i \rangle = \prod_{j \neq i} P_j$ has $p_i'$ order and so is disjoint from the $p_i$-group $P_i$. Therefore $G$ is the direct sum, hence product, of the $P_i$ by Theorem [2.34].
2.10 Problems

(2.36). Problem. Prove that the inverse map \( g \mapsto g^{-1} \) is an antiautomorphism of every group \( G \) that, for each subgroup \( H \) of \( G \), induces a bijection between the set of right cosets of \( H \) and the set of left cosets of \( H \).

(2.37). Problem. Let \((G,\cdot)\) be a group. Let \( a \in G \). Define, on the set \( G \), a new multiplication \( \circ \) by
\[
x \circ y = x \cdot a \cdot y.
\]
Prove that there is a bijection \( \varphi: G \rightarrow G \) with \( \varphi(g) \circ \varphi(h) = \varphi(g \cdot h) \) for all \( g, h \in G \).

What is the identity element of \((G,\circ)\)?

(2.38). Problem. (Reidermeister Quadrangle Condition) Let \( A \) be a Latin square with entries from the set \( X \). That is, \( A \) is an \( X \times X \) array in which every element of \( X \) occurs exactly once in each row and exactly once in each column.

Prove that the rows and columns of \( A \) can be relabeled to make it into the multiplication table of some group if and only if, for all \( a, b, c \in X \), whenever the pattern
\[
\begin{bmatrix}
\cdots & \cdots \\
\cdots & a & \cdots & b & \cdots \\
\cdots & \cdots \\
\cdots & c & \cdots & d & \cdots \\
\cdots & \cdots 
\end{bmatrix}
\]
occurs in rows \( i, j \) and columns \( m, n \) and
\[
\begin{bmatrix}
\cdots \\
\cdots \\
\cdots & a & \cdots & b & \cdots \\
\cdots \\
\cdots & c & \cdots & d' & \cdots \\
\cdots 
\end{bmatrix}
\]
is in rows \( i', j' \) and columns \( m', n' \), then \( d = d' \).

(Let \( C \) be the set all triples \((r, c, e)\in X^3\) for which \( e \) is the entry to be found in the cell of \( A \) at the intersection of row \( r \) and column \( c \). Then the hypothesis is: for all \( i, j, m, n, i', j', m', n' \in X \),
\[
(i, m, a), (i, n, b), (j, m, c), (j, n, d), (i', m', a), (i', n', b), (j', m', c), (j', n', d') \in C
\]
is in \( C \).)

implies \( d = d' \).

(2.39). Problem. Let \( B \trianglelefteq G \). Prove that \( Bx B . y B \supseteq Bx y B \), for all \( x, y \in G \), and that equality always holds if and only if \( B \) is normal in \( G \).

(2.40). Problem.
(a) Prove that if \( G \) is solvable then \( U' \subset U \) for all \( 1 \neq U \leq G \).
(b) Let \( G \) be finite. Prove that \( G \) is solvable if and only if \( U' \subset U \) for all \( 1 \neq U \leq G \).

(2.41). Problem. Let \( G \) be a finite group with any one of the following properties:
2.10. PROBLEMS

(a) \( U < N_G(U) \) for all \( U < G \).
(b) \( U \) is subnormal in \( G \) for all \( U \leq G \).
(c) \([N,G] < N\) for all nonidentity normal \( N \).
(d) \( Z(G/N) \) is nontrivial for all proper normal \( N \).

Prove that \( G \) is nilpotent. (That is, for finite groups each of the properties of Proposition (2.28) characterizes nilpotent groups. This is false for each when we include infinite groups.)

(2.42). Problem. Prove that in arbitrary \( G \) we have \( L_i(G) \geq G^{(i)} \) for all \( i \geq 0 \).

(2.43). Problem. Let \( P \) be nilpotent of class at most 2. (That is, \( P' \leq Z(P) \)). Set \( \bar{P} = P/Z(P) \). Prove
(a) \([a,b][a,c] = [a,bc] \).
(b) \([a,c][b,c] = [ab,c] \).
(c) \( a^k b^k = (ab)^{(k^2)} \).
(d) The map \( f(x,y) = [x,y] \) is a well-defined biadditive map from the abelian group \( \bar{P} \) into the abelian group \( Z(P) \).
(e) If \( \bar{P} \) and \( Z(P) \) are elementary abelian \( p \)-groups, then the map \( q(x) = x^p \) is a well-defined map from the \( \mathbb{Z}_p \)-space \( \bar{P} \) to the \( \mathbb{Z}_p \)-space \( Z(P) \) that is linear for \( p \) odd and for \( p = 2 \) satisfies \( f(x,y) = q(x+y) + q(x) + q(y) \).

(2.44). Problem. Prove that in a finite group, any subnormal nilpotent subgroup is contained in the Fitting subgroup.

(2.45). Problem. Let \( G \) contain the normal abelian subgroups \( N_i \) for \( 1 \leq i \leq n \). Set \( N = \langle N_i | 1 \leq i \leq n \rangle \), which is nilpotent by Theorem (2.27)(c). Prove that \( N \) has nilpotence class at most \( n \).

(2.46). Problem.
(a) Let \( G = \bigoplus_{i \in I} G_i \) be the direct sum of the nonabelian simple groups \( G_i \). Show that \( H \) is subnormal in \( G \) if and only if \( H = \bigoplus_{j \in J} G_j \), for some subset \( J \) of \( I \).
Remark. This result is not true if two of the simple groups \( G_i \) are abelian and isomorphic.

(b) Prove that direct sum of isomorphic simple groups is characteristically simple.
Groups are often encountered as permutation groups or linear groups. These are often the right places to look for factorization (reduction) methods.

### 3.1 Permutation groups

#### 3.1.1 Basics

Recall that for the set Ω, the symmetric group $\text{Sym}(\Omega)$ is the group $\text{Aut}_{\text{Set}}(\Omega)$ of all bijections of $\Omega$ with itself. For finite $|\Omega| = n$, the group $\text{Sym}(\Omega)$ is isomorphic to $\text{Sym}({1, 2, \ldots, n})$, which we usually write as $\text{Sym}(n)$.

(3.1). **Lemma.** For $n$ a positive integer, $|\text{Sym}(n)| = n!$.

If $\varphi: G \longrightarrow \text{Sym}(\Omega)$ is a permutation representation (that is, a $\text{Set}$-representation), then we say that $\Omega$ is a $G$-space. We write $\ker_G(\Omega)$ for the kernel of the representation $\varphi$, and the representation $\varphi$ is *faithful* if its kernel is trivial. If $G \leq \text{Sym}(\Omega)$ then we say that $(G, \Omega)$ is a permutation group. We also abuse this terminology by extending it to include faithful permutation representations $\varphi: G \longrightarrow \text{Sym}(\Omega)$.

If $f$ is a bijection (that is, a $\text{Set}$-isomorphism) of the two sets $\Omega$ and $\Delta$, then we have the induced isomorphism $f^*$ of $\text{Sym}(\Omega) = \text{Aut}_{\text{Set}}(\Omega)$ and $\text{Sym}(\Delta) = \text{Aut}_{\text{Set}}(\Delta)$, as in Section 1.4.

$$
\begin{array}{c}
\Omega \\ f \downarrow \\
\Delta
\end{array}
\longrightarrow
\begin{array}{c}
\Omega \\ f \downarrow \\
\Delta
\end{array}
\quad
\begin{array}{c}
a \mapsto \quad a \\ a^* \mapsto \quad a^*
\end{array}
$$

with $a \mapsto a^{f^*} = a^* = f^{-1}af$.
For the permutation representation \( \rho_\Omega : G \to \text{Sym}(\Omega) \) this provides us with the equivalent representation \( \rho_\Delta : G \to \text{Sym}(\Delta) \) given by \( \rho_\Delta = \rho_\Omega f^* \):

\[
\begin{array}{ccc}
  G & \xrightarrow{\rho_\Omega} & \text{Sym}(\Omega) \\
  \searrow & & \downarrow f^* \\
  \rho_\Delta & & \text{Sym}(\Delta)
\end{array}
\]

In this case, \( \Omega \) and \( \Delta \) are said to be isomorphic \( G \)-spaces. If further \( (G, \Omega) \) and \( (H, \Delta) \) are permutation groups, and there is a group isomorphism \( \varphi : G \to H \) for which the following diagram commutes:

\[
\begin{array}{ccc}
  G & \xrightarrow{\rho_\Omega} & \text{Sym}(\Omega) \\
  \varphi \downarrow & & \downarrow f^* \\
  H & \xrightarrow{\rho_\Delta} & \text{Sym}(\Delta)
\end{array}
\]

then the semiequivalence \( (\varphi, f) \) is a permutation isomorphism of \( (G, \Omega) \) and \( (H, \Delta) \).

Permutation representations are important for at least two reasons. They are relatively easy to work with and calculate in, and every group has a faithful representation as a permutation group. We have discussed \( G \) acting on itself by conjugation, but a more elementary action exists.

**Theorem. (Cayley’s Theorem)** Every group \( G \) is faithfully represented in \( \text{Sym}(G) \) via right translation:

\[
g \mapsto \rho(g) \quad \text{where} \quad x^{\rho(g)} = xg \quad \text{for} \quad x \in G.
\]

**Proof.** We have

\[
(x^{\rho(g)})^{\rho(h)} = (xg)h = x(gh) = x^{\rho(gh)}.
\]

The action is faithful since \( 1^{\rho(g)} = g \) implies that \( \rho(g) \) is nontrivial when \( g \) is not the identity.

The associated representation \( \rho : G \to \text{Sym}(G) \) is called the right regular representation.

**3.1.2 Transitivity**

For \( \omega \) in the \( G \)-space \( \Omega \), we set

\[
\omega^G = \{ \omega^g \mid g \in G \},
\]

the orbit (or \( G \)-orbit) of \( \omega \) for this action. If the only orbit is \( \Omega \), then we say that \( G \) is transitive on \( \Omega \). Otherwise \( G \) is intransitive.

In most situations, questions about permutation groups can be reduced to questions about transitive permutation groups.
(3.3). Proposition. If $G$ is a permutation group on $\Omega$ with orbits $\Omega_i$, for $i \in I$, then $G$ is isomorphic to a subdirect product of the groups $G_i = G/\text{ker}_G(\Omega_i)$, each acting faithfully and transitively on $\Omega_i$.

Proof. This follows from the Chinese Remainder Theorem \[2.33\] □

The subgroup

$$G_\omega = \{ g \in G \mid \omega^g = \omega \},$$

is the stabilizer of $\omega$ in $G$. We sometimes also use the notation $\text{Stab}_G(\omega)$.

If $\Delta$ is a subset of $\Omega$, then

$$G_\Delta = \text{Stab}_G(\Delta) = \{ g \in G \mid \Delta^g = \Delta \},$$

the global stabilizer of $\Delta$, while

$$G_{[\Delta]} = \bigcap_{\delta \in \Delta} G_\delta = \{ g \in G \mid \delta^g = \delta, \text{ all } \delta \in \Delta \}$$

is the pointwise stabilizer of $\Delta$. It probably would be better to denote (as some do) the global stabilizer of $\Delta$ by $N_G(\Delta)$ and the pointwise stabilizer by $C_G(\Delta)$.

A permutation representation $\varphi : G \to \text{Sym}(\Omega)$ is semiregular if $G_\omega = 1$, for all $\omega \in \Omega$. (In particular, it is faithful.) It is regular if it is semiregular and transitive (as in the right regular representation).

Just as factor groups give us canonical models for homomorphic images, so coset spaces give us canonical models for transitive permutation spaces.

For $H \leq G$, consider the coset space $H \backslash G = \{ Hx \mid x \in G \}$ which is naturally a $G$-space under the action of right translation:

$$\rho_H : G \to \text{Sym}(H \backslash G) \text{ given by } (Hx)^{\rho_H(g)} = Hxg,$$

so that

$$((Hx)^{\rho_H(g)})^{\rho_H(k)} = (Hxg)^k = Hx(gk) = Hx^{\rho_H(gk)}.$$

Of course, the right regular representation is $\rho_1_G$.

(3.4). Theorem. Let $G$ be transitive on $\Omega$. For a fixed $\omega \in \Omega$, set $H = G_\omega$ and $H \backslash G = \{ Hg \mid g \in G \}$. Then the set $\Omega$ and the coset space $H \backslash G$ are isomorphic as $G$-spaces. In particular $|\omega^G| = [G:G_\omega]$.

Proof. For $hx$ in the coset $Hx$ we have $\omega^{hx} = (\omega^h)^x = \omega^x$. Conversely, if $\omega^x = \omega^y$, then $yx^{-1} \in H$ and $Hx = H(yx^{-1})x = Hy$. Therefore the map $f: \Omega \to H \backslash G$ given by

$$\alpha \xrightarrow{L} Hx \iff \alpha = \omega^x$$

\[\text{This can be viewed as the set of $H$-orbits for in the left regular representation of $G$; see Problem } 3.24\]
is a well-defined bijection. If \( g \) is in \( G \) then \( \alpha^g = (\omega^x)^g = \omega^{xg} \), so we have the commutative diagram

\[
\begin{array}{ccc}
\alpha & \xrightarrow{g^*} & \alpha^g \\
f \downarrow & & \downarrow f \\
Hx & \xrightarrow{\rho_H^*} & Hxg
\end{array}
\]

That is, \( \rho_H = \rho_{\alpha f^*} \); and the two \( G \)-spaces are isomorphic, as claimed.

As \( G \) is transitive on \( \Omega \),

\[
|\omega^G| = |\Omega| = |H\backslash G| = |G:\Omega|.
\]

\textbf{(3.5). Lemma.} If \( \alpha^h = \beta \), then \((\alpha^g)^{h^g} = \beta^g\).

\textbf{Proof.} \((\alpha^g)^{h^g} = (\alpha^g)^{g^{-1}h^g} = (\alpha^h)^g = \beta^g\). That is, the diagram

\[
\begin{array}{ccc}
\alpha & \xrightarrow{h} & \beta \\
g \downarrow & & \downarrow g \\
\alpha^g & \xrightarrow{h^g} & \beta^g
\end{array}
\]

commutes. \( \square \)

So if \( h \) has cycle representation

\[ h = \ldots (\ldots, \alpha, \beta, \ldots) \ldots \]

then \( h^g \) has cycle representation

\[ h^g = \ldots (\ldots, \alpha^g, \beta^g, \ldots) \ldots \]

The permutation \( h \in \text{Sym}(\Omega) \) has cycle type \( 1^{a_1} 2^{a_2} \ldots i^{a_i} \ldots \), where \( a_i \) is the number of orbits of length \( i \) that \( h \) has in \( \Omega \). Those terms with \( a_i = 0 \) are always deleted. The term \( 1^{a_1} \) is also usually deleted as well (although for infinite \( \Omega \) this can cause confusion).

The lemma tells us that conjugacy in \( \text{Sym}(\Omega) \) preserves cycle type. Indeed, two elements of \( \text{Sym}(\Omega) \) are conjugate if and only if they have the same cycle type.

\textbf{(3.6). Corollary.} If \( \Omega \) is a \( G \)-space and \( \omega \in \Omega \), then \((G_\omega)^g = G_{\omega^g}\) for all \( g \in G \). \( \square \)

If \( H \) is a subgroup of \( G \), then the core \( \ker_G(H) \) of \( H \) in \( G \) is the largest normal subgroup of \( G \) contained in \( H \).

\textbf{(3.7). Corollary.} If \( \Omega \) is a transitive \( G \)-space and \( \omega \in \Omega \), then the core of \( G_\omega \) is \( \ker_G(\Omega) \). \( \square \)

\textbf{(3.8). Lemma. (A Frattini argument)} Let \( G \) be transitive on \( \Omega \) and \( \omega \in \Omega \). For \( N \subseteq G \), we have \( \omega^N = \Omega \) if and only if \( G = G_\omega N \).
3.1. PERMUTATION GROUPS

Proof. Assume $\omega^N = \Omega$. For $g \in G$, we have $\omega^g = \alpha = \omega^n$, for some $n \in N$. Therefore $gn^{-1} \in G_\omega$, and $g = (gn^{-1})n \in G_\omega N$. Conversely, if $G = G_\omega N$, then for any $\alpha \in \Omega$, there is a $g \in G$ with $\omega^g = \alpha$. Then $g = g_1n_1$, for $g \in G_\omega$ and $n_1 \in N$, so that $\omega^{n_1} = \omega^{g_1n_1} = \omega^g = \alpha$. Hence $\omega^N = \Omega$.

If $\Omega$ is a $G$-space, then so is each $\Omega^k$, with action in each coordinate. We are particularly interested in the case $k = 2$.

Any subset of $\Omega^2$ is a relation and any union of orbits of $G$ on $\Omega^2$ is an invariant relation. An orbit of $G$ on $\Omega^2$ is an orbital of $G$. We may think of an invariant relation as a directed graph whose automorphism group contains $G$. We may even think of it as an edge-colored graph, with the edges from orbital $O_i$ colored with $i$.

To each orbital $O$, there is associated a paired orbital $O^\uparrow$ given by

$$(a, b) \in O \iff (b, a) \in O^\uparrow.$$  

Every $G$-invariant relation $\Gamma$ has an underlying $G$-invariant undirected graph $\Gamma \cup \Gamma^\uparrow$, and any $G$-invariant relation $\Gamma = \Gamma^\uparrow$ is naturally an undirected graph.

The rank of transitive $G$ on $\Omega$ is the number of $G$-orbits on $\Omega^2$. The diagonal

$$\Delta = \{ (\alpha, \alpha) \mid \alpha \in \Omega \}$$

is always an orbital, so $G$ has rank 1 on $\Omega$ if and only if $|\Omega| = 1$. The transitive group $(G, \Omega)$ has rank 2 precisely when $|\Omega| > 1$ and $G$ is transitive on

$$\Omega^2 \setminus \Delta = \left[ \begin{array}{c} \Omega \\ 2 \end{array} \right].$$

That is, for all pairs $\alpha \neq \beta$ and $\alpha' \neq \beta'$ from $\Omega$, there is a $g \in G$ with $\alpha.g = \alpha'$ and $\beta.g = \beta'$. In this case $G$ is said to be 2-transitive or doubly transitive on $\Omega$.

3.9. Proposition.

(a) If $G$ is transitive on $\Omega$ then the rank of $G$ on $\Omega$ is the number of orbits of $G_\omega$ on $\Omega$.

(b) If $G$ is transitive on $\Omega$ then the rank of $G$ on $\Omega$ is the number of $H \setminus H$ cosets in $H \setminus G$.

Proof. By Theorem [3.4] these are equivalent.

For (a), let $\Sigma$ be an orbit of of $G_\omega$ in $\Omega$. Then there is a unique orbital $O$ with

$$O \cap \{ (\alpha, \omega) \mid \alpha \in \Omega \} = \{ (\alpha, \omega) \mid \alpha \in \Sigma \}.$$  

This gives a bijection between orbitals and orbits of $G_\omega$.

3.10. Corollary. $G$ is 2-transitive on $\Omega$ if and only if $G$ is transitive on $\Omega$ and $G_\omega$ is transitive on $\Omega \setminus \omega$.  

More generally, \( G \leq \text{Sym}(\Omega) \) is said to be \( k \)-transitive on \( \Omega \) if it is transitive on \( \binom{\Omega}{k} \). If \( G \) is \( k \)-transitive on \( \Omega \), then it is also \( k' \)-transitive, for all \( k' \leq k \).

Additionally, \( G \) is \( k \)-homogeneous on \( \Omega \) if it is transitive on \( \binom{\Omega}{k} \). Of course \( k \)-transitivity implies \( k \)-homogeneity, but the converse is far from true. Indeed, for \( |\Omega| = k \) finite, the only \( k \)-transitive subgroup of \( \text{Sym}(\Omega) \) is \( \text{Sym}(\Omega) \) itself, while every subgroup of \( \text{Sym}(\Omega) \) is \( k \)-homogeneous. In particular, an arbitrary \( G \) that is \( k \)-homogeneous may not be \((k-1)\)-homogeneous.

### 3.1.3 Primitivity

In the last section we discussed \( G \)-invariant relations—graphs. Now we specialize to the case of \( G \)-invariant equivalence relations, where the corresponding graphs are disjoint unions of complete graphs.

There are three obvious invariant equivalence relations \( \sim \) on \( \Omega \):

1. \( \alpha \sim \omega \) for all \( \alpha, \omega \in \Omega \), with the single equivalence class \( \Omega \);
2. \( \alpha \sim \omega \) if and only if \( \alpha = \omega \), with \( |\Omega| \) equivalence classes, all of size 1;
3. \( \alpha \sim \omega \) if and only if there is a \( g \in G \) with \( \alpha g = \omega \), with equivalence classes the orbits of \( \Omega \).

The first two are the trivial equivalence relations.

We say that \( G \) is primitive in its action on \( \Omega \) if the only invariant equivalence relations are the trivial ones. If \( G \) is primitive on \( \Omega \), then either \( G \) is transitive on \( \Omega \) or \( G \) is trivial on \( \Omega \) of size 2. Therefore one usually requires of primitive groups that they be transitive.

If \( G \) is transitive on \( \Omega \) but not primitive, then it is imprimitive. A block of imprimitivity for \( G \) acting on \( \Omega \) is an equivalence class for some nontrivial invariant equivalence relations.

#### (3.11). Theorem

If \( G \) is \( 2 \)-transitive on \( \Omega \), then \( G \) is primitive on \( \Omega \).

**Proof.** Suppose \( \Sigma \) is a block with \( \alpha, \beta \in \Sigma \) with \( \alpha \neq \beta \). For every \( \gamma \neq \alpha \) there is a \( g \in G_\alpha \) with \( \beta^g = \gamma \). Then

\[
\gamma \in \{\alpha, \gamma\} = \{\alpha, \beta\}_g \subseteq \Sigma^g = \Sigma,
\]

as \( \alpha \in \Sigma \cap \Sigma^g \). Therefore \( \Sigma = \Omega \) and \( G \) is primitive. \( \square \)

#### (3.12). Proposition

Let \( G \) be transitive on \( \Omega \) with \( \omega \in \Omega \).

(a) \( G \) is primitive on \( \Omega \) if and only if \( G_\omega \) is maximal in \( G \).

(b) The map \( N \rightarrow \omega^N \) gives an isomorphism of the lattice of subgroups \( N \) of \( G \) with \( G_\omega \leq N \leq G \) with the lattice of blocks of imprimitivity from \( \omega \) upto \( \Omega \).

**Proof.** (b) The bijection is given by

\[
N \rightarrow \omega^N \text{ and its inverse } \Delta \rightarrow \text{Stab}_G(\Delta).
\]
3.1. PERMUTATION GROUPS

Let \( G_\omega \leq N \leq G \), and set \( \Delta = \omega^N \). If \( \beta \in \Delta \cap \Delta^g \) then there are \( n_1, n_2 \in N \) with \( \omega^{n_1} = \beta = (\omega^{n_2})^g \). Therefore \( \omega^{n_2g^{-1}}n_1^{-1} = \omega \) and \( n_2g^{-1}n_1^{-1} \in G_\omega \leq N \). Thus \( g \in N \) and \( \Delta^g = (\omega^N)^g = \alpha^N = \Delta \). That is, \( \Delta \) is a block of imprimitivity. Furthermore, as \( N \) is transitive on \( \Delta \) we have \( \text{Stab}_N(G) = G_\omega N = N \) by the Frattini argument of Lemma (3.8).

Let \( \omega \in \Delta \), a block of imprimitivity for \( G \) on \( \Omega \). For each \( \beta \in \Delta \) there is a \( g \in G \) with \( \omega^g = \beta \) as \( G \) is transitive. Then \( \beta \in \Delta \cap \Delta^g \), so \( \Delta = \Delta^g \) and \( g \in N = \text{Stab}_G(\Delta) \) with \( \Delta = \omega^N \).

(a) The subgroup \( G_\alpha \) is maximal in \( G \) if and only if there are no subgroups in between \( G_\alpha \) and \( G \) if and only if there are no blocks in between \( \alpha \) and \( \Omega \) if and only if \( G \) is primitive on \( \Omega \).

(3.13). PROPOSITION. Let \( G \) be transitive on \( \Omega \) and \( N \) a normal subgroup of \( G \). The \( N \)-orbits in \( \Omega \) are blocks of imprimitivity for \( G \), and \( G/N \) is transitive on the set of these blocks.

Proof. We have \( G_\alpha \leq G N \leq G \) and \( G_{\alpha N} = N \) as discussed in Section 2.8, so this follows from the previous proposition.

In a sense, every block of imprimitivity arises in this manner. The block set for an imprimitive group is an equipartition of \( \Omega \), a partition into parts of equal size. The global stabilizer in \( \text{Sym}(\Omega) \) of this equipartition then contains \( G \) and has these blocks as its orbits under a normal subgroup.

(3.14). COROLLARY. If \( G \) is primitive on \( \Omega \) and \( N \) is normal in \( G \) then \( N \) is either trivial or transitive on \( \Omega \).

(3.15). LEMMA. (Brey-Iwasawa-Wilson Lemma) Let \( G \) be primitive on \( \Omega \) and \( A \leq G_\omega \) with \( \langle A^G \rangle = G \). For \( N \leq G \), either \( N \) is trivial on \( \Omega \) or \( G/N \simeq A/A \cap N \).

Proof. Assume that \( N \) is not trivial on \( \Omega \). Thus normal \( N \) is not in the core of the maximal subgroup \( G_\omega \), and \( G = G_\omega N = N G(A)N \). In particular \( A^G = A^N \) and \( G = \langle A^G \rangle = \langle A^N \rangle = AN \). But then \( G/N = AN/N \simeq A/A \cap N \), as claimed.

(3.16). LEMMA. (Iwasawa’s Lemma) Let the perfect group \( G \) be primitive on \( \Omega \) and abelian \( A \leq G_\omega \) with \( \langle A^G \rangle = G \). For \( N \leq G \), either \( N \) is trivial on \( \Omega \) or \( G = N \).

Proof. As \( A \) is abelian, its quotient \( A/A \cap N \) is also abelian. But \( G \) is perfect; so by the previous lemma if \( N \) is not in the kernel, then \( G/N \simeq A/A \cap N \) is trivial.

3.1.4 Sylow’s Theorems

Assume that the finite group \( G \) has order \( |G| = p^a m \) with \( p \) prime and \( \gcd(p, m) = 1 \). Then, as discussed in Section 2.8, a subgroup of order \( p^a \) is a Sylow \( p \)-subgroup. Two of Sylow’s three theorems are really results about permutation
groups. We emphasize that by proving them first here without reference to Sylow’s First Theorem.

(3.17). Theorem.

(a) (Sylow’s Second Theorem) Any two Sylow $p$-subgroups of the finite group $G$ are conjugate.

(b) (Sylow’s Third Theorem) Assume that the finite group $G$ contains a nontrivial Sylow $p$-subgroup. Then for any $p$-subgroup $Q$ of $G$ the number of Sylow $p$-subgroups containing $Q$ is congruent to 1 modulo $p$. In particular, the number of Sylow $p$-subgroups is congruent to 1 modulo $p$, and every $p$-subgroup is in at least one Sylow $p$-subgroup.

Proof. Of course, if there are no Sylow $p$-subgroups, then the Second Sylow Theorem is true trivially. Now assume that $P$ is a Sylow $p$-subgroup. Let $\Omega = \{ P^g \mid g \in G \}$, the set of conjugates of $P$ in $G$ and clearly a transitive $G$-space under conjugation.

For any $p$-subgroup $Q$ of $G$

$$ G_P \cap Q = N_Q(P) \leq P, $$

as the Sylow $p$-subgroup $P$ is contained in hence equal to the $p$-group $PN_Q(P)$. In particular, $P$ is the only Sylow $p$-subgroup normalized by $P$. Therefore in its action on $\Omega$, the $P$-orbits all have length a multiple of $p$ except for the single orbit $\{P\}$. In particular $|\Omega|$ is congruent to 1 modulo $p$. This in turn implies that for any $p$-subgroup $Q$, its number of orbits of length 1 in $|\Omega|$ is congruent to 1 modulo $p$.

If we apply the last argument to any Sylow $p$-subgroup $Q$, we learn that there is a conjugate $P^g$ that contains $Q$. That is, $Q = P^g$ for some $g \in G$. This is the Second Sylow Theorem. Thus $\Omega$ consists of all Sylow $p$-subgroups, and the previous arguments give the Third Sylow Theorem. \hfill $\square$

(3.18). Corollary. (The Frattini Argument) Let $p$ be a prime. If $N$ is normal in the finite group $G$, then $G = N_G(P)N$, where $P$ is a Sylow $p$-subgroup of $N$.

Proof. Set $\Omega = \{\text{Sylow } p\text{-subgroups of } N\}$, on which $G$ acts by conjugation. Then $N$ is transitive on $\Omega$ by Sylow’s Second Theorem and the point stabilizer is $G_P = N_G(P)$. Therefore this follows from our general Frattini Argument, Lemma (3.8). \hfill $\square$

We proved Sylow’s First Theorem as Theorem (2.31). We now give a more permutation theoretic proof due to Wielandt.

(3.19). Theorem. (Sylow’s First Theorem) If the finite group $G$ has order $|G| = p^am$ with $p$ prime, $a \in \mathbb{N}$, and $\gcd(p, m) = 1$, then $G$ contains subgroups of order $p^a$ and index $m$.

\footnote{Of course, the Class Equation used in the earlier proof is really a permutation argument. In the action of $G$ on itself by conjugation, the conjugacy classes are the orbits and the length of each orbit is given by Theorem (3.4).}
Proof. Consider \( \Omega = \binom{G}{p^a} \), the set of all subsets of \( G \) having cardinality \( p^a \). This is a \( G \)-space via right translation.

Let \( \Delta \) be a \( G \)-orbit in \( \Omega \) and \( D \in \Delta \), a \( p^a \)-subset of \( G \). For every \( g \in G \), there is at least one \( h \in G \) with \( g \in Dh \in \Delta \). Therefore the length \( |\Delta| \) of the orbit must be at least \( |G|/p^a = m \) (and with equality, every \( g \) is in exactly one \( Dh \)).

Assume for the moment that \( \Delta \) is one of these short orbits. Then \( |\text{Stab}_G(D)| = |G|/|\Delta| = p^a \); the stabilizer is a Sylow \( p \)-subgroup \( P \). We can further assume that \( D \) was chosen to contain \( 1_G \), so \( P \subseteq DP = D \) as \( P \) stabilizes \( D \). This forces \( P = D \), and \( \Delta = \{ Ph \mid h \in G \} \) is the coset space \( P \backslash G \). We conclude that each Sylow \( p \)-subgroup \( P_i \) contributes to \( \Omega \) exactly one orbit of length \( m \), namely \( P_i \backslash G \).

Every orbit not of length \( m \) has greater length, so its stabilizer cannot have order a multiple of \( p^a \). In particular, the orbit length is a multiple of \( p \). We conclude that

\[
|\Omega| = km + pn,
\]

where \( k \) is the number of distinct Sylow \( p \)-subgroups in \( G \) and \( n \) is some integer. If we can prove that \(|\Omega|\) is not a multiple of \( p \), then \( k \) cannot be zero. In that case, there is at least one Sylow \( p \)-subgroup and our proof of the First Sylow Theorem will be done.

The trick here is that the needed calculation regarding \(|\Omega|\) does not really depend on the group \( G \) but only on its order. If we replace \( G \) by any other group \( G_0 \) of the same order, then we have

\[
|\Omega| = |\Omega_0| = km + pn_0
\]

where \( k_0 \) is the number of distinct Sylow \( p \)-subgroups in \( G_0 \). With a careful choice of \( G_0 \), this calculation may be easier to make than the earlier one. And that is indeed the case: let \( G_0 \) be the cyclic group \( \mathbb{Z}_{|G|} \). Then \( G_0 \) has a unique Sylow \( p \)-subgroup. Thus \( k_0 = 1 \), and

\[
|\Omega| = |\Omega_0| = m + pn_0.
\]

This is not a multiple of \( p \) as \( m \) is not, and we are done!

\( \square \)

### 3.1.5 Problems

(3.20). Problem. For the permutation group \((G, \Omega)\), prove that the following are equivalent:

1. \((G, \Omega)\) is transitive and \( G_\gamma = 1 \), for some \( \gamma \in \Omega \).
2. \((G, \Omega)\) is permutation isomorphic to the right regular representation.
3. For all \( \alpha, \beta \in \Omega \) there is a unique \( g \in G \) with \( \alpha^g = \beta \).

(3.21). Problem. Prove that a transitive, faithful permutation representation of an abelian group is regular.

(3.22). Problem. Prove:
A subgroup of a semiregular group is itself semiregular.
Each orbit of a semiregular permutation representation of $G$ is isomorphic to the right regular representation $\rho$.

If $H$ is finite and semiregular on $\Omega_1$ and $\Omega_2$ with $|\Omega_1| = |\Omega_2|$, then $\Omega_1$ and $\Omega_2$ are isomorphic $H$-spaces.

(3.23). Problem. Suppose $H_1, H_2 \leq G$ with finite $H_1 \cong H_2$. Then for the right regular representation of $G$, $\rho: G \rightarrow \text{Sym}(G)$, there is an $s \in \text{Sym}(G)$ with $\rho(H_1)^s = \rho(H_2)$.

(3.24). Problem. Let $N$ be a group and let the image $N^\rho$ of $N$ under the right regular representation $\rho: N \rightarrow \text{Sym}(N)$.

(a) Let $\lambda: N \rightarrow \text{Sym}(N)$ be the left regular representation of $N$ given by

$$k \mapsto \lambda(k) \text{ with } g^{\lambda(k)} = k^{-1}g,$$

for all $g \in N$.

(i) Prove that $\lambda$ is an isomorphism of $N$ with its image $N^\lambda$ in $\text{Sym}(N)$.

(ii) Prove that $C_{\text{Sym}(N)}(N^\rho) = N^\lambda$.

(b) Let $M = N_{\text{Sym}(N)}(N^\rho)$ and $A = \text{Stab}_M(1_N)$, the stabilizer of $1_N$ in $M$. Prove that $M = AN^\rho$ and that this is the internal semidirect product of $N^\rho$ by $A$.

(c) Prove that $A \simeq \text{Aut}(N)$.

(3.25). Problem. Let $G \leq \text{Sym}(\Omega)$. Prove that $G$ is $k$-transitive on $\Omega$ if and only if it is transitive on $\Omega$ and, for $a \in \Omega$, $G_a$ is $(k-1)$-transitive on $\Omega \setminus \{a\}$.

(3.26). Problem. (D.G. Higman) A graph is connected if you can get from any vertex to any other by walking along a finite length path of edges, disregarding edge direction. It is strongly connected if the path can always be chosen to be directed.

(a) Prove that transitive $(G, \Omega)$ is primitive if and only if all nondiagonal orbital graphs are strongly connected.

(b) Let $G$ be transitive on finite $\Omega$, and let $\Gamma$ be a $G$-invariant graph on $\Omega$. Prove that $\Gamma$ is connected if and only if it is strongly connected. (“If you can walk from a to b, then you can drive.”)

Remark. An infinite directed path shows that this can be false for infinite $\Omega$.

(3.27). Problem. Let the group $G$ contain the set $R = \{r_i \mid i \in I\}$. The Cayley graph $C(G; R)$ has as vertex the elements of $G$ and edges

$$x \rightarrow y \iff yx^{-1} \in R.$$ 

We can make it a colored graph via

$$x \overset{i}{\rightarrow} y \iff yx^{-1} = r_i.$$ 

$G$ acts by translation as a regular group of automorphisms on $C(G; R)$ since

$$xg \overset{i}{\rightarrow} yg \iff yg(xg)^{-1} = r_i \iff yx^{-1} = r_i \iff x \overset{i}{\rightarrow} y.$$ 

Thus the Cayley graph is an orbital graph for the right regular permutation representation. If we wish it to be undirected, we must require $R$ to be closed under inverses.

The full automorphism group could be much larger than $G$. (Imagine $R = G \setminus \{1\}$.)

(a) Prove that $C(G; R)$ is connected if and only if $G = \langle R \rangle$.

(b) Assume $G = \langle R \rangle$. Prove that the elements of $G$ are the only automorphisms of $C(G; R)$ that respect the edge coloring.
3.2 Linear groups

3.2.1 Basics

A $K$-linear representation of the group $G$ is a homomorphism $\varphi: G \rightarrow \text{GL}_K(V)$, where $V$ is a vector space over the division ring $K$. For $g \in G$ and $v \in V$, we usually write $v^{\varphi(g)}$ in the more compact form $v^g$. The $K$-space $V$ is a $G$-module over $K$.

If $\varphi$ is faithful, then $G$ is said to be a linear group. The degree of the representation is $\dim_K(V)$. A related concept is a projective representation, that being a homomorphism $\varphi: G \rightarrow \text{PGL}_K(V)$. As can be seen in Theorem 1.3, most of the finite simple groups are realized best as projective linear groups. That is a prime motivation for studying linear and projective representations.

Care must be taken with the terminology, since we are not requiring $V$ to have finite dimension. In the literature, the term “linear group” is usually reserved for those groups with faithful representations of finite degree, the finite dimensional linear groups.

If $K$ is a field, then a $K\text{-Vec}$-representation $\varphi: G \rightarrow \text{GL}_K(V)$ extends by linearity to a representation of the group algebra $KG \rightarrow \text{End}_K(V)$. This powerful observation allows the methods of associative algebras (such as the Wedderburn-Artin theory) to be applied in group theory. This becomes more unwieldy for division rings $K$; so we avoid this sharp tool, although it does leave its mark in our “module” terminology.

If $f$ is an invertible $K$-linear transformation $f: V_1 \rightarrow V_2$ (that is, a $K\text{-Vec}$-isomorphism) of the two $K$-spaces $V_1$ and $V_2$, then we have the induced isomorphism $f^*$ of $\text{GL}_K(V_1) = \text{Aut}_{K\text{-Vec}}(V_1)$ and $\text{GL}_K(V_2) = \text{Aut}_{K\text{-Vec}}(V_2)$, as in Section 1.3.

$$
\begin{array}{ccc}
V_1 & \rightarrow & V_1 \\
\downarrow f & & \downarrow f \\
V_2 & \rightarrow & V_2
\end{array}
$$

with

$$a \mapsto a^{f^*} = a^* = f^{-1}af. $$

Two $K$-linear representations $\varphi_1: G \rightarrow \text{GL}_K(V_1)$ and $\varphi_2: G \rightarrow \text{GL}_K(V_2)$ are equivalent in $K\text{-Vec}$ if, for some isomorphism $f: V_1 \rightarrow V_2$ and its induced isomorphism $f^*$, the diagram

$$
\begin{array}{ccc}
G & \xrightarrow{\varphi_1} & \text{GL}_K(V_1) \\
\downarrow f & & \downarrow f^* \\
G & \xrightarrow{\varphi_2} & \text{GL}_K(V_2)
\end{array}
$$

commutes. In this case we say that $V_1$ and $V_2$ are isomorphic $G$-modules.

In the larger category $\text{Vec}$ the two linear representations $\varphi_1: G \rightarrow \text{GL}_{K_1}(V_1)$
and \( \varphi_2: G \rightarrow \text{GL}_{K_2}(V_2) \) are equivalent if the diagram

\[
\begin{array}{ccc}
G & \xrightarrow{\varphi_1} & \text{GL}_{K_1}(V_1) \\
\downarrow & & \downarrow f^* \\
\varphi_2 & & \text{GL}_{K_2}(V_2)
\end{array}
\]

commutes, where now \( f^* \) is induced by a \textit{Vec}-isomorphism: an invertible semilinear map \( f: K_1V_1 \rightarrow K_2V_2 \). A \textit{semilinear map} (or \( \tau \)-semilinear map) \((\tau, t)\) from \( KV \) to \( FW \) is a homomorphism of additive groups \( t: (V, +) \rightarrow (W, +) \) that additionally, for the field embedding \( \tau: K \rightarrow F \), satisfies

\[
(\alpha v)^t = \alpha^\tau v^t,
\]

for all \( \alpha \in K, v \in V \).

Permutation representations give rise to linear representations. Let \( G \) act as permutations on the set \( \Omega \). For an arbitrary division ring \( K \), let the \( K \)-\textit{permutation module} \( K\Omega \) be the \( K \)-vector space with basis \( B = \{ e_\omega \mid \omega \in \Omega \} \). For each \( g \in G \) we define the linear transformation \( \varphi(g) \in \text{GL}_K(K\Omega) \) by

\[
e_{\omega}^g = e_{\omega^g}
\]

for all \( \omega \in \Omega \). The map \( \varphi: g \rightarrow \text{GL}_K(K\Omega) \) is then a representation of \( G \), the \( K \)-\textit{permutation representation}.

The matrix representing \( \varphi(g) \) in the basis \( B \) has a unique nonzero entry in each row and each column, that entry being a 1. Such a matrix \( M \) is called a \textit{permutation matrix} and is orthogonal in the sense that its transpose is its inverse: \( MM^\top = I \).

As an immediate consequence of Cayley’s Theorem [3.2], we have

(3.28). \textbf{Theorem.} Every group has a faithful representation as a \( K \)-linear group. \( \square \)

This is false if we restrict ourselves to representations of finite degree.

An elementary abelian \( p \)-group can be thought of as a vector space over the field \( \mathbb{F}_p \). Therefore linear representations also play an important role in the internal representation theory discussed earlier in Lemma [2.9]

(3.29). \textbf{Proposition.} Let \( V \) be an elementary abelian \( p \)-group. Then \( \text{Aut}(V) = \text{GL}_{\mathbb{F}_p}(V) \). \( \square \)

### 3.2.2 Irreducibility

With permutation groups we progressed from intransitive to transitive to primitive groups. We attempt similar reductions for linear groups. For permutation groups, we initially factored intransitive groups into transitive groups. For linear groups, the corresponding move is from reducible groups to irreducible groups, but it turns out that there is more than one flavor of each.
The representation \( \varphi : G \rightarrow \text{GL}_K(V) \) is reducible if there is a \( G \)-invariant (actually, \( \varphi(G) \)-invariant) \( K \)-subspace \( W \) with \( 0 < W < V \). If \( \varphi \) is not reducible, then it is irreducible. We then also say that \( G \) is irreducible on the \( V \) and that the \( G \)-module \( V \) is irreducible.

(3.30) Lemma. Let \( W \) be a submodule of the \( G \)-module \( V \) over \( K \) with \( 0 < W < V \). Further, let \( V^+ = W \oplus V/W \), the \( K \)-space direct sum of \( W \) and \( V/W \).

(a) The quotient \( K \)-space \( V/W \) has a natural structure as \( G \)-module given by \((v + W)g = v^g + W\).

(b) \( V^+ \) has a natural structure as \( G \)-module \( W \oplus V/W \) given by \( (u, (v + W))g = (u^g, v^g + W) \).

If in the lemma there is in \( V \) a \( G \)-submodule \( X \) with \( V = W \oplus X \), then \( V/W \) and \( X \) are isomorphic \( G \)-modules. We say that the extension is split and that \( V \) is \( G \)-decomposable (or just decomposable) with \( G \)-decomposition given by \( V = W \oplus X \). If \( V \) has no proper decompositions, then it is indecomposable. We can think of decomposability as a strong form of reducibility. Decomposability implies reducibility, and irreducibility implies indecomposability. If \( \Omega \) is an intransitive permutation space for \( G \), then the associated permutation module is decomposable, being the direct sum of smaller permutation modules.

In Proposition (3.3) we used the Chinese Remainder Theorem to reduce the study of intransitive permutation groups to that of transitive groups. We can use the present lemma to attempt a similar reduction from reducible to irreducible representations of linear groups. There are two problems with the approach. In the permutation case, we always knew that an orbit provides a transitive “subrepresentation,” but here there is no guarantee that a given module has an irreducible submodule. More fundamentally, and again unlike the permutation case, even when the map from \( G \) into \( \text{GL}_K(V) \) is faithful, there is no guarantee that the related representation in \( \text{GL}_K(V') \) is also faithful. The kernel will be trivial if the extension is split (in which case \( V \) and \( V' \) are isomorphic \( G \)-modules), but not in general. We will return to the case of nontrivial kernels in Section 3.2.4.

It is possible that a \( G \)-module over \( K \) is irreducible only because we are considering it over the wrong division ring. If \( K \) is a subdivision ring of \( L \), then the \( L \)-space \( W \) has a natural structure as \( K \)-space of dimension \( \dim_K(W) = [L: K] \dim_L(W) \). For example, the correspondence between \( a + bi \in \mathbb{C} \) and \((a, b) \in \mathbb{R}^2\) allows us to think of a complex representation of degree \( n \) as a real representation of degree \( 2n \). As a partial converse, one can think of any \( G \)-module \( X \) of dimension \( m \) over \( K \) as a \( G \)-module \( _LX \) of dimension \( m \) over \( L \) by extending coefficients to the tensor product module \( _LX = L \otimes_K X \). In this case the new module \( _LX \) may be \( G \)-reducible even though the original module \( _KX \) was \( G \)-irreducible. In the example, the real module \( _\mathbb{R}W \) of dimension \( m = 2n \) when extended to \( _\mathbb{C}W \) is a direct sum of two complex modules of dimension \( n \), one isomorphic to the original \( W \) and the second isomorphic to \( W \) twisted by
complex conjugation. An irreducible $G$-module over $K$ that remains irreducible over all extensions $L$ of $K$ is absolutely irreducible. In most places, the discussion of absolute irreducibility is restricted to the situation in which $K$ and $L$ are both fields.

### 3.2.3 Primitivity

The $G$-module $V$ is completely reducible if it is a sum of irreducible $G$-modules. In this case, for each irreducible $G$-submodule $W$ of $V$ we set $H_G(W)$ to be the sum in $V$ of all irreducible submodules of $V$ that are isomorphic to $W$ as $G$-modules. The module $H_G(W)$ is the homogeneous component corresponding to $W$.

**(3.31). Proposition.** Let the completely reducible $G$-module $V$ over $K$ be the sum $\sum_{e \in E} W_e$ of irreducible $G$-modules $W_e$.

(a) There is a subset $J$ of $E$ with $V = \bigoplus_{j \in J} W_j$.

(b) Let $I$ be a subset of $J$ such that $\{W_i \mid i \in I\}$ is a maximal set of pairwise nonisomorphic irreducible $G$-modules. Then every irreducible $G$-submodule of $V$ is isomorphic to one of the $W_i$ and $V = \bigoplus_{i \in I} H_G(W_i)$.

**Proof.** (a) Consider the partially ordered set $\mathcal{I}$ of subsets $S$ of $E$ with $\sum_{s \in S} W_s = \bigoplus_{s \in S} W_s$, ordered by containment. For every chain in $\mathcal{I}$, the union of the chain is also in $\mathcal{I}$; so by Zorn’s Lemma there is a maximal subset $J$. If $V' = \bigoplus_{j \in J} W_j$ is proper in $V$, then there is a $W_e$ not contained in $V_0$, since $V = \sum_{e \in E} W_e$. By irreducibility of $W_e$ we have $W_e \cap V' = 0$, hence $W_e + V' = W_e \oplus V'$. But then $J \cup \{e\} \in \mathcal{I}$, against maximality of $J$. Therefore $V = V'$.

(b) Let $U$ be an irreducible $G$-submodule of $V$. For the nonzero element $u \in U$, there is a finite subset $J_0$ of $J$ with $u \in V_0 = \bigoplus_{j \in J_0} W_j$, hence by irreducibility $U \leq V_0$. Choose such a $J_0$ of minimal cardinality. Clearly $J_0$ is nonempty; let $k \in J_0$. Then $U$ is not in $X_0 = \bigoplus_{j \in J \setminus k} W_j$, and by irreducibility $U$ meets this partial sum trivially. Therefore we have $U \oplus X_0 = U \oplus X_0$, and by the Second Isomorphism Theorem $U \simeq (U \oplus X_0)/X_0 \leq V_0/X_0 \simeq W_k$. By irreducibility of $W_k$, the modules $U$ and $W_k$ are isomorphic.

For each $i \in I$, let $J_i$ be the subset of $J$ consisting of those $W_j$ isomorphic to $W_i$. Then $V_j = \bigoplus_{j \in J_i} W_j$ is certainly in $H_G(W_i)$ and $V = \bigoplus_{i \in I} V_i$. The argument of the previous paragraph shows than any irreducible $G$-submodule $U$ isomorphic to $W_i$ is contained within a sum of irreducible modules $W_j$ with $j \in J_i$. Therefore $U \leq V_i$ and so $V_i = H_G(W_i)$.

Let $V$ be a $G$-module over $K$ and $N$ a normal subgroup of $G$. For each $g \in G$ and $X$ an $N$-submodule of $V$, the image $X^g$ is a new $N$-submodule of $V$. Indeed, for each $n \in N$ and $x^g \in X^g$, we have

$$(x^g)^n = (x^{gng^{-1}})^g \in X^g,$$

as $N$ is normal in $G$ and $X$ is an $N$-module. We also have $X = (X^g)^{g^{-1}}$, so $X$ is irreducible if and only if $X^g$ is irreducible.
3.2. LINEAR GROUPS

(3.32). Theorem. (Clifford’s Theorem) Let $V$ be an irreducible $G$-module over $K$ and $N$ a normal subgroup of $G$. Assume that $V$ contains an irreducible $N$-submodule $W$. (This will always be the case when $\dim_K(V) < \infty$). Then we have:

(a) $V$ is completely reducible as an $N$-module, and every irreducible $N$-submodule of $V$ is isomorphic to $W^g$, for some $g \in G$.

(b) $V$ is the direct sum of the distinct homogeneous components $H = H_N(W^g)$, and $G/N$ permutes these transitively under $H \mapsto H^g$.

(c) If $H = H_N(W^g)$ is an $N$-homogeneous component of $V$ and $A$ is the stabilizer of $N$ in $G$, then $H$ is an irreducible $A$-module.

Proof. (a,b) As $W$ is $N$-irreducible, each $W^g$ is $N$-irreducible. The sum $\sum_{g \in G} W^g$ is then a $G$-submodule of $V$. As $V$ is an irreducible $G$-module, $V = \sum_{g \in G} W^g$, and the rest follows by the proposition.

(c) For each $A$-submodule $L$ of $H$, the direct sum of the distinct $L^g$ is a $G$-submodule of $V$. As $G$ is irreducible on $G$, this forces $L$ to be either 0 or $L$. That is, $A$ is irreducible on $H$.

If there are two or more $N$-homogeneous components in Clifford’s Theorem, then we have an important instance of a frequent occurrence. An irreducible $G$-module $V$ is imprimitive if $V = \bigoplus_{i \in I} H_i$ is the direct sum of subspaces $H_i$ (of fixed dimension) permuted transitively by $G$. If the $G$-module $V$ is not imprimitive, then it is primitive.

3.2.4 Unipotent linear groups

As promised, we return to Lemma (3.30) to study the kernel of the stabilizer of a subspace.

(3.33). Lemma. The stabilizer of the subspace $W$ in $GL_K(V)$ is the semidirect product of $U = \{ M \in GL_K(V) \mid M|_W = 1_W, M|_{V/W} = 1_{V/W} \}$ by $L = GL_K(W) \times GL_K(X)$, where $X$ is some complement to $W$ in $V$.

If $V = W \oplus X$ is a decomposition into $G$-invariant subspaces $W$ and $X$ of $V$, then the subgroup stabilizing each subspace is $L = GL_K(W) \times GL_K(X)$.

Proof. In matrices:

\[
\left\{ \begin{pmatrix} A & 0 \\ * & B \end{pmatrix} \right\} = \left\{ \begin{pmatrix} I & 0 \\ * & I \end{pmatrix} \right\} \times \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\}
\]

where

\[
U = \left\{ \begin{pmatrix} I & 0 \\ * & I \end{pmatrix} \right\} \quad \text{and} \quad L = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\}.
\]

More generally, if $V = V_0 \geq V_1 \geq \cdots \geq V_k = 0$ is an $G$-invariant series in the $K$-space $V$, then the stability group of the series is the subgroup

\[
\left\{ g \in G \mid g|_{V_{i-1}/V_i} = 1_{V_{i-1}/V_i}, \ 1 \leq i \leq k \right\}.
\]
We shall see below that such a group is nilpotent of class at most \( k \). (See Problem (6.38))

**Lemma.** Let \( V = V_0 \geq V_1 \geq \cdots \geq V_k = 0 \) be a \( G \)-invariant series for the faithful \( G \)-module \( V \) over \( K \). Then \( V^+ = \bigoplus_{i=1}^k V_{i-1}/V_i \) is a \( G \)-module over \( K \).

If we restrict to the finite dimensional case, \( \dim_K(V) = n < \infty \), then, for an appropriate choice of basis, the kernel \( N \) of the representation of \( G \) on \( V^+ \) consists of all matrices of the form

\[
\begin{pmatrix}
I & 0 & 0 & 0 \\
* & I & 0 & 0 \\
* & * & \ddots & 0 \\
* & * & * & I \\
* & * & * & * & I
\end{pmatrix}
\]

where identity matrices have degree \( \dim_K(V_{i-1}/V_i) \) for \( k \geq i \geq 1 \), going from top to bottom.

The group of all \( n \times n \) matrices over \( K \) with 1’s on the diagonal and 0’s above the diagonal is the *lower unitriangular group*, which we will denote \( U(n)_K \). All such kernels as \( N \) above are all *block lower unitriangular* (with \( k \) blocks) and are contained in \( U(n)_K \).

The unipotent elements of \( GL_n(K) \) are those that are conjugate to an element of \( U(n)_K \). More generally, a *unipotent element* \( g \) of \( GL_n(K) \) (arbitrary dimension) is one with \((g - 1)^m = 0\) (in \( \text{End}_K(V) \)), for some integer \( m \). A *unipotent subgroup* of \( GL_n(K) \) is one all of whose elements are unipotent.

**Lemma.**

(a) For \( \text{char} K = 0 \), every nonidentity unipotent element of \( GL_n(K) \) has infinite order.

(b) For \( \text{char} K = p > 0 \), an element of \( GL_n(K) \) is unipotent if and only if it is a \( p \)-element. In this case, if \((g - 1)^m = 0\), then \( g^{p^{m-1}} = 1 \).

(c) A unipotent element \( g \in GL_n(K) \) is conjugate to an element of \( U(n)_K \) and, if \( \text{char} K = p > 0 \), has \( g^{p^{n-1}} = 1 \).

**Proof.** In characteristic \( p \), if \( g^p = 1 \), then \( g^{p^k} - 1 = (g - 1)^{p^k} = 0 \). Therefore in (b) \( p \)-elements are always unipotent.

Let \( g \) be a unipotent element with, say, \((g - 1)^m = 0\). Every \( v \in V \) is contained in a \( g \)-invariant subspace of dimension \( m_v \) at most \( m \), namely \( U_v = \sum_{i=0}^{m-1} K^i v^{(g-1)^i} = \sum_{i=0}^{m-1} K^{v^{g^i}} \).

Consider a \( v \) with \( v^g \neq v \); that is, \( U_v \) does not have dimension 1. For an appropriate basis, \( g \) is represented on \( U_v \) by a lower unitriangular matrix. Choose \( i > j \) with \( g_{ij} = a \neq 0 \) and, subject to that, with \( i - j \) minimal. Then \((g^k)_{ij} = ka \), for all \( k \). In characteristic 0 this is never 0; so \( g \) has infinite order on \( U_v \), giving (a).
3.2. LINEAR GROUPS

In characteristic $p$, we have $(g^p)_{ij} = 0$; and this is true for all $i', j'$ with $i' - j' \leq i - j$. Continuing in this manner, we see that $g^{p^{m-1}}$ is trivial on $U_v$. That is, for $l = \max_{v \in V} (m_v) \leq m$, the endomorphism $g^{p^{m-1}}$ is trivial on every $U_v$, and so is trivial on $V$. In particular $g^{p^{m-1}} = 1$. This gives (b).

If $g \in \text{GL}_n(K)$ then as above there is a basis in which $g$ is represented by a unitriangular matrix. And certainly $l \leq n$, so (c) is complete.

When $\dim_K(V)$ is finite, the unitriangular subgroups of $\text{GL}_K(V)$ are nilpotent. See Problem \[6.38\]

3.2.5 Sylow’s First Theorem (third time)

**(3.36).** Theorem. (Sylow’s First Theorem) If the finite group $G$ has order $|G| = p^a m$ with $p$ prime, $a \in \mathbb{N}$, and $\gcd(p, m) = 1$, then $G$ contains subgroups of order $p^a$ and index $m$.

**Proof.** Consider $G$ acting faithfully on a module $\mathbb{F}_p^n$ (for instance, the permutation module $V = \mathbb{F}_p G$). In this action, it permutes the set $\Omega$ of all nonzero vectors of $V$. Here $|\Omega| = p^n - 1$ is not a multiple of $p$. Therefore some orbit of $G$ on $\Omega$ has order prime to $p$. If the orbit has size greater than 1, then by induction on order a point stabilizer contains a Sylow $p$-subgroup of $G$. If the orbit has size 1, say $v$, then $G$ that acts on the nonzero vectors of the smaller space $V/\mathbb{F}_p v$. By induction on dimension the group induced by $G$ on this quotient space has a Sylow $p$-subgroup $\bar{P}$. The kernel of that action is a normal Sylow $p$-group, and the preimage $P$ of $\bar{P}$ in $G$ is then a Sylow $p$-subgroup of $G$. $\square$

**(3.37).** Corollary. $U_n(p^a)$ is a Sylow $p$-subgroup of $\text{GL}_n(p^a)$.

**Proof.** This can of course be proven by a calculation of the order of $\text{GL}_n(p^a)$. Also the argument used above can be used to show first that every $p$-subgroup fixes a 1-space and indeed a vector, and then induction takes over. $\square$

3.2.6 Problems

**(3.38).** Problem. 2. Let $V$ be the $K$-permutation module for the finite group $G = \text{Sym}(\Omega)$; that is, $V = \bigoplus_{\omega \in \Omega} K e_\omega$, with $e^g_\omega = e_{g \omega}$, for all $g \in \text{Sym}(\Omega)$ and $\omega \in \Omega$. Let

$$U = \left\{ \sum_{\omega \in \Omega} a_\omega e_\omega \mid \sum_{\omega \in \Omega} a_\omega = 0, a_\omega \in K \right\}$$

and

$$Z = \left\{ \sum_{\omega \in \Omega} a_\omega e_\omega \mid a_\omega = a \in K, \text{ for all } \omega \right\}.$$

(a) Prove that $U$ and $Z$ are $G$-submodules of $V$.
(b) Prove that 0, $Z$, $U$, and $V$ are the only $G$-submodules of $V$. 

(3.39). Problem. Consider $\text{Mat}_n(K)$, the space of $n \times n$ matrices from $K$, as a module for the group $G = \text{GL}_n(K) \times \text{GL}_n(K)$, where, for $M \in \text{Mat}_n(K)$ and $(A,B) \in G$, we have

$$M^{(A,B)} = A^T MB.$$ 

Prove that $\text{Mat}_n(K)$ is irreducible for $G$.

(3.40). Problem. Let $G$ and $H$ be finite groups, and let $X : G \to \text{GL}_K(V)$ and $Y : H \to \text{GL}_K(W)$ be $K$-representations of $G$ and $H$.

(a) Prove that $X \oplus Y : G \times H \to \text{GL}_K(V \oplus W)$ given by

$$(v, w)_{X \oplus Y}^{(g, h)} = (v^X(g), w^Y(h))$$

is a representation of $G \times H$.

(b) Prove that $X \otimes Y : G \times H \to \text{GL}_K(V \otimes_K W)$ (tensor product) given by

$$(v \otimes w)_{X \otimes Y}^{(g, h)} = v^X(g) \otimes w^Y(h)$$

is a representation of $G \times H$.

(c) Prove that if $X \otimes Y$ is irreducible then $X$ and $Y$ are irreducible.

Remark. In the special case $G = H$ the group $G$ itself has a natural embedding on the diagonal of $G \times H = G \times G$, namely $\delta : G \to G \times G$ given by $\delta(g) = (g, g)$. The composition of this with the representations $X \oplus Y$ and $X \otimes Y$ (restricted to the image of $\delta$) gives new $K$-representations of $G$ as the “sum” and “product” of the two original representations. With this in mind, the collection of all $K$-representations of $G$ can naturally be given structure of a ring, indeed a $K$-algebra since the effect of scalar multiplication is easy to see. (We do want to factor by equivalence).

The source of this nice additional structure is the innocent diagonal mapping $\delta$. The natural abstract setting is that of Hopf algebras. These are associative $K$-algebras $A$ that in addition to having the usual multiplication $\mu : A \otimes_K A \to A$ also have a well-behaved comultiplication $\delta : A \to A \otimes_K A$. The previous paragraph is then about the special (and motivating) example where $A$ is the group algebra $KG$.

(3.41). Problem. Prove that an element $g$ of $\text{End}_K(V)$ with $(g - 1)^m = 0$ for some $m$ must belong to $\text{GL}_K(V)$.
Finiteness and Reduction

Many mathematical arguments follow the path of breaking a large problem into a number of smaller problems. Particular examples are the three “unique factorization” results presented in Section 1.1. The questions then are:

(i) What do we mean by “smaller”?
(ii) How do we achieve the “break”?

For us, smallness will usually be gauged by a finiteness condition—a property that the object under study shares with finite objects. Once a suitable finiteness condition is imposed, then reduction via something resembling induction becomes available.

4.1 Finiteness: Sylow’s First Theorem, one last time

Of course, the basic finiteness condition for a group is the requirement that the group be finite. As already discussed, the classification of finite simple groups Theorem[1.3] proceeds by induction, studying an arbitrary finite simple group $G$ all of whose proper simple sections are on the theorem’s list and ultimately proving that $G$ then is also on the list.

As an example of how such reductions go, we have a last\textsuperscript{1} proof of Sylow’s First Theorem.

\textbf{(4.1). Proposition.} The First Sylow Theorem is valid in all finite groups if and only if it is valid in all finite simple groups.

\textbf{Proof.} One direction is clear. Now assume that the First Sylow Theorem holds in all finite simple groups. Let $G$ be an arbitrary finite group and $p$ a

\textsuperscript{1}I promise!
prime. We prove that $G$ satisfies the First Sylow Theorem for the prime $p$ by induction on $|G|$.

If $G$ is simple then we are done by hypothesis. Therefore we may assume that $G$ contains a normal subgroup $N$, not equal to $G$ or to 1. By induction $N$ and $G/N$ both have Sylow $p$-subgroups. Let $P$ be a Sylow $p$-subgroup of $N$. By the Second Sylow Theorem, all Sylow $p$-subgroups of $N$ are conjugate, and by the Frattini argument $G = N_G(P)N$.

By the Second Isomorphism Theorem $G/N \cong N_G(P)/N_N(P)$. In particular, $[G:N_G(P)]$ is not a multiple of $p$, and a Sylow $p$-subgroup of $N_G(P)$ is a Sylow $p$-subgroup of $G$. Especially a Sylow $p$-subgroup of $G/N$ is isomorphic to one of $N_G(P)/N_N(P)$.

As $P$ is Sylow in $N$, the index $[N_N(P):P]$ is not a multiple of $p$. By the Third Isomorphism Theorem

$$N_G(P)/P \cong N_N(P)/N_N(P).$$

Therefore a preimage of a Sylow $p$-subgroup of $N_G(P)/N_N(P)$ in $N_G(P)/P$ is a Sylow $p$-subgroup of $N_G(P)/P$. In turn a preimage of that in $N_G(P)$ is a Sylow $p$-subgroup of $N_G(P)$ and so of $G$. \hfill $\Box$

(4.2). Proposition. For the prime $p$, assume:

Every finite simple group that has order a multiple of $p$ but is not $a$-group has a permutation representation with no fixed points and of degree not a multiple of $p$.

Then the First Sylow Theorem holds for the prime $p$ holds.

Proof. The proof is by induction on the order of the arbitrary finite group $G$. If $G$ itself is a $p$-group, then there is nothing to prove.

By the previous proposition, we need only consider finite simple $G$ that is not a $p$-group. By the assumption, it has a faithful permutation representation with no fixed points and of degree not a multiple of $p$. But then it has in this an orbit, not of length 1 but of length not a multiple of $p$. As $G$ is simple, it is faithful on this orbit. For $\omega$ a point in this orbit, $G_\omega$ is a proper subgroup of $G$. By induction, it contains a Sylow $p$-subgroup which is then a Sylow $p$-subgroup of $G$. \hfill $\Box$

(4.3). Proposition. Let $p$ be a prime. If $G$ is a finite simple group of order $p^a m$ with $a \in \mathbb{Z}^+$ and $1 \neq m$ coprime to $p$, then $G$ has a permutation representation with no fixed points and of degree not a multiple of $p$.

Proof. As $m \neq 1$, the group $G$ is nonabelian simple by Proposition [2.18].

We give three constructions of an appropriate $G$-space $\Omega$:

1. (Class equation proof) Let $\Omega = G \setminus \{1\}$ with conjugation action. Any orbits of length 1 would correspond to elements of the center of nonabelian simple $G$. 

4.2. Finite generation and countability

(2) (Wielandt’s permutation proof) Let $\Omega = G^p$ with translation action. As $m \neq 1$, all orbits of $G$ on $\Omega$ are nontrivial. The following binomial coefficient calculation shows that $|\Omega|$ is not a multiple of $p$:

$$|\Omega| = \binom{p^a m}{p^a} = \frac{(p^a m)(p^a m - 1) \cdots (p^a m - p) \cdots (p^a m - p^a - 1) \cdots (p^a m - p^a + 1)}{(p^a)(p^a - 1) \cdots (p^a - p) \cdots (p^a m - p^a - 1) \cdots (1)}.$$ 

(3) (Unipotent subgroup proof) Let $\Omega = V \setminus \{0\}$ where $V$ is an $F_p$-space that is a faithful $G$-module and, subject to that, has minimal degree. (The permutation module $F_p G$ proves that such a $V$ exists.) If there is an orbit of length 1, then $G$ has abelian hence trivial action on the 1-space it spans. But then the quotient of $V$ by that 1-space would give a representation of smaller degree that is faithful as $G$ is nonabelian simple.

(4.4). Theorem. (Sylow’s First Theorem) If the finite group $G$ has order $|G| = p^a m$ with $p$ prime, $a \in \mathbb{N}$, and $\gcd(p, m) = 1$, then $G$ contains subgroups of order $p^a$ and index $m$.

Proof. Proposition (4.3) combines with Proposition (4.2) to give the result.

4.2 Finite generation and countability

In many applications the groups studied are not necessarily finite but do have a finite description. The fundamental group of a surface is often finitely generated or even finitely presented. Here the group $G$ is finitely generated if there is a finite subset $X$ of $G$ with $G = \langle X \rangle$, and it is additionally finitely presented if there is some finite set of relations $R$ such that $G \cong \langle X \mid R \rangle$; that is, $G$ is isomorphic to the free group $F(X)$ on $X$ modulo its normal subgroup $(F(X))_R$.

There are many important results in this area; see [Rob82, §14.1]. Here we are content with one that is of great importance both theoretically and computationally.

(4.5). Theorem. Let $G$ be a group and $H$ a subgroup of finite index in $G$.

(a) (Schreier) If $G$ is finitely generated, then $H$ is finitely generated.

(b) (Reidermeister-Schreier) If $G$ is finitely presented, then $H$ is finitely presented.

Proof. (a) Let $G$ be generated by the finite set $X$, and let $Y = \{ g_i \mid i \in I \}$ be a finite set of coset representatives for $H$ in $G = \bigcup_{i \in I} H g_i$. For ease, we assume $1_G = g_0 \in Y$.

For each $g \in G$ let the coset representative $\bar{g} \in Y$ be given by $g \in H \bar{g}$. We claim that $H$ is generated by the finite set of Schreier generators

$$W = \{ (xy)^{p^a-1} \mid x \in X \cup X^{-1}, y \in Y \}.$$
Indeed every element $g$ of $G$ can be written, for some $n \in \mathbb{Z}^+$, as $y_1 \prod_{i=1}^{n} x_i$ with $x_i \in X \cup X^{-1}$ and $y_1 \in Y$. (Recall that $1_G = g_0 \in Y$.) Then

$$g = y_1 \prod_{i=1}^{n} x_i = (y_1 x_1)(y_1 x_1^{-1} y_1 x_1) \prod_{i=2}^{n} x_i = ((y_1 x_1)(y_1 x_1^{-1}))(y_1 x_1) \prod_{i=2}^{n} x_i = w_1 \left(y_2 \prod_{i=2}^{n} x_i \right)$$

with $w_1 = (y_1 x_1) y_1 x_1^{-1} \in W \subseteq H$ and $y_2 = y_1 x_1 \in Y$. Therefore by induction on $n$, every element $g$ of $G$ can be rewritten as a product $\prod_{i=1}^{n} w_i y_{n+1}$ of elements $w_i$ in $W$ and a final member $y_{n+1}$ of $Y$. If $g$ happens to belong to $H$, then $\prod_{i=1}^{n} w_i \in H$ forces $y_{n+1} = g_0 = 1_G$, hence $g \in \langle W \rangle$. Therefore $H = \langle W \rangle$.

(b) (Sketch). If $R$ is a set of relations defining $G$ with respect to the generating set $X$, then $S = \{ yry^{-1} \mid y \in Y, r \in R \}$ is a set of relations defining $H$ with respect to the generating set $W$, where, as above, the Reidermeister rewriting process allows us to rewrite the relations of $S$ as words in the generating set $W$ of $H$. The set $S$ is finite if $R$ is finite.

The difficulty that must be resolved before we have a complete proof is that, while by (a) the subset $W$ (actually a bijective preimage) within $F(X)$ certainly generates the full preimage of $H$, it might not do so freely. Schreier solved this by proving that, given a careful initial choice of the set $Y$ of representatives, a free generating set results from deleting all elements of $W$ that are the identity in $F(X)$.

Every finitely generated group is countable. Indeed every countably generated group is countable. Countability is thus a weaker finiteness property than finite generation. It still can be useful. In particular, a countable group can be expressed as the union of an ascending chain of its subgroups. Suppose $G = \{ g_i \mid i \in \mathbb{Z}^+ \}$ is a countable group. For each $i$ set $G_i = \langle g_1, \ldots, g_i \rangle$. Then $G = \bigcup_{i \geq 1} G_i$ with

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_i \leq \cdots$$

This may allow us to check certain properties of $G$ more easily in one of the finitely generated subgroups $G_i$.

(4.6). Lemma. The nontrivial group $G$ is simple if and only if for every pair of elements $g, h \in G$ with $g \neq 1$, there is a finite subset $X(h, g)$ of $G$ with $h \in \langle g^2, (g^{-1})^x \mid x \in X(h, g) \rangle$. 

Proof. If $G$ is simple, then $G = \langle g^G \rangle$ and $h$ is a product of a finite number of conjugates of $g$ or its inverse.

Conversely, assume that for each $h$ and $g \neq 1$ the set $X(h, g)$ exists. Let $N$ be a nontrivial normal subgroup of $G$ and choose $1 \neq n \in N$. Then for every $h$ in $G$ every element of $\{ n^x, (n^{-1})^x \mid x \in X(h, n) \}$ is in $N$, hence $h \in N$. That is, $N = G$ and $G$ is simple.

Of course for a given $g, h$ there can be many appropriate finite subsets $X(h, g)$.

(4.7). Theorem. (P. Hall) Let $G$ be a simple group. Then every countable subset of $G$ is contained in a countable simple subgroup of $G$.

Proof. Let $S$ be a countable subset of $G$. Then define

$$S(S) = \langle S, X(h, g) \mid 1 \neq g, h \in S \rangle,$$

where $X(h, g)$ is a set as in the lemma. As $S$ is countable and each $X(h, g)$ is finite, $S(S)$ is also countable. Set $S^0(S) = \langle S \rangle$ and recursively define $S^i(S) = S(S^{i-1}(S))$ for integral $i \geq 2$. Then

$$S \subseteq S^0(S) \subseteq S^1(S) \cdots \subseteq S^i(S) \subseteq \cdots$$

with $S$ and each subgroup in the sequence countable.

Then $S^\infty = \bigcup_{i \geq 1} S^i(S)$ is a countable subgroup of $G$ containing $S$, and by the lemma it is simple.

4.3 Limits and finite approximation

Above we used the fact that every countable set is an ascending union of finite subsets hence every countable group is an ascending union of finitely generated subgroups. But every set is the union of its finite subsets, and so every group is the union of its finitely generated subgroups. Can we make these trivial observations useful?

The set of subgroups $\Gamma = \{ G_i \mid i \in I \}$ is a local system in $G$ if

(i) $G_i \leq G$ for each $i \in I$, and $G = \bigcup_{i \in I} G_i$

(ii) for each $i, j \in I$, there is a $k \in I$ with $\langle G_i, G_j \rangle \leq G_k$.

In this case we say that $G$ is the directed limit of its local system $\Gamma$.

We may also call this the finitely directed limit, since an easy induction shows that for any finite subset $J$ of $I$ there is a $k$ with $\langle G_j \mid j \in J \rangle \leq G_k$. Correspondingly, $G$ is the countably directed limit of the local system $\Gamma$ provided for every countable subset $J$ of $I$ there is always a $k \in I$ with $\langle G_j \mid j \in J \rangle \leq G_k$.

(4.8). Proposition.

$^2$This is actually the internal directed limit. There is a corresponding more general external directed limit, which we do not define.
CHAPTER 4. FINITENESS AND REDUCTION

(a) Every group is the directed limit of its finitely generated subgroups.

(b) Every group is the countably directed limit of its countable subgroups.

Proof. If \( G_i \) is generated by \( X_i \), then \( \langle G_i \mid i \in I \rangle \) is generated by \( \{ X_i \mid i \in I \} \).

Phillip Hall’s Theorem \( \text{(4.7)} \) can now be refined to say

\[ (4.9) \text{. Theorem. (P. Hall)} \text{ Every simple group is the countably directed limit of its countable simple subgroups.} \]

Proof. Let \( \{ G_i \mid i \in I \} \) be the set of all countable simple subgroups of simple \( G \). By Theorem \( \text{(4.7)} \) we have \( G = \bigcup_{i \in I} G_i \). Let \( J \) be a countable subset of \( I \). Then \( \bigcup_{j \in J} G_j \) remains countable, so by Theorem \( \text{(4.7)} \) again there is a \( k \in I \) with \( \langle G_j \mid j \in J \rangle \leq G_k \).

Usually groups have many local systems of finitely generated subgroups. For any group property \( \mathcal{X} \), the group \( G \) is locally-\( \mathcal{X} \) provided it has a local system, all of whose members enjoy the property \( \mathcal{X} \). Especially a group that has a local system of finite subgroups is called a locally finite group.

Every finite group is locally finite, of course, but there are others. In particular, every torsion abelian group is locally finite, and we will soon encounter additional interesting infinite examples in Theorem \( (4.15) \).

\[ (4.10) \text{. Theorem. Let } G \text{ be a group. Then the following are equivalent:} \]

1. \( G \) is locally finite.
2. Every finite subset of \( G \) generates a finite subgroup.
3. Every finite subset of \( G \) is contained in a finite subgroup.

\[ (4.11) \text{. Theorem. (Schmidt’s Theorem) Let } N \text{ be normal in the group } G. \text{ Then } G \text{ is locally finite if and only if } G/N \text{ and } N \text{ are locally finite.} \]

Proof. If \( G \) is locally finite then so are its subgroup \( N \) and its image \( G/N \). Now assume that normal \( N \) and \( G = G/N \) are locally finite. Let \( X \) be a finite subset of \( G \), and set \( H = \langle X \rangle \).

As \( \bar{X} \) is a finite subset of locally finite \( \bar{G} \), we have \( \langle \bar{X} \rangle = \bar{H} \) finite. That is, \( HN/N \) is finite. By the Second Isomorphism Theorem, \( H/H \cap N \) is finite, and especially \( H \cap N \) has finite index in finitely generated \( H \). By Schreier’s Theorem \( (4.5) \) a), the subgroup \( H \cap N \) is also finitely generated. Within locally finite \( N \) this tells us that \( H \cap N \) is finite. As both \( H/H \cap N \) and \( H \cap N \) are finite, \( H \) itself is finite, as required.

Locally finite group theory admits many of the techniques of finite group theory, since the presence of the local system says that the group can be well approximated by its finite subgroups.

Dually, at times we may be able to approximate a group by its finite quotients. For any group property \( \mathcal{X} \), the group \( G \) is residually-\( \mathcal{X} \) provided that for
4.3. LIMITS AND FINITE APPROXIMATION

every nonidentity element $g$ of $G$ there is a normal subgroup $N_g$ with $g \notin N_g$ for which the quotient $G/N_g$ has property $X$. Of special interest here is the class of groups that are residually finite. This does not imply that $\langle g \rangle$ is finite or intersects $G/N_g$ trivially. Indeed $\mathbb{Z}$ is residually finite but has no subgroups of finite order. More generally:

(4.12). Theorem. (Schreier) Every free group is residually finite.

Proof. In the free group $F(X)$ let

$$g = x_1x_2 \cdots x_n$$

be a nonidentity element, written as a word in the various $x$ and $x^{-1}$ for $x \in X$, the only restriction being that we never have $\{x_i, x_{i+1}\} = \{x, x^{-1}\}$. (That is, $x_1x_2 \cdots x_n$ is a reduced word in $F(X)$.)

We define a map $x_i \mapsto \pi_i$ from $F(X)$ to $\text{Sym}(n+1)$ choosing each $\pi_i$ to extend the mapping $i \mapsto i+1$. Notice that for different $i, j$ we may have $\pi_i = \pi_j$, but our restriction on the $x_i$ implies that nevertheless the choices can be made consistently. Having done this, we have a map $\pi: F(X) \rightarrow \text{Sym}(n+1)$ in which $\pi(g) \neq 1_{F(X)}$ since $1^{\pi(g)} = n + 1$. Thus $\ker \pi = N_g$ is the desired finite index normal subgroup of $F(X)$ with $g \notin N_g$.

For residually finite groups, again a simple induction shows that for every finite subset $S$ of $G$ with $1_G \notin S$, there is a normal subgroup $N_S$ of $G$ with $S \cap N_S = \emptyset$.

(4.13). Theorem. Let $G$ be a group. Then the following are equivalent:

(1) $G$ is residually finite.

(2) $G$ is a subdirect product of finite groups.

Proof. If $G$ is residually finite, then the Chinese Remainder Theorem tells us that $G$ is a subdirect product of the various finite groups $G/N_g$.

If $G$ is a subdirect product of finite groups, then every element $g$ of $G$ projects nontrivially onto at least one of the finite quotients. Projection onto that coordinate then gives a homomorphism of $G$ onto a finite group for which $g$ is not in the kernel.

Especially free groups are subdirect products of finite groups.

For an arbitrary group $G$, its profinite topology declares all subgroups of finite index index in $G$ to be a base of open neighborhoods of the identity (with additional open sets being provided by the cosets of these subgroups). This topology is then Hausdorff precisely when $G$ is residually finite. Many interesting results about finite $p$-groups as a class arise from study of the larger class of pro-$p$ groups: those groups that are residually finite $p$-groups. Again free groups are examples, for all $p$, although this is harder to prove.
4.4 Representational finiteness

For a linear representation \( \varphi : G \to \text{GL}_K(V) \), finiteness conditions may impose restrictions on the division ring \( K \) or on the \( K \)-space \( V \).

The most common finiteness restriction made on a division ring \( K \) is that it have finite dimension over its center. Indeed later on we shall only consider division rings equal to their centers—fields. Even there additional restrictions may be of help. For instance, by Jordan canonical form a faithful \( \mathbb{C} \)-representation of a finite group can be realized over a finite Galois extension of the rationals. We will not spend much time on such matters, although later we will see that mileage can be gained by requiring \( K \) itself to be finite.

We have already noted that every group can be faithfully represented as a linear group. On the other hand many but not all infinite groups can be faithfully represented on finite dimensional vector spaces. We have seen in Clifford’s Theorem (3.32) and in Problem (6.38) that finite dimensionality of a representation is a useful finiteness condition. Indeed finite dimensionality of \( V \) is such an important hypothesis that, unlike us (see page 59), many (for instance, Robinson [Rob82]) reserve the term linear group for those groups that can be faithfully represented on a finite dimensional space. A weaker, but still useful, condition is that of local linearity, where \( G \) has a local system of subgroups, each of which has a faithful representation of finite dimension. This includes all locally finite groups and many other groups as well.

We now introduce groups that might be termed “internally locally linear” as they have faithful possibly infinite dimensional representations within which every finitely generated subgroup acts faithfully on some finite dimensional subspace.

If \( g \in \text{Sym}(\Omega) \), then the support of \( g \) on \( \Omega \), written \( \text{Supp}_\Omega(g) \), is the set \( \{ \omega \in \Omega \mid \omega^g \neq \omega \} \). The identity certainly has finite support. The inverse of an element of finite support also has finite support, as does the product of two elements of finite support. Therefore the elements of finite support,

\[
\text{FSym}(\Omega) = \{ g \in \text{Sym}(\Omega) \mid |\text{Supp}_\Omega(g)| < \infty \},
\]

form a subgroup of \( \text{Sym}(\Omega) \) called the finitary symmetric group. Of course, if \( \Omega \) itself is finite, then \( \text{FSym}(\Omega) = \text{Sym}(\Omega) \). If \( \Omega \) is infinite then this is not the case, and \( \text{FSym}(\Omega) \) consists of the “nearly trivial” permutations.

(4.14). Theorem. \( \text{FSym}(\Omega) \trianglelefteq \text{Sym}(\Omega) \).

Proof. By Lemma 3.5 conjugacy preserves the cardinality of the support of a permutation. \( \Box \)

If \( N \) is any nontrivial normal subgroup of \( \text{Sym}(\Omega) \) with \( 1 \neq n \in N \) and \( 1 \neq g \in \text{FSym}(\Omega) \), then Lemma 3.5 also proves \( [n, g] \in N \cap \text{FSym}(\Omega) \). This observation is the beginning of the classification of all normal subgroups of \( \text{Sym}(\Omega) \). These include the normal subgroup \( \text{FSym}_\alpha(\Omega) \) consisting of all permutations with support of cardinality less than \( \alpha \), for each infinite cardinal \( \alpha \) less than or equal to \( |\Omega| \).
A fundamental result is

(4.15). \textbf{Theorem.} For every $\Omega$, the group $FSym(\Omega)$ is locally finite.

\textbf{Proof.} For the finite subset $\{g_1, \ldots, g_n\}$ of $FSym(\Omega)$, let $H = \langle g_1, \ldots, g_n \rangle$ and $\Delta = \bigcup_{i=1}^n \text{Supp}_\Omega(g_i)$, a finite subset of $\Omega$ which is $H$-invariant. We may identify the finite group $\text{Sym}(\Delta)$ with the pointwise stabilizer of $\Omega \setminus \Delta$ in $FSym(\Omega)$, and then the map $H \rightarrow \text{Sym}(\Delta) \leq FSym(\Omega)$ is injective.

Thus every finite subset of $G$ is contained in a finite subgroup, and $G$ is locally finite by Theorem \textbf{(4.10)} \qquad \square

The corresponding group of “nearly trivial” linear transformations is

$$FGL_K(V) = \{ g \in \text{GL}_K(V) \mid \dim_K(V^{g-1}) < \infty \}.$$  

The group (as it is) $FGL_K(V)$ is the \textit{finitary linear group} and is normal in $\text{GL}_K(V)$. In matrix terms, this group can be thought of as those invertible linear transformations $g$ for which, with a suitable choice of basis, the matrix $g - 1$ only has a finite number of nonzero rows. A group and representation are \textit{stably linear} if they satisfy the stronger condition of having a fixed basis for which each $g - 1$ has only a finite number of nonzero rows and nonzero columns—that is, a finite number of nonzero entries.

Finitary linear groups need not be locally finite, but groups that are both locally finite and finitary linear have a beautiful and well-understood structure. These include $FSym(\Omega)$.

(4.16). \textbf{Theorem.} $FSym(\Omega)$ is finitary linear over every $K$.

\textbf{Proof.} Consider $g \in FSym(\Omega)$ acting on the permutation module $K\Omega$. For $\omega \in \Omega$, we have $e^g_\omega = 0$ if and only if $\omega$ is fixed by $g$. That is, the only elements of the $K$-basis $\{ e_\omega \mid \omega \in \Omega \}$ that have nontrivial image under $g - 1$ are those with $\omega$ in the support of $g$. For elements $g$ of $FSym(\Omega)$ this support is finite, therefore $V^{g-1}$ has a finite spanning set and $g \in FGL(K)K\Omega$. \qquad \square

\section{4.5 Chain conditions}

Chain conditions illustrate both “finiteness” and “reduction” in that the groups considered exhibit finiteness properties precisely because they admit some type of reduction.

In any partially ordered set $(I, \succeq)$, the \textit{descending chain condition} states that any chain

$$a_1 \succeq a_2 \succeq a_3 \succeq \cdots$$

stabilizes at some point: there is an $N \in \mathbb{Z}^+$ with $a_i = a_j$, for all $i, j \geq N$. Equivalently we have the \textit{minimal condition}: every nonempty subset of $I$ contains at least one minimal element. In the opposite partially ordered set $(I, \preceq)$ where $a_1 \preceq a_2$ if and only if $a_1 \succeq a_2$ in $(I, \succeq)$, these become the \textit{ascending chain condition} and \textit{maximal condition}.
For us, there are group theoretic and representation theoretic versions of each. Clifford’s Theorem \(3.32\) is valid for all \(G\)-modules with the minimal condition on submodules.

For a given group \(G\), there are several posets that may be considered: those of all subgroups of \(G\), all normal subgroups of \(G\), and all subnormal subgroups of \(G\).

The Jordan-Hölder Theorem \(1.2\) addresses composition series for the group \(G\)—those chains of subnormal subgroups \(G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_k = 1\) with each quotient \(G_i = G_{i-1}/G_i\) simple—stating that the multiset of simple factors is uniquely determined up to isomorphism. If instead we consider the poset of normal subgroups of a group, a chain that cannot be refined is a chief series. In this context there is also the appropriate Jordan-Hölder Theorem. (See [Rob82, Theorem 3.1.4].) The corresponding factors are chief factors, and the next result gives their structure in many situations of interest (for instance when \(G\) is finite).

A minimal normal subgroup of \(G\) is a subgroup \(N\) with \(1 \neq N \leq G\) and such that, whenever \(W \leq G\) with \(W \leq N\), either \(1 = W\) or \(W = N\). For finite groups these must exist by order arguments, but in general they might not. The group \((\mathbb{Z}, +)\) has no minimal normal subgroups.

\(4.17\). Theorem. Let \(G\) be a group that satisfies the minimal condition on subnormal subgroups and \(N\) minimal normal in \(G\). Then there is an index set \(I\) and a set of subgroups \(\{S_i \mid i \in I\}\) such that

(a) each \(S_i\) is simple and minimal normal in \(N\);
(b) for each \(i, j \in I\), there is a \(g_{ij} \in G\) with \(S_{g_{ij}} = S_j\);
(c) \(N = \langle S_i \mid i \in I \rangle = \bigoplus_{i \in I} S_i\).

Proof. This theorem and its proof should be compared with Clifford’s Theorem \(3.32\) the proposition on completely reducible modules that precedes it, and their proofs.

Let \(S\) be a minimal normal subgroup of \(N\). Then \(\langle S^g \mid g \in G \rangle\) is clearly nontrivial, normal in \(G\), and contained in \(N\); so \(N = \langle S^g \mid g \in G \rangle\). Choose a set of conjugates \(\{S_i = S^{g_i} \mid i \in I\}\) that generates \(N\) and is minimal subject to this. That is, \(N = \langle S_i \mid i \in I \rangle\) and \(N > S_J = \langle S_j \mid j \in J \rangle\), for all \(J \subsetneq I\). (Such a set exists by Zorn’s Lemma.)

As the \(S_J\) are conjugates of \(S_i\), they too are minimal normal in \(N\); and each \(S_J\) is normal in \(N\). Set \(g_{ij} = g_i^{-1} g_j\). We now have (b) and half of (a).

For each \(i\), the subgroup \(S_i \cap S_{I \setminus i}\) is normal in \(N\) but is not equal to \(S_i\) by minimality of \(I\). Since \(S_i\) is minimal normal in \(N\), we find \(S_i \cap S_{I \setminus i} = 1\), giving (c) by Theorem \(2.34\).

Finally, if \(T \subseteq S_i\), then

\[ N_N(T) \supseteq (S_i, S_{I \setminus i}) = N, \]
by (c). As $S_i$ is minimal normal in $N$, this forces $T = 1$. Therefore $S_i$ is simple, completing (a) and the theorem.

A characteristically simple group $G$ is minimal normal in the split extension of $G$ by $\text{Aut}(G)$. In particular in appropriate situations (for instance for finite $G$) the theorem describes all characteristically simple groups. (Compare Problem [2.46])

4.6 Problems

(4.18). Problem. Prove that a group with a local system of simple subgroups is simple.

(4.19). Problem. Recall that a group $G$ is quasisimple if it is perfect $G = G'$ and $G/Z(G)$ is simple.
(a) Prove that the nontrivial group $G$ is quasisimple if and only if for every pair of elements $g$ and $h$ in $G$ with $g \not\in Z(G)$ it is possible to write $h$ as the product of a finite number of conjugates of $g$ and $g^{-1}$.
(b) Prove that a group with a local system of quasisimple subgroups is quasisimple.

(4.20). Problem. Let $G$ be a simple and locally finite group. Prove that for every finite subgroup $H$ of $G$, there are finite subgroups $F$ and $N$ of $G$ with
(i) $F \supseteq N$;
(ii) $F/N$ simple;
(iii) $H \leq F$ and $H \cap N = 1$.

Remark. This important observation, due to Kegel, says that every finite subgroup $H$ of the locally finite simple group $G$ can be “covered” by a finite simple section $F/N$ of $G$. This is a “finite” version of P. Hall’s “countable” result Theorem [4.7].

Hint: Consider $S^2(H)$.

(4.21). Problem. Let $F$ be a division ring. Prove that $F$ is a locally finite division ring if and only if $F$ is an algebraic extension of the ground field $\mathbb{F}_p$, for some prime $p$. In particular, a locally finite division ring is a countable field. (Here, by a locally finite division ring, we mean a division ring in which every finite subset is contained in some finite sub-division ring.)

Hint: You may use Wedderburn’s theorem that all finite division rings are fields.

(4.22). Problem.
(a) Prove that if $G$ is a permutation group on $\Omega$ with all orbits finite, then $G/\ker_{\Omega}(G)$ is residually finite.
(b) An FC-group is a group in which all conjugacy classes are finite. Abelian groups are examples; for instance $\mathbb{Z}$ is an FC-group that is residually finite, but $(\mathbb{Q}, +)$ is an FC-group that is not residually finite. (Indeed $(\mathbb{Q}, +)$ has no subgroups of finite index.) Prove that if $G$ is an FC-group, then $G/Z(G)$ is residually finite.

(4.23). Problem.
(a) Let $g \in \text{Sym}(\Omega)$ have the orbit $\Delta$ on $\Omega$ and set $W = \bigoplus_{s \in \Delta} K e_s$, a $(g)$-invariant subspace in the action on the permutation module $K\Omega$. Prove that $W^{g^{-1}}$ has $K$-dimension $|\Delta| - 1$.
(b) Prove $F\text{Sym}(\Omega) = \text{Sym}(\Omega) \cap \text{FGL}_K(K\Omega)$. 
5.1 Transpositions

In $\text{Sym}(\Omega)$ and its subgroup $\text{FSym}(\Omega)$ a transposition is a 2-cycle $(a,b)$ for distinct $a, b \in \Omega$.

(5.1) Lemma.

(a) The transpositions form a conjugacy class of elements of order 2 in $\text{Sym}(\Omega)$ and $\text{FSym}(\Omega)$.

(b) If $g = (a,b)$ and $h = (c,d)$, then, respectively,

$$|gh| = 1, 2, 3 \quad \text{as} \quad |\{a,b\} \cap \{c,d\}| = 2, 0, 1 .$$

In the last case $\langle(a,b), (b,c)\rangle = \text{Sym}(\{a,b,c\}) \leq \text{FSym}(\Omega)$.

(c) We have

$$C_{\text{Sym}(\Omega)}((a,b)) = \langle(a,b)\rangle \times \text{Sym}(\Omega \setminus \{a,b\})$$

and

$$C_{\text{FSym}(\Omega)}((a,b)) = \langle(a,b)\rangle \times \text{FSym}(\Omega \setminus \{a,b\}) .$$

Here for each subset $\Delta$ of $\Omega$, we have identified $\text{Sym}(\Delta)$ with the subgroup of $\text{Sym}(\Omega)$ that fixes $\Omega \setminus \Delta$ pointwise (and so for the corresponding finitary subgroups as well). This is standard, and we will continue to make this identification without comment.

The elements $(1, 2)(1, 3) = (1, 2, 3)$ of Lemma 5.1(b) are the 3-cycles of $\text{Sym}(\Omega)$ while the products $(1, 2) \cdot (3, 4) = (1, 2)(3, 4)$ are the $2^2$-elements.

(5.2) Theorem.

(a) The subgroup of $\text{Sym}(\Omega)$ generated by the class of transpositions is $\text{FSym}(\Omega)$. 59
CHAPTER 5. SYMMETRIC AND ALTERNATING GROUPS

(b) If $G$ is a subgroup of $\text{FSym}(\Omega)$ that is generated by transpositions, then, for the partition $\Omega = \bigsqcup_{i \in I} \Omega_i$ of $\Omega$ into distinct $G$-orbits $\Omega_i$, we have $G = \bigoplus_{i \in I} \text{FSym}(\Omega_i)$.

**Proof.** Each transposition is finitary, so the group they all generate is contained in the finitary symmetric group. For (a) it remains to observe that 

$$(1,2,3,\ldots,m) = (1,2)(1,3) \cdots (1,m).$$

Now let $G = \langle X \rangle \leq \text{FSym}(\Omega)$ with $X$ a set of transpositions, and let $Y$ be the set of all transpositions that are in $G$.

Define a graph with vertex set $\Omega$ and $a \sim b$ if and only if $(a,b)$ is one of the transpositions in $Y$. Let the connected components of $\Omega$ in this graph be $\Omega_i$ for $i \in I$. We claim that $G = \bigoplus_{i \in I} \text{FSym}(\Omega_i)$. The $\Omega_i$ are the orbits of $G$ on $\Omega$, so $G$ is contained in this direct sum. It remains to prove that $G$ contains each $\text{FSym}(\Omega_i)$.

Let distinct $a, b$ be in the connected component $\Omega_i$, and select

$$a = a_0 \sim a_1 \sim \cdots \sim a_m = b,$$

an $\Omega_i$-path from $a$ to $b$, chosen to be as short as possible.

If $m > 1$, then we have

$$a = a_0 \sim a_1 \sim a_2 \sim \cdots \sim a_m = b.$$

But then, with $f = (a_0, a_1)$ and $g = (a_1, a_2)$, both transpositions of $G$ and $Y$, we have $f^g = (a_0, a_2)$ in $G$ and hence in $Y$. But then the path

$$a = a_0 \sim a_2 \sim \cdots \sim a_m = b,$$

is shorter than the original one. This is a contradiction, and so $m = 1$. That is, $(a_0, a_m) = (a, b)$ is a transposition of $Y$ and $G$, and this holds for arbitrary $a, b$ from $\Omega_i$. Therefore all transpositions with support from $\Omega_i$ belong to $Y$ and $G$, hence by (a) the subgroup $\text{FSym}(\Omega_i)$ is in $G$. \qed

### 5.2 The Weyl group $W(A_k)$

For $k \in \mathbb{Z}^+$ consider the group

$$W(A_k) = \langle a_1, \ldots, a_k \mid a_i^2 = 1, (a_ia_{i+1})^3 = 1, (a_ia_j)^2 = 1 \text{ for } |i - j| > 1 \rangle,$$

the Coxeter group of type $A_k$. The $W$ stands for Weyl. This groups is also the Weyl group of type $A_k$, but that involves different definitions.

We first discuss some elementary consequences of these relations. Under the map sending every $a_i$ to $-1 \in \{\pm 1\}$ all relations are satisfied, so there is a homomorphism onto a group of order 2. In particular all of the elements $a_i$ have order exactly two in $W(A_k)$ rather than one.
5.2. THE WEYL GROUP $W(A_k)$

The relation $(a_ia_j)^2 = 1$ states $a_ia_ja_ia_j = 1$. As all $a_i$ have order 2, this becomes

$$a_ia_j = a_ia_i;$$

that is, if $|i - j| > 1$ then the elements $a_i$ and $a_j$ commute in $W(A_k)$. Similarly

$$(a_ia_{i+1})^3 = 1$$
reads as $a_ia_{i+1}a_{i+1}a_{i+1} = 1$ or

$$a_ia_{i+1} = a_{i+1}a_ia_{i+1},$$

the so-called braid relation; see Problem (5.23).

(5.3). THEOREM. The map $f : a_i \mapsto (i, i+1)$, for $1 \leq i \leq k$, extends to an isomorphism $\varphi$ of $W(A_k)$ and $\text{Sym}(k+1)$.

Proof. By Lemma (5.1) the given transpositions in $\text{Sym}(k+1)$ satisfy the corresponding relations of $W(A_k)$, and by Theorem (5.2) these transpositions generate all of $\text{Sym}(k+1)$. Therefore the map $f$ extends at least to a surjective homomorphism $\varphi$ from $W(A_k)$ onto $\text{Sym}(k+1)$.

Set $W_k = W(A_k)$. We claim:

(i) For $B = \langle a_1, \ldots, a_{k-1} \rangle \leq W_k$ and $n = a_k$, we have $W_k = B \cup BnB$.

(ii) $|W_k| \leq (k+1)!$.

Once we have claim (ii) we will be done, since by the previous paragraph we already have $|W_k| \geq (k+1)! = |\text{Sym}(k+1)|$.

Our proof of the claims will be by induction on $k$. For $k = 1$ we have $B = 1$ and

$$W_1 = \{1\} \cup \{1n1\} = \{1, a_1\} \simeq Z_2 \simeq \text{Sym}(1+1).$$

We now assume $k \geq 2$.

The image of $B$ under $\varphi$ is $\text{Sym}(k)$. Therefore by induction $B \simeq \text{Sym}(k)$ and also its subgroup $C = \langle a_1, \ldots, a_{k-2} \rangle$ is isomorphic to $\text{Sym}(k-1)$. Furthermore, by induction (or direct calculation) $B = C \cup CmC$ for $m = a_{k-1}$.

By the relations for $W_k = W(A_k)$,

$$nmn = a_ka_{k-1}a_k = a_{k-1}a_ka_{k-1} = mnn$$

and

$$[C, n] = [(a_1, \ldots, a_{k-2}), a_k] = 1.$$
verified at length is $BnB.BnB \subseteq B \cup BnB$. Indeed

\[
BnB.BnB = Bn(C \cup CmC)nB
= B(nCn \cup nCmCn)B
= B(C \cup CmnC)nB
= B(C \cup CmnmC)B
= B \cup BnmnB
= B \cup BnB,
\]
as desired.

For (ii) we have $|B| = k!$, and so the list of all triples $(b_1, n, b_2)$ with $b_1, b_2 \in B$ has length $(k!)^2$. For $c \in C$, the two list members $(b_1, n, b_2)$ and $(b_1c^{-1}, n, cb_2)$ satisfy $b_1nb_2 = b_1c^{-1}ncb_2$ as $c$ commutes with $n$. Thus

\[
|BnB| \leq (k!)^2/|C| = (k!)^2/(k - 1)! = k \cdot k!.
\]

Therefore by (i)

\[
|W_k| = |B \cup BnB| \leq k! + k \cdot k! = (k + 1)k! = (k + 1)!,
\]

completing our proof of claim (ii) and so of the theorem. \qed

5.3 The alternating group and simplicity

The alternating group $\operatorname{Alt}(\Omega)$ is the subgroup of $\operatorname{FSym}(\Omega)$ consisting of all finitary permutations that can be written as a product of an even number of transpositions.

(5.4) Theorem. For $|\Omega| \geq 2$, the alternating group $\operatorname{Alt}(\Omega)$ is a normal subgroup of index 2 in $\operatorname{FSym}(\Omega)$. Indeed $\operatorname{Alt}(\Omega) = \operatorname{FSym}(\Omega)'$ is the unique subgroup of index 2 in $\operatorname{FSym}(\Omega)$.

Proof. First consider the case $|\Omega| = n$, finite. Then by Theorem [5.3] we have

\[
\operatorname{FSym}(\Omega) = \operatorname{Sym}(\Omega) \simeq \operatorname{Sym}(n) \simeq W(A_{n-1}).
\]

Thus, as noted before, there is a surjective homomorphism from $W(A_{n-1})$ to $\{\pm 1\}$ given by $a_i \mapsto -1$, and this provides a surjective homomorphism

\[
\operatorname{sgn}: \operatorname{Sym}(n) \longrightarrow \mathbb{Z}_2.
\]

Each $a_i$ of $W(A_{n-1})$ maps to a transposition of $\operatorname{Sym}(n)$, so the kernel of $\operatorname{sgn}$ has index 2 in $\operatorname{Sym}(n)$ and consists of all products of an even number of transpositions. That is, $\ker \operatorname{sgn} = \operatorname{Alt}(n)$ is normal of index 2.

Now consider arbitrary $\Omega$. As $\Omega$ is the directed limit of its finite subsets $\Delta$, $\operatorname{FSym}(\Omega)$ is the directed limit of its finite subgroups $\operatorname{FSym}(\Delta)$, as in Theorem
5.3. THE ALTERNATING GROUP AND SIMPLICITY

Each embedding of $\text{FSym}(\Delta)$ into $\text{FSym}(\Omega)$ takes the transpositions of $\text{FSym}(\Delta)$ to transpositions of $\text{FSym}(\Omega)$. Therefore the various sign homomorphisms $\text{sgn}_\Delta$ combine to give a uniform sign homomorphism $\text{sgn}_\Omega$ on $\text{FSym}(\Omega)$ with kernel $\text{Alt}(\Omega)$.

The group $\text{FSym}(\Omega)$ is generated by its transposition class by Theorem (5.2)(a), so its derived quotient has order at most 2 by Proposition (2.17). The subgroup $\text{Alt}(\Omega)$ has index 2 in $\text{FSym}(\Omega)$. If $\mathcal{N} \neq \text{Alt}(\Omega)$ also had index 2, then $\mathcal{N} \cap \text{Alt}(\Omega)$ would be normal with an abelian quotient of order 4. The contradiction proves that $\text{Alt}(\Omega) = \text{FSym}(\Omega)'$ is the unique subgroup of index 2 in $\text{FSym}(\Omega)$.

(5.5). Corollary. For $n \geq 2$, the group $\text{Alt}(n) = \text{Alt}\{1, 2, \ldots, n\}$ has order $n! / 2$.

The homomorphism 

$$\text{sgn}: \text{FSym}(\Omega) \rightarrow \mathbb{Z}_2.$$ 

of the theorem, which takes each transposition to $-1 \in \{\pm 1\} \simeq \mathbb{Z}_2$, is called the sign homomorphism. The elements of its kernel $\text{Alt}(\Omega)$ are the even permutations of $\Omega$ while those of $\text{FSym}(\Omega)$ that are not in $\text{Alt}(\Omega)$ are the odd permutations.

(5.6). Proposition.

(a) $\text{Alt}(\Omega)$ is generated by its 3-cycles and its $2^2$-elements.

(b) If $|\Omega| > 4$, then $\text{Alt}(\Omega)$ is generated by its conjugacy class of 3-cycles.

(c) If $|\Omega| > 4$, then $\text{Alt}(\Omega)$ is generated by its conjugacy class of $2^2$-elements.

Proof. (a) If $g = \prod_{i=1}^{2m} t_i$, then $g = \prod_{j=1}^m (t_{2j-1} t_{2j})$, so this follows from Lemma (5.1).

(b) By Lemma (3.5) the 3-cycles form a single conjugacy class in $\text{FSym}(\Omega)$. As the odd permutation $(4, 5)$ centralizes $(1, 2, 3)$, this is also a single class in $\text{Alt}(\Omega)$ provided $|\Omega| > 4$. Then $(1, 3, 2)(3, 2, 4) = (1, 2)(3, 4)$, so (a) gives the result.

(c) By Lemma (3.5) in $\text{Sym}(\Omega)$ the $2^2$-elements form a single conjugacy class. As the odd permutation $(1, 2)$ centralizes $(1, 2)(3, 4)$, the collection of $2^2$-elements remains a single class in $\text{Alt}(\Omega)$. Furthermore $(1, 2)(4, 5) \cdot (1, 3)(4, 5) = (1, 2, 3)$, so again (a) gives the result.

Of course, for $n = 3, 4$, the group $\text{Alt}(n)$ is still generated by its 3-cycles, but a 3-cycle is not conjugate to its inverse in these two groups.

(5.7). Proposition. For $n \leq 4$, the group $\text{Sym}(n)$ is solvable.\footnote{As Galois knew!}

(5.8). Theorem. If $|\Omega| > 4$, then $\text{Alt}(\Omega)$ is nonabelian and simple.
CHAPTER 5. SYMMETRIC AND ALTERNATING GROUPS

Proof. Let \( 1 \neq n \in N \leq \text{Alt}(\Omega) \) and \( a, b, c \in \Omega \) with \( a^n = b \neq a \) and \( b^n = c \). Choose \( d \notin \{a, b, c\} \) so that for \( h = (a, b, d) \in \text{Aut}(\Omega) \) we have \( h^n = (b, c, e) \) where \( e = d^n \). Then

\[
g = [h, n] = h^{-1}h^n = (a, d, b)(b, c, e) \in N \cap \text{Alt}\{a, b, c, d, e\}.
\]

As \( d^3 = c \neq d \), we have \( g \neq 1 \). In particular \( \text{Alt}(\Omega) \) is not abelian. The element \( g \) must have cycle type one of 3, 2, or 5. In the first two cases we find \( N = \text{Alt}(\Omega) \) by Proposition (5.6), therefore we may assume that \( a, b, d, c, e \) are distinct and so \( g = (a, d, c, e, b) \).

Now let \( k = (a, d, c) \). Then

\[
[g, k] = g^{-1}g^k = (b, e, c, d, a)(d, c, a, e, b) = (a, d, e) \in N,
\]

and again \( N = \text{Alt}(\Omega) \) by Proposition (5.6).

(5.9). Corollary. If \(|\Omega| > 4\), then \( \text{Alt}(\Omega) \) is the unique minimal normal subgroup in \( \text{Sym}(\Omega) \).

Proof. A permutation of \( \Omega \) that maps every 3-subset to itself must then map every point to itself (as the intersection of 3-subsets, using \(|\Omega| > 3\)). Therefore by Lemma (3.5) and Proposition (5.6) we have \( C_{\text{Sym}(\Omega)}(\text{Alt}(\Omega)) = 1 \).

For \( 1 \neq n \in N \leq \text{Sym}(\Omega) \) choose a \( g \in \text{Alt}(\Omega) \) that does not commute with \( n \). Then

\[
1 \neq [g, n] = g^{-1}(n^{-1}gn) = (g^{-1}n^{-1}g)n \in \text{Alt}(\Omega) \cap N.
\]

Therefore \( \text{Alt}(\Omega) \cap N \) is a nontrivial normal subgroup of simple \( \text{Alt}(\Omega) \), hence \( \text{Alt}(\Omega) \leq N \).

5.4 Geometry and automorphisms

This section is focused on proof of:

(5.10). Theorem. For \(|\Omega| \neq 2, 6\) we have

\[
\text{Aut}(\text{Sym}(\Omega)) = \text{Aut}(\text{FSym}(\Omega)) = \text{Sym}(\Omega).
\]

Additionally \( \text{Aut}(\text{Sym}(2)) = 1 \) and \( \text{Sym}(6) \) has index at most 2 in \( \text{Aut}(\text{Sym}(6)) \).

The proof of the theorem follows a standard and important model: we define a geometric object upon which the group acts; we then reconstruct the geometry within the group; we finally identify the group’s automorphisms within the geometry’s automorphisms. The process is not always precise (as in the present case for \(|\Omega| = 6\)) but in practice this allows us to locate a large portion of the

\[\text{Indeed, one of the most compelling aspects of finite group theory and geometry is the way in which a small number of anomalous or sporadic examples force themselves upon us in the midst of a general result.}\]
5.4. GEOMETRY AND AUTOMORPHISMS

The automorphism group of the group within the more manageable automorphism group of the geometry. For instance, here the geometry is that of the underlying set for the symmetric group as structured by its set of unordered pairs.

The general model is our motivation for a somewhat grandiose name:

(5.11). **Theorem.** *(Fundamental Theorem of Set Geometry)* Let $|\Omega| \geq 5$. Consider the graph $K(\Omega, 2)$ whose vertex set is the set $\binom{\Omega}{2}$ with $\{i, j\}$ adjacent to $\{k, l\}$ precisely when $|\{i, j\} \cap \{k, l\}| = 1$. Then $\text{Aut}(K(\Omega, 2)) = \text{Sym}(\Omega)$ with the natural action.

**Proof.** As $|\Omega| \geq 3$ the group $\text{Sym}(\Omega)$ acts naturally and faithfully on $K(\Omega, 2)$.

The maximal cliques (maximal complete subgraphs) of $K(\Omega, 2)$ are of two distinct types:

$$T_{a, b, c} = \{\{a, b\}, \{b, c\}, \{a, c\}\} \text{ for } \{a, b, c\} \in \binom{\Omega}{3}$$

of cardinality 3 and

$$C_a = \{\{a, w\} \mid w \in \Omega \setminus \{a\}\} \text{ for } a \in \Omega.$$ 

of cardinality $|\Omega| - 1 \geq 3$. Automorphisms of the graph must take maximal cliques to maximal cliques. Therefore for any $g \in \text{Aut}(K(\Omega, 2))$ and each $a \in \Omega$, there is a unique $a^g \in \Omega$ with $C_a = C_{a^g}$. This gives a natural action of the automorphism group on $\Omega$ and a surjective homomorphism $\text{Aut}(K(\Omega, 2)) \rightarrow \text{Sym}(\Omega)$.

The kernel of this homomorphism fixes globally each clique $C_a$. But then, for each pair $a, b \in \Omega$, the kernel must fix $\{a, b\} = C_a \cap C_b$. Therefore every pair $\{a, b\} \in \binom{\Omega}{2}$ is fixed, and the kernel is trivial. We conclude that $\text{Aut}(K(\Omega, 2))$ and $\text{Sym}(\Omega)$ are isomorphic. \[ \square \]

(5.12). **Proposition.** Let $T$ be the conjugacy class of transpositions in $\text{Sym}(\Omega)$ with $|\Omega| \geq 3$. The noncommuting graph $\Gamma$ of $T$ is the graph whose vertices are the members of $T$ with $a$ and $b$ adjacent when $a$ and $b$ do not commute.

(a) $\Gamma \simeq K(\Omega, 2)$.

(b) The subgroup of $\text{Aut}(\text{Sym}(\Omega))$ that stabilizes the class $T$ of transpositions is equal to $\text{Sym}(\Omega)$.

(c) The subgroup of $\text{Aut}(\text{FSym}(\Omega))$ that stabilizes the class $T$ of transpositions is equal to $\text{Sym}(\Omega)$.

**Proof.** We have $T = \{\{a, b\} \mid \{a, b\} \in \binom{\Omega}{2}\}$. By Lemma [5.1] the two transpositions $(i, j)$ and $(k, l)$ do not commute if and only if $|\{i, j\} \cap \{k, l\}| = 1$. Therefore $\Gamma$ is isomorphic to $K(\Omega, 2)$, as in (a).

In (b) and (c) let $G$ be, respectively, the stabilizer in $\text{Aut}(\text{FSym}(\Omega))$ and $\text{Aut}(\text{Sym}(\Omega))$ of the class $T$. By Lemma [3.5] we have $C_{\text{Sym}(\Omega)}(\text{FSym}(\Omega)) = 1$, and we may identify $\text{Sym}(\Omega)$ with its image in $G$. 

By (a) and Theorem \([5.11]\), if \(\Omega \geq 5\) then \(G\) induces automorphisms of \(\Gamma\) and \(K(\Omega, 2)\); and we have a surjective homomorphism \(\varphi : G \rightarrow \text{Sym}(\Omega)\) with natural action. The kernel of this action fixes all vertices of \(\Gamma\), the class of transpositions. This remains true for \(|\Omega| = 3\), as in \(\text{Sym}(3)\) the point stabilizers are the transpositions plus the identity, and also for \(\Omega = 4\), as in \(\text{Sym}(4)\) the point stabilizers are the Sylow 3-normalizers, isomorphic to \(\text{Sym}(3)\).

Thus the kernel of \(\varphi\) acts trivially on \(\text{FSym}(\Omega)\), the group generated by all transpositions \((a, b)\) (by Theorem \([5.2]\)). In particular, we are done in (b), where \(G \leq \text{Aut}(\text{FSym}(\Omega))\).

Now suppose \(g\) is an element of \(G \leq \text{Aut}(\text{Sym}(\Omega))\) that is in the kernel of \(\varphi\) and so acts trivially on \(\text{FSym}(\Omega)\). For arbitrary \(s \in \text{Sym}(\Omega) \leq G\), the commutator \([s, g] = s^{-1}s^g\) is in \(\text{Sym}(\Omega)\) but remains in the kernel of \(\varphi\). As already noted \(C_{\text{Sym}(\Omega)}(\text{FSym}(\Omega)) = 1\), so we conclude \([s, g] = 1\). Therefore \(g\) fixes all elements \(s\) of \(\text{Sym}(\Omega)\), and again \(\ker \varphi\) is trivial. This completes (c).

(5.13). **Proposition.** If \(d \in \text{Sym}(\Omega)\) is an element of order 2 having at least \(k\) orbits of length 2 on \(\Omega\), then there is a normal elementary abelian 2-subgroup of order at least \(2^k\) that is normal in the centralizer of \(d\) in both \(\text{FSym}(\Omega)\) and \(\text{Sym}(\Omega)\).

**Proof.** The centralizer of the element \((a_1, a_2) \cdots (a_{2k-1}, a_{2k}) \cdots\) has the normal subgroup \(\langle (a_1, a_2), \ldots, (a_{2k-1}, a_{2k}) \rangle\) both in \(\text{FSym}(\Omega)\) and in \(\text{Sym}(\Omega)\).

(5.14). **Lemma.** For \(|\Omega| \geq 2\) with \(|\Omega| \neq 6\), the conjugacy class of transpositions is stabilized by \(\text{Aut}(\text{FSym}(\Omega))\) and by \(\text{Aut}(\text{Sym}(\Omega))\).

**Proof.** By Lemma \([5.1]\) the centralizers of \((a, b)\) in \(\text{FSym}(\Omega)\) and \(\text{Sym}(\Omega)\) are, respectively, \(\langle (a, b) \rangle \times \text{Sym}(\Omega \setminus \{a, b\})\) and \(\langle (a, b) \rangle \times \text{FSym}(\Omega \setminus \{a, b\})\). Thus, by Theorem \([5.8]\) and Corollary \([5.9]\) for \(|\Omega| \geq 7\) the largest normal 2-subgroup of the centralizer of a transposition in \(\text{FSym}(\Omega)\) has order 2. On the other hand, for any other element of order 2 in \(\text{FSym}(\Omega)\), the corresponding centralizer has a normal 2-subgroup of larger order by the previous proposition. Therefore all automorphisms of these groups cannot take a transposition to an element of order 2 with support of size greater than 2 and must take transpositions to transpositions.

For \(|\Omega| \in \{2, 3, 4, 5\}\) the transpositions are the only elements of order 2 in \(\text{Sym}(\Omega)\) but not in \(\text{Alt}(\Omega) = \text{Sym}(\Omega)'\), so again automorphisms must take transpositions to transpositions.

**Proof of Theorem \([5.10]\)**

Certainly \(\text{Aut}(\text{Sym}(2)) = 1\). Also an automorphism of \(\text{Sym}(6)\) must fix \(\text{Alt}(6)\) (say, by Corollary \([5.9]\)). But \(\text{Sym}(6) \setminus \text{Alt}(6)\) has two conjugacy classes of involutions—the transpositions and those of cycle type \(2^3\). Therefore the index of \(\text{Sym}(6)\) in \(\text{Aut}(\text{Sym}(6))\) is at most 2 by Proposition \([5.12]\).

We may now assume \(|\Omega| \neq 2, 6\). Thus by Lemma \([5.14]\) both \(\text{Aut}(\text{Sym}(\Omega))\) and \(\text{Aut}(\text{FSym}(\Omega))\) stabilize the class of transpositions. By Proposition \([5.12]\) again, \(\text{Sym}(\Omega)\) is the full automorphism group of \(\text{Sym}(\Omega)\) and \(\text{FSym}(\Omega)\).
5.5 PROBLEMS

(5.15) Problem. Let \( n \in \mathbb{Z}^+ \). A subgroup of \( \text{Sym}(n) \) is \((n - 2)\)-transitive if and only if it contains \( \text{Alt}(n) \).

Remark. \( \text{Sym}(6) \) contains a 3-transitive subgroup that does not contain \( \text{Alt}(6) \); see Problem (5.20) below.

(5.16) Problem. (Thompson Transfer) Assume that the finite group \( G \) has a Sylow 2-subgroup \( S \) containing subgroup \( T \) of index 2 in \( S \) and an element \( s \) of order 2 in \( S \) with \( s^2 \cap T = \emptyset \). Prove that \( G \) has a normal subgroup of index 2 that does not contain \( s \).

Hint: Consider \( s \) in the permutation action of \( G \) on the cosets of \( T \).

(5.17) Problem. Prove that the finite group \( G \) with a cyclic Sylow 2-subgroup \( S \) has a normal subgroup \( N \) of odd order with \( G = N \rtimes S \).

Hint: Consider the action of \( S \) in the right regular representation of \( G \).

(5.18) Problem. Prove that if \( G \) is a subgroup of \( \text{Alt}(\Omega) \) that is generated by 3-cycles, then, for the partition \( \Omega = \bigsqcup_{i \in I} \Omega_i \) of \( \Omega \) into distinct \( G \)-orbits \( \Omega_i \), we have \( G = \bigoplus_{i \in I} \text{Alt}(\Omega_i) \).

(5.19) Problem. Prove that for \( |\Omega| \geq 4 \) but \( |\Omega| \neq 6 \) we have

\[ \text{Aut}(\text{Alt}(\Omega)) = \text{Sym}(\Omega). \]

Also \( \text{Sym}(6) \) has index at most 2 in \( \text{Aut}(\text{Alt}(6)) \).

(5.20) Problem.

(a) Let \( G \) be \( \text{Sym}(5) \) or \( \text{Alt}(5) \). Prove that the normalizer of a Sylow 5-subgroup has index 6 in \( G \).

(b) Prove that \( \text{Sym}(6) \) contains a 3-transitive subgroup that does not contain \( \text{Alt}(6) \).

(c) Prove that \( [\text{Aut}(\text{Sym}(6)):\text{Sym}(6)] \geq 2 \) and \( [\text{Aut}(\text{Alt}(6)):\text{Sym}(6)] \geq 2 \). (Hence we have equality by Theorem (5.10) and the previous problem.)

(5.21) Problem. Let \( G = \langle D \rangle \) be generated by the conjugacy class \( D = d^2 \) of elements of order 2 with the property that:

\[ \text{for all } d, e \in D \text{ we have } |de| \in \{1, 2, 3\}. \]

Such a conjugacy class is called a class of 3-transpositions in the 3-transposition group \( G \). This concept and terminology, due to B. Fischer, arise because a basic example is the class of transpositions in \( \text{FSym}(\Omega) \); see Lemma [5.1].

Consider the special case in which we additionally have:

\((\text{Sym}(5))\) For \( a, b, c, d \in D \) with connected diagram, the subgroup \( \langle a, b, c, d \rangle \) is isomorphic to \( \text{Sym}(k) \) for \( k \leq 5 \) with \( a, b, c, d \) all being mapped to transpositions.

Assume also that there is a subgroup \( H \) of \( G \) with \( H = (H \cap D) \cong \text{Sym}(5) \) (the elements of \( D \cap H \) acting as the transpositions of \( \text{Sym}(5) \)). Prove that there is a set \( \Omega \) with \( G \cong \text{FSym}(\Omega) \), the elements of \( D \) being mapped to the transpositions of \( \text{FSym}(\Omega) \).

Hint: Consider the maximal subsets \( C \) of \( D \) with the property that \( e, f \in C \) implies \( (ef)^3 = 1 \).
(5.22). Problem. Let $G_0$ be the symmetric group $\text{Sym}(5)$, and let $G_1$ be the symmetric group $\text{Sym}(G_0) \simeq \text{Sym}(120)$. Identify $G_0$ with the subgroup of $\text{Sym}(G_0)$ that is the right regular representation of $G_0$. Continue in this fashion: identify each $G_i$ with its regular representation as a subgroup of $G_{i+1} = \text{Sym}(G_i)$. Set $G = \bigcup_{i \in \mathbb{N}} G_i$, a group that is the ascending union of the $G_i$.

(a) Prove that $G$ is locally finite and simple. HINT: Consider Problem (4.18).

(b) Prove that if $H_1$ and $H_2$ are isomorphic finite subgroups of $G$, then there is an element $s \in G$ with $H_1^s = H_2$. HINT: Consider Problem (3.23).

Remark. The group $G$ is Phillip Hall’s universal locally finite group.

(5.23). Problem. Consider the braid group

$$B_k = \langle \alpha_1, \ldots, \alpha_k \mid \alpha_i \alpha_{i+1} \alpha_i = \alpha_{i+1} \alpha_i \alpha_{i+1}, \alpha_i \alpha_j = \alpha_j \alpha_i \text{ for } |i - j| > 1 \rangle.$$

(a) Prove that the map $\alpha_i \mapsto a_i$ extends to a homomorphism of the braid group onto $W(A_k) \simeq \text{Sym}(k+1)$.

(b) Prove that in $B_k$, every generator $\alpha_i$ has infinite order and $B_k / B'_k \simeq \mathbb{Z}$.\footnote{This should be formalized using directed limits, but we hope it is clear what is intended.}
6 Matrices

(6.1). Proposition. \( \text{Mat}_n(R) \simeq \text{Mat}_n(R^{\text{op}})^{\text{op}} \) via transpose.

Proof. \( \Box \)

(6.2). Corollary. \( \text{GL}_n(R) \simeq \text{GL}_n(R^{\text{op}}) \) via transpose-inverse.

Proof. \( \Box \)

6.1 Elementary matrices and operations

We start by considering the group \( \text{GL}_n(R) \) of all invertible matrices with entries from the ring \( R \) with identity.

Within \( \text{GL}_n(R) \) there are three types of elementary matrices:

(i) Elementary permutations \( \pi_{(i,j)} \). These are just the permutation matrices corresponding to the transpositions \( (i,j) \) of the symmetric group;

(ii) Elementary diagonal matrices \( h_j(u) \). These are the diagonal matrices in which all diagonal entries are 1 except for the \( (j,j) \)-entry which is \( u \), a unit in \( R \);

(iii) Elementary transvections \( t_{i,j}(a) \). These are the matrices \( I + ae_{i,j} \) with \( a \in R \) and \( i \neq j \), where \( e_{i,j} \) is a matrix unit—all its entries are 0 except for a 1 in the \( (i,j) \)-position.

The matrix group generated by the elementary permutation matrices \( \pi_{(i,j)} \) is the group of all \( n \times n \) permutation matrices—the image of \( \text{Sym}(n) \) under \( \pi \)—and we often identify this subgroup with \( \text{Sym}(n) \) (so we may write \( (i,j) \) in place of \( \pi_{(i,j)} \) and in general \( w \) for \( \pi_w \)).
The group generated by all the elementary diagonal matrices \( h_j(U) \) is the group \( H_n(R) \) of all invertible diagonal matrices, and the elementary permutation and diagonal matrices together generate the group of monomial matrices.

The group \( E_n(R) \) is \( \langle t_{i,j}(a) \mid i \neq j, a \in R \rangle \), generated by all elementary transvections, while the group generated by all three types of elementary matrices is \( GE_n(D) \).

As \( e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l} \) we immediately have

**Lemma.**

(a) \( t_{i,j}(a) t_{i,j}(b) = t_{i,j}(a+b) \) and especially \( t_{i,j}(a)^{-1} = t_{i,j}(-a) \).

(b) \( [t_{i,j}(a), t_{k,l}(b)] = t_{i,l}(ab)^{b_{i,k}} \), for \( i \neq l \).

Let \( U^+_n(R) \) be the subgroup of upper unitriangular matrices and \( U^-_n(R) \) be the corresponding subgroup of lower unitriangular matrices. We will usually write \( U_n(R) \) in place of \( U^+_n(R) \).

**Proposition.**

(a) \( U_n(R) = U^+_n(R) = \langle t_{i,j}(a) \mid a \in R, i < j \rangle \).

(b) \( U^-_n(R) = \langle t_{i,j}(a) \mid a \in R, i > j \rangle \).

**Proof.** (a) The proof is algorithmic (which is to say, by induction on \( n \)). Let \( A \) be upper unitriangular, so that \( a_{j,j} = 1 \) for all \( j \) and \( a_{i,j} = 0 \) for all \( i > j \). Set \( A = A^{(1)} \). Then let \( t_1 = \prod_{j=2}^n t_{1,j}(-a_{1,j}) \) and \( A^{(2)} = A^{(1)}t_1 \). The matrix \( A^{(2)} \) is upper unitriangular and additionally \( a_{1,1}^{(1)} = 1 \) is the only nonzero entry in its first row. We proceed to construct from each \( A^{(i)} \) an new matrix \( A^{(i+1)} = A^{(i)}t_i \) where \( t_i = \prod_{j=i+1}^n t_{i,j}(-a_{i,j}) \), the matrix \( A^{(i+1)} \) being upper unitriangular and having all nondiagonal entries 0 in its first \( i \) rows.

In particular \( A^{(n)} \) is the identity matrix. Therefore \( A \prod_{i=1}^{n-1} t_i = I \) and \( A = (\prod_{i=1}^{n-1} t_i)^{-1} \in \langle t_{i,j}(a) \mid a \in R, i < j \rangle \), as desired.

A similar argument gives (b).

**Proposition.** \( U_n(R) \) is nilpotent of class \( n - 1 \).

**Proof.** For each \( 1 \leq i \leq n \), let \( U_k = \langle t_{i,j}(a) \mid j - i \geq k \rangle \). In particular \( U_n = 1 \) and \( U_1 = U \) by the previous proposition. By Lemma (6.3) we always have \( [U_k, U_l] \leq U_{k+l} \). Therefore

\[
1 = U_n \leq U_{n-1} \leq \cdots \leq U_k \leq \cdots \leq U_1 = U
\]

is an ascending central series for \( U \). Indeed the same lemma tells us that \( U_{n-1} = Z(U) \); and, continuing in this fashion (by induction), we actually have the upper central series for \( U \). Its length is \( n - 1 \), so \( U \) has class \( n - 1 \). (See also Problem [6.38])

There are many proofs for Proposition (6.4), some perhaps more elegant than the one given here. But we have chosen a proof that shows its relation to
elementary matrix operations. We have shown that by a succession of elementary column operations (corresponding to right multiplication by \( t_{i,j}(b_{i,j}) \) for \( i < j \)) an upper unitriangular can be reduced to the identity. This means that the original matrix is the inverse of the product of the corresponding elementary transvections \( t_{i,j}(a) \).

Let us discuss elementary operations on rows and columns in terms of multiplication by elementary matrices. There are three types of elementary row operations that can be made on the matrix \( A \):

(i) Left multiplication by \( \pi_{(i,j)} \) switches rows \( i \) and \( j \) of \( A \);
(ii) Left multiplication by \( h_j(u) \) modifies row \( j \) of \( A \) by multiplying all its entries on the left by \( u \);
(iii) Left multiplication by \( t_{i,j}(a) \) adds \( a \) times row \( j \) of to row \( i \) of \( A \).

Similarly for elementary column operations:

(i) Right multiplication by \( \pi_{(i,j)} \) switches columns \( i \) and \( j \) of \( A \);
(ii) Right multiplication by \( h_j(u) \) modifies column \( j \) of \( A \) by multiplying all its entries on the right by \( u \);
(iii) Right multiplication by \( t_{i,j}(a) \) adds column \( i \) times \( a \) to column \( j \) of \( A \).

(6.6). Lemma. (Whitehead Lemma)

Let \( R \) be a ring with identity. For \( u, v \) units in \( R \) and \( a \in R \):

(a) \[
\begin{pmatrix}
0 & -u^{-1}
\end{pmatrix}
= \begin{pmatrix}
1 & 0
\end{pmatrix}
\begin{pmatrix}
1 & -u^{-1}
\end{pmatrix}
\begin{pmatrix}
1 & 0
\end{pmatrix};
\]
(b) \[
\begin{pmatrix}
u & 0
\end{pmatrix}
= \begin{pmatrix}
1 & 0
\end{pmatrix}
\begin{pmatrix}
0 & -u^{-1}
\end{pmatrix};
\]
(c) \[
\begin{pmatrix}
[u, v] & 0
\end{pmatrix}
= \begin{pmatrix}
(vu)^{-1} & 0
\end{pmatrix}
\begin{pmatrix}
u & 0
\end{pmatrix}
\begin{pmatrix}
0 & u^{-1}
\end{pmatrix}
\begin{pmatrix}
v & 0
\end{pmatrix};
\]
(d) \[
\begin{pmatrix}
u & 0
\end{pmatrix}
= \begin{pmatrix}
1 & a
\end{pmatrix}
\begin{pmatrix}
0 & -1
\end{pmatrix};
\]
(e) \[
\begin{pmatrix}
u^{-1}au & 0
\end{pmatrix}
= \begin{pmatrix}
u^{-1} & 0
\end{pmatrix}
\begin{pmatrix}
1 & a
\end{pmatrix}
\begin{pmatrix}
v & 0
\end{pmatrix};
\]
(f) \[
\begin{pmatrix}
u^{-1}au & 0
\end{pmatrix}
= \begin{pmatrix}
1 & a
\end{pmatrix}
\begin{pmatrix}
v & 0
\end{pmatrix}
\begin{pmatrix}
0 & 1
\end{pmatrix};
\]

A primary lesson the Whitehead Lemma[6.6] teaches is that almost all elementary operations can be accomplished using elementary transvections: the monomial operation \( \pi_{(i,j)}h_i(-1) \) and the diagonal operations \( h_i(u)h_j(u^{-1}) \) and \( h_i([u, v]) \) can all be realized by a succession of elementary transvections (using Lemma[6.6](a,b,c)); as matrices they belong to \( \text{E}_n(R) \). More specifically

(6.7). Proposition. Let \( U \) be the group of units of the ring \( R \) and \( \text{GL}_1(R) = \{ h_1(u) \mid u \in U \} \leq \text{GL}_n(R) \). Then \( \text{E}_n(R) \leq \text{GE}_n(R) = \text{E}_n(R)\text{GL}_1(R) \) with \( \text{GE}_n(R)/\text{E}_n(R) \) a quotient of \( U/U' \).
CHAPTER 6. MATRICES

**Proof.** By the Whitehead Lemma \([6.6]d,e\) the group \( \text{GL}_1(R) \) normalizes \( E_n(R) \).

We have

\[
\pi_{(i,j)} = \pi_{(i,j)} (h_i(-1)h_i(-1)) (h_1(-1)h_1(-1)) \\
= (\pi_{(i,j)}h_i(-1)) (h_1(-1)h_1(-1)) h_1(-1) \in E_n(R)\text{GL}_1(R)
\]

and

\[
h_i(u) = h_i(u) (h_1(u^{-1})h_1(u)) \\
= (h_i(u)h_1(u^{-1})) h_1(u) \in E_n(R)\text{GL}_1(R).
\]

Therefore \( E_n(R) \leq E_n(R)\text{GL}_1(R) = GE_n(R) \). Furthermore

\[
\text{GE}_n(R)/E_n(R)E_n(R)\text{GL}_1(R)/E_n(R) \simeq \text{GL}_1(R)/E_n(R) \cap \text{GL}_1(R)
\]

with \( \text{GL}_1(R) \simeq U \) and

\[
\text{GL}_1(R)' = \{ h_1([u,v]) \mid u,v \in U \} \leq E_n(R) \cap \text{GL}_1(R). \quad \square
\]

### 6.2 Bruhat decomposition

Gaussian elimination over the field \( F \) is designed to move, via a sequence of elementary row operations, from an arbitrary matrix \( A \) to one \( P \) that is in row echelon form:

- the nonzero rows of \( P \) are at its bottom, and, for each nonzero row \( i \) and minimal \( j \) with \( p_{i,j} \neq 0 \), all other entries \( p_{k,l} \) with \( i \leq k \) and \( l \leq j \) are equal to zero.

This is a canonical form result in the sense that Gaussian elimination seeks a relatively simple representative for the orbits of \( \text{GL}_n(F) \) in its left action on the set of matrices with \( n \) rows and entries from \( F \).

In this section we address a similar problem. We consider square matrices \( \text{Mat}_n(D) \) with entries from the division ring \( D \) and three different equivalence relations on this set:

- (i) Row equivalence, only allowing as elementary row operations the addition of a multiple of a row to a row higher in the matrix.

- (ii) Column equivalence, only allowing as elementary column operations the addition of a multiple of a column to a column to its right in the matrix.

- (iii) Row and column equivalence, only allowing as elementary operations the addition of a multiple of a row to a row higher in the matrix and the addition of a multiple of a column to a column to its right in the matrix.
That is, in view of Proposition (6.4), we look at the orbits of $\text{Mat}_n(D)$ under, respectively, left multiplication by elements of $U_n(D)$, right multiplication by elements of $U_n(D)$, and left and right multiplication by elements of $U_n(D)$.

The special nonzero $p_{ij}$ of echelon form are sometimes called the pivots. With that in mind we say that a row pivot of the nonzero row vector $\vec{v}$ is its first nonzero element. More precisely, the row pivot location is the smallest $j$ with $\vec{v}_j \neq 0$, the corresponding row pivot value then being $\vec{v}_j$. We say that a matrix is in row pivot form if every column contains at most one row pivot.

We define a column pivot similarly. The column pivot location of a nonzero column vector is the largest row index for which that column has a nonzero entry, the corresponding column pivot value. A matrix is then in column pivot form if every row contains at most one column pivot.

A partial monomial matrix is a square matrix that has at most one nonzero entry in each row and each column. It is additionally a monomial matrix if it has exactly one nonzero entry in each row and each column. Every partial monomial matrix can be written as the product of a permutation matrix and a diagonal matrix, with this factorization unique if the matrix is monomial. Equally well, every partial monomial matrix can be written as the product of a diagonal matrix and a permutation matrix, again uniquely when the matrix is monomial.

(6.8). **Lemma.** For the partial monomial matrix $P \in \text{Mat}_n(D)$, the following are equivalent:

1. $P$ is invertible.
2. $P$ has no zero row.
3. $P$ has no zero column.
4. $P$ is monomial. □

If a matrix is in row or column pivot form, then the corresponding pivot locations and values form a partial monomial matrix which we call the pivot matrix.

(6.9). **Proposition.** Let $P \in \text{Mat}_n(D)$ be a partial monomial matrix.

(a) $P U_n(D) = \{ M \mid M \text{ is in row pivot form with pivot matrix } P \}$.

(b) $U_n(D) P = \{ M \mid M \text{ is in column pivot form with pivot matrix } P \}$.

**Proof.** The first part actually includes Proposition (6.4) a) for division rings, and the proof by elementary column operations is essentially the same. The second part is similar, using elementary row operations. □

(6.10). **Lemma.** If the matrix $M \in \text{Mat}_n(D)$ is simultaneously in row pivot form and in column pivot form, then the row pivot locations are the same as the column pivot locations.

---

1If this were over a ring $R$, we would require further that these entries be units of $R$. 

CHAPTER 6. MATRICES

CHAPTER 6. MATRICES

**Proof.** The proof is by induction on \(n\) with nothing to prove when \(n = 1\) or \(M\) is a 0-matrix.

The leftmost nonzero column of \(M\) has exactly one nonzero entry, as otherwise it would contain two row pivots and \(M\) would not be in row pivot form. Delete from \(M\) that column and the row containing that pivot.

Certainly the remaining matrix is still in row pivot form. Furthermore, the only column pivot in the deleted row must have been that of the deleted column, since \(M\) was in column pivot form. Therefore the row and column pivots of the new matrix are those it inherits from \(M\), and we are done by induction. \(\Box\)

**Theorem.** For \(A \in \text{Mat}_n(D)\) there are \(U_1, U_2 \in \text{U}_n(D)\) and a partial monomial matrix \(P\) with \(A = U_1 PU_2\). Furthermore this determines \(P\) uniquely.

**Proof.** We first prove existence of such a factorization. The proof makes use of a “Gaussian elimination” style algorithm:

**Initialize.** \(j = 1; A^{(1)} = A\); label all locations in \(A^{(1)}\) open.

**Step \(j\).** If \(j = n + 1\), halt.

If there is no \(i\) with \((i, j)\) open and \(a_{i,j}^{(j)} \neq 0\), then

\[
\rho(j) = 0; t_j = 1; A^{(j+1)} = A^{(j)}; \\
\text{the closed locations of } A^{(j+1)} \text{ are the closed locations of } A^{(j)}; \\
j \rightarrow j + 1 \text{ and continue to the next step; }
\]

else

\[
\rho(j) = \text{the largest } i \text{ with } (i, j) \text{ open and } a_{i,j}^{(j)} \neq 0; \\
t_j = \prod_{i=1}^{\rho(j)-1} t_{i,\rho(j)} (-a_{i,j}^{(j)}(a_{\rho(j),j}^{(j)})^{-1}); \\
A^{(j+1)} = t_j A^{(j)}; \\
\text{the closed locations of } A^{(j+1)} \text{ are the closed locations of } A^{(j)} \\
\text{and the locations } (\rho(j), k) \text{ for } k \geq j; \\
j \rightarrow j + 1 \text{ and continue to the next step.}
\]

In words, we scan the columns of \(A\) from left to right. At each new column, we choose the lowest nonzero entry that is not in a row from which we have already chosen an entry. We then use elementary row operations to zero out all entries in the column above the chosen one.

**Claim:** All nonzero entries in columns \(1, \ldots, j - 1\) of \(A^{(j)}\) are in closed locations.

**Proof.** The proof is by induction on \(j\) with nothing to prove for \(j = 1\). Assume the claim is true for \(j\).

By its construction at Step \(j\), the only nonzero entries in column \(j\) of \(A^{(j+1)}\) are in closed locations. Additionally, since \(a_{\rho(j),j}^{(j)}\) was open, all \(a_{\rho(j),k}^{(j)}\) for \(k < j\) were open as well, hence 0 by induction. But then the various multiplications \(t_{i,\rho(j)}(*)\) and their product \(t_j\) leave
columns 1, \ldots, j - 1 unchanged from $A^{(j)}$ to $A^{(j+1)}$. In particular all locations in these columns that were nonzero, hence closed, in $A^{(j)}$ remain nonzero and closed in $A^{(j+1)}$.

This completes the proof of the claim.

In particular, all nonzero entries in $B = A^{(n+1)}$ are in closed locations. Therefore in a given row $i$, the only possible nonzero entries are $b_{i, \rho^{-1}(i)}$ and those to its right.

We conclude that $B$ is in row pivot form with pivots $b_{\rho(j), j}$ for those $j$ with $\rho(j) \neq 0$. Set $V = \prod_{j=1}^{n} t_j \in U_n(D)$ so that $VA = B$. By Proposition 6.9 there is a $U \in U_n(D)$ with $VA = BU$ for a partial monomial matrix $P$.

That is, $A = U_1 PU_2$ with $U_1 = V^{-1}$ and $U_2 = U$ both in $U_n(D)$, as desired.

Suppose $U_1 PU_2 = A = W_1 Q W_2$ with $Q$ partial monomial and $W_1, W_2 \in U_n(D)$. Then for $X_1 = W_1^{-1} U_1$ and $X_2 = W_2 U_2^{-1}$, both in $U_n(D)$, we have $X_1 P = C = Q X_2$. By Proposition 6.9 again, the matrix $C$ is in both row pivot and column pivot form with respective pivot matrices $P$ and $Q$. By Lemma 6.10 we have $P = Q$. That is, factorizations $A = U_1 PU_2$, with $U_1, U_2 \in U_n(D)$ and $P$ partial monomial, determine $P$ uniquely.

The matrices $U_1$ and $U_2$ of the theorem are not in general unique (think of the case $A = I$), but see Problem 6.41 below.

The $P$ of the theorem is then the partial monomial form $\text{pm}(A)$ of the matrix $A$. When $A$ and $P$ are invertible (as in Lemma 6.8) we also write $\text{mon}(A)$ for $P$, the monomial form of $A$. The matrix $\text{pm}(A)$ can always be written as $H_1 J$ and $J H_2$ with $H_1$ and $H_2$ uniquely determined diagonal matrices (the same, up to a permutation of the diagonal entries) and a permutation matrix $J$. When $A$ is invertible, $J$ is uniquely determined as the permutation matrix $\pi_\sigma$ for $\sigma = \rho^{-1}$, where $\rho$ is the permutation constructed during the proof of the theorem.

### Theorem 6.12.

Let $A \in \text{Mat}_n(D)$. The following are equivalent:

1. $A \in \text{GL}_n(D)$.
2. $\text{pm}(A) \in \text{GL}_n(D)$.
3. $A$ is left invertible.
4. $\text{RS}(A) = D D^{1:n}$.
5. $A$ is right invertible.
6. $\text{CS}(A) = D^{n:1}$.

**Proof.** Clearly (1) implies (3) and (5). Also (3) and (4) are equivalent as $\text{RS}(A) = D D^{1:n}$ if and only if there exists an $X$ with $XA = I$, since the rows of $X$ give the coefficients needed to write the canonical basis elements for $D D^{1:n}$ as linear combinations of the rows of $A$. Similarly (5) and (6) are equivalent.

Let $P = \text{pm}(A)$ with $A = U_1 PU_2$ for $U_1, U_2 \in U_n(D)$. If $A$ is invertible, then $P^{-1} = U_2 A^{-1} U_1$. If $P$ is invertible, then $A^{-1} = U_2^{-1} P^{-1} U_1^{-1}$. Therefore (1) and (2) are equivalent.
It remains to prove that (3) and (5) imply (2). Suppose
\[ X_1 Q X_2 \cdot Y_1 R Y_2 = I, \]
with \( X_1, X_2, Y_1, Y_2 \in U_n(D) \) and \( Q, R \) partial monomial matrices. Then \( QW R = Z \), with \( W = X_2 Y_1 \) and \( Z = X_1^{-1} Y_2^{-1} \) both invertible. Therefore partial monomial \( Q \) has no zero row and so by Lemma (6.8) is invertible, and similarly partial monomial \( R \) has no zero column and so is invertible. \( \square \)

(6.13). Corollary. Let \( A, B \in \text{GL}_n(D) \). Then \( AB \) is invertible if and only if \( A \) and \( B \) are invertible.

Proof. If \( A \) and \( B \) are invertible then \( (AB)^{-1} = B^{-1}A^{-1} \). If \( X \) is the inverse of \( AB \), then \(XA \) is a left inverse for \( B \) and \( BX \) is a right inverse for \( A \). \( \square \)

The following technical lemma is the basis for our verification of the Bruhat Decomposition in the next theorem and of the Dieudonné determinant in the next section.

(6.14). Lemma. Let \( W \in \text{Sym}(n) \), \( U \in U_n(D) \), and \( J = (j, j + 1) \in \text{Sym}(n) \) (where we identify \( \text{Sym}(n) \) with the permutation matrices of \( \text{GL}_n(D) \)). Then
\[ \text{mon}(WUJ) = \begin{cases} WJ & \text{or} \ W_{h_j(b)h_{j+1}(-b^{-1})} \text{ for some nonzero } b \in D. \end{cases} \]

Proof. Let \( k^W = j \) and \( l^W = j + 1 \).

The matrix \( A = WU \) is in row pivot form with \( \text{mon}(A) = W \). Then in \( AJ = WUJ \) we have switched columns \( j \) and \( j + 1 \) and left all else unchanged. In particular \( a_{i,j}^W \) remains a row pivot as long as \( (i, i^W) \) is not \( (k, j) \) or \( (l, j + 1) \). Therefore we expect pivots for rows \( \{k, l\} \) ultimately to be in columns \( \{j, j + 1\} \). That is, appropriate elementary operations should reveal \( \text{mon}(AJ) \) as \( WH \) or \( WJH \) for some \( H = h_j(b)h_{j+1}(c) \). The precise verification remains.

First suppose that \( k < l \) so that in rows \( k \) and \( l \) of \( A \) we have
\[ A_{k,l} = \begin{pmatrix} 0 & \cdots & 0 & 1 & a & \cdots & \ast & \cdots & \ast \\ 0 & \cdots & 0 & 0 & 1 & \cdots & \ast & \cdots & \ast \end{pmatrix} \]
with
\[ W_{k,l} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}. \]

Here we have separated the columns \( j \) and \( j + 1 \) from the others.

Therefore
\[ (AJ)_{k,l} = \begin{pmatrix} 0 & \cdots & 0 & a & 1 & \ast & \cdots & \ast \\ 0 & \cdots & 0 & 1 & 0 & \ast & \cdots & \ast \end{pmatrix}, \]
and for \( U_1 = t_{k,l}(-a) \)
\[ (U_1 AJ)_{k,l} = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 & \ast & \cdots & \ast \\ 0 & \cdots & 0 & 1 & 0 & \ast & \cdots & \ast \end{pmatrix}. \]
Thus $U_1(WUJ) = U_1AJ = WJU_2$, for some $U_2 \in U_n(D)$. That is,

$$\text{mon}(WUJ) = \text{mon}(U_1WUJ) = \text{mon}(WJU_2) = WJ,$$

one of the stated conclusions.

Next we suppose $l < k$ so that

$$W_{l,k} = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

with

$$A_{l,k} = \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 & * & \cdots & * \\ 0 & \cdots & 0 & 1 & b & * & \cdots & * \end{pmatrix}$$

and

$$(AJ)_{l,k} = \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & * & \cdots & * \\ 0 & \cdots & 0 & b & 1 & * & \cdots & * \end{pmatrix}.$$ 

If $b$ happens to be equal to 0, then $AJ = WJU_2$ for some $U_2 \in U_n(D)$, so that $\text{mon}(WUJ) = \text{mon}(AJ) = WJ$ again. Therefore it remains to consider the case $b \neq 0$. Let $U_1 = \nu_{l,k}(-b^{-1})$ so that

$$(U_1AJ)_{l,k} = \begin{pmatrix} 0 & \cdots & 0 & 0 & -b^{-1} & * & \cdots & * \\ 0 & \cdots & 0 & b & 1 & * & \cdots & * \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 & 0 & 1 & * & \cdots & * \\ 0 & \cdots & 0 & 1 & -b & * & \cdots & * \end{pmatrix} h_j(b)h_{j+1}(-b^{-1}).$$

As the group of diagonal matrices normalizes $U_n(D)$, this gives

$$U_1AJ = (WU_2)h_j(b)h_{j+1}(-b^{-1}) = Wh_j(b)h_{j+1}(-b^{-1})U_3,$$

for $U_2, U_3 \in U_n(D)$. Therefore

$$\text{mon}(WUJ) = \text{mon}(AJ) = \text{mon}(U_1AJ) = Wh_j(b)h_{j+1}(-b^{-1}),$$

the second of our two possibilities. \hfill \Box

(6.15). Theorem. (Bruhat decomposition)

Let $D$ be a division ring. Set $G = GL_n(D)$, $U = U_n(D)$, and $H = H_n(D)$. Next let $B = HU = UH$. Finally let $N$ be the subgroup of all monomial matrices in $G$ so that its subset $S = \{ s_j = (j, j + 1) \mid 1 \leq j \leq n - 1 \}$ generates $W = \text{Sym}(n)$, which we identify with the subgroup of all permutation matrices in $G$.

(a) (BN1) $G = BNB$ and $H = B \cap N \leq N$.

(b) (BN2) $N/H \cong W = \langle S \rangle$ and $s^2 = 1 \neq s$ for each $s \in S$.

(c) (BN3) For $w \in W$ and $s \in S$ we have $BwB.BsB \subseteq BwB \cup BwsB$.

(d) (BN4) For each $s \in S$ we have $sBs \neq B$. 

Proof.

(a) Certainly $H = B \cap N \leq N$. As $B = HU = UH$, also $G = UNU = BN B$ by Theorem (6.11).

(b) We have seen this before. For instance, it is a consequence of Theorem (5.2)(b).

(c) By Lemma (6.14)

\[ wUs \subseteq UwHU \cup UwsU. \]

As $B = HU = UH$, 

\[ BwUsB \subseteq BwB \cup BwsB. \]

Also $H \leq N$, so $Bw \geq Hw = wH$ and $BwU = BwB$. Therefore 

\[ BwB.BsB = BwBsB \subseteq BwB \cup BwsB. \]

(d) We have $sHs = H$ but $sUs \neq U$. For instance $t_{j,j+1}(a)^{(j,j+1)} = t_{j+1,j}(a)$. That is, 

\[
\begin{pmatrix}
  0 & 1 \\
  1 & 0 \\
\end{pmatrix}
\begin{pmatrix}
  1 & a \\
  0 & 1 \\
\end{pmatrix}
\begin{pmatrix}
  0 & 1 \\
  1 & 0 \\
\end{pmatrix} = 
\begin{pmatrix}
  1 & 0 \\
  a & 1 \\
\end{pmatrix}.
\]

\Box

6.3 The Dieudonné determinant

For the division ring $D$, let $D' = [D, D]$ be the derived subgroup of the multiplicative subgroup of $D$ and let $\tilde{D}$ be the commutative monoid whose elements are the orbits $\bar{d} = dD'$ for $d \in D$ with multiplication given by

\[ \bar{d}\bar{e} = (dD')(eD') = (de)D' = \bar{de} \]

That is, $\tilde{D}$ is the abelian group $D/D'$ extended to a monoid by adjoining the element $\bar{0}$ and declaring $0d = \bar{0} = 0d$ for all $\bar{d}$. As $D$ is a division ring, $\tilde{D}$ has no nonzero zero divisors.

Following Dieudonné, we shall define a map

\[ Ddet : \text{Mat}_n(D) \longrightarrow \tilde{D}, \]

the Dieudonné determinant. In this section we will prove:

(6.16). Theorem. The map $Ddet$ is a surjective multiplicative homomorphism from $\text{Mat}_n(D)$ to $\tilde{D}$ with $Ddet(A) \neq \bar{0}$ if and only if $A \in \text{GL}_n(D)$. If $D$ is a field, then $Ddet = \text{det}$, the usual determinant.

We define $Ddet$ in three stages:

(i) For the diagonal matrix $H$ with diagonal entries $h_i$, for $1 \leq i \leq n$, we set

\[ Ddet(H) = (\prod_{i=1}^{n} h_i)D' = \prod_{i=1}^{n} \bar{h}_i. \]
(ii) For the partial monomial matrix \( N = PH \) with \( P \) a permutation matrix and \( H \) a diagonal matrix, we set \( \text{Ddet}(N) = \text{sgn}(P) \text{Ddet}(H) \).

(iii) For arbitrary \( A \in \text{Mat}_n(D) \), we set \( \text{Ddet}(A) = \text{Ddet}(\text{pmon}(A)) \).

This is well-defined by Theorem \((6.11)\) with justification only needed for \( \text{Ddet}(N) \). In that case, the factorization \( N = PH \) is unique as long as \( N \) is invertible. For noninvertible \( N \) there can be more than one factorization \( P_1H_1 = N = P_2H_2 \); however \( \text{Ddet}(N) = \text{sgn}(P_1) \text{Ddet}(H_1) = \text{sgn}(P_2) \text{Ddet}(H_2) = 0 \), independent of the signs of \( P_1 \) and \( P_2 \).

We instead could have used any factorization \( N = KP \) of partial monomial \( N \), since in that case \( K = PHP^{-1} = H P^{-1} \) is a diagonal matrix with the same diagonal entries as \( H \), only permuted using \( P \). In particular

\[
\text{Ddet}(K) = \prod_{j=1}^{n} k_j D' = \prod_{j=1}^{n} h_{j,1} D' = \prod_{i=1}^{n} h_i D' = \text{Ddet}(H).
\]

Several parts of Theorem \((6.16)\) are immediate. Purely as a map \( \text{Ddet} \) is surjective since the diagonal matrix \( H \) with \( h_{1,1} = d \) and \( h_{i,i} = 1 \) for \( i \geq 2 \) has \( \text{Ddet}(H) = d \). Over fields \( D \) the determinant of a unitriangular matrix is 1; so

\[
\text{det}(A) = \text{det}(\text{pmon}(A)) = \text{Ddet}(\text{pmon}(A)) = \text{Ddet}(A)
\]

always, and \( \text{Ddet} \) recovers the usual determinant.

Invertibility is easy to verify.

\textbf{(6.17). Lemma.} The matrix \( A \in \text{Mat}_n(D) \) is noninvertible if and only if \( \text{Ddet}(A) = 0 \). In particular, \( \text{Ddet}(AB) = 0 \) if and only if \( \text{Ddet}(A) = 0 \) or \( \text{Ddet}(B) = 0 \).

\textbf{Proof.} By Theorem \((6.12)\) the noninvertible matrices \( A \) are precisely those with \( \text{pmon}(A) = PH \) for \( P \) a permutation and \( H \) a diagonal matrix having at least one 0 on its diagonal. That is, \( A \) is noninvertible if and only if \( \text{Ddet}(A) = 0 \). The rest follows from Corollary \((6.13)\). \( \Box \)

To complete our proof of the theorem, we are reduced to showing that \( \text{Ddet} \) is a multiplicative homomorphism. By the lemma we need only consider \( \text{GL}_n(D) \). As a starting point, we handle some easy cases.

\textbf{(6.18). Lemma.}

(a) If \( U \in \text{U}_n(D) \), then \( \text{Ddet}(AU) = \text{Ddet}(UA) = \text{Ddet}(A) \).

(b) If \( H \in \text{H}_n(D) \), then \( \text{Ddet}(AH) = \text{Ddet}(HA) = \text{Ddet}(A) \text{Ddet}(H) \).

\textbf{Proof.}

(a) This is immediate as \( \text{pmon}(AU) = \text{pmon}(UA) = \text{pmon}(A) \).
(b) Let $A = U_1 P K U_2$ with $U_1, U_2 \in U_n(D)$, $P$ a permutation matrix, and $K$ diagonal. As $H_n(D)$ normalizes $U_n(D)$, we have $AH = U_1 P K U_2 H = U_1 P K U_3$ for some $U_3 \in U_n(D)$; so $\text{pmon}(AH) = PKH$ and

$$D \det(AH) = D \det(PKH) = \text{sgn}(P) \prod_{i=1}^{n} k_i h_i D'$$

$$= \text{sgn}(P) \prod_{i=1}^{n} k_i D' \prod_{i=1}^{n} h_i D' = D \det(A) D \det(H).$$

Similarly $HA = HU_1 P K U_2 = U_4 H P K U_2$ so that $\text{pmon}(HA) = HPK = PHP K$ and

$$D \det(HA) = D \det(PHP K) = D \det(P) D \det(H P) D \det(K)$$

$$= D \det(P) D \det(H) D \det(K) = D \det(A) D \det(H)$$

by the previous calculation (used several times).

\[\Box\]

(6.19). Theorem. We have $D \det(A) D \det(B) = D \det(AB)$ for all $A, B \in \text{GL}_n(D)$. In particular the map $D \det: \text{GL}_n(D) \rightarrow D/D'$ is a surjective homomorphism from $\text{GL}_n(D)$ onto the abelian group $D/D'$.

Proof. By Theorem (6.11) we may write $A = U_1 HWU_2$ and $B = V_1 TKV_2$ for $U_1, U_2, V_1, V_2 \in U_n(D)$, $H, K \in H_n(D)$, and $W, T \in \text{Sym}(n)$ (identified with permutation matrices).

Write $T = \prod_{i=1}^{k} J_i$, where each $J_i$ is one of the transpositions $(j, j + 1)$ with $1 \leq j \leq n - 1$. In particular $D \det(T) = \text{sgn}(T) = (-1)^k$. Our proof is by induction on $k$, the case $k = 0$ being contained in the previous lemma. By that lemma, we also have:

$$D \det(A) = D \det(U_1 HWU_2) = D \det(H) \text{sgn}(W)$$

$$D \det(B) = D \det(V_1 TKV_2) = \text{sgn}(T) D \det(K)$$

$$D \det(AB) = D \det(U_1 HWU_2 V_1 TKV_2) = D \det(H) D \det(WU) D \det(K)$$

for $U = U_2 V_1 \in U_n(D)$. Therefore to prove $D \det(A) D \det(B) = D \det(AB)$ we must verify

$$D \det(WU) = \text{sgn}(W) \text{sgn}(T).$$

Assume $k \geq 1$ and write $WU = WU J \prod_{i=2}^{k} J_i$ for $J = J_1 = (j, j + 1)$. Then by Lemma (6.14) we have

$$WUJ = U_3 W JU_4 \quad \text{or} \quad WUJ = U_3 W h_j(b) h_{j+1}(-b^{-1}) U_4$$

for some $U_3, U_4 \in U_n(D)$ and some $0 \neq b \in D$.

In these two cases the previous lemma gives, respectively,

$$D \det(WUJ) = D \det(U_3 W JU_4) = D \det(WJ) = -\text{sgn}(W)$$
6.4. \((B,N)\)-PAIRS

and

\[
\text{Ddet}(WUJ) = \text{Ddet}(U_3Wh_j(b)h_{j+1}(-b^{-1})U_4) \\
= \text{Ddet}(W)b(-b^{-1}) = -\text{sgn}(W).
\]

That is, in both cases \(WUJ\) is a matrix \(C\) with \(\text{Ddet}(C) = -\text{sgn}(W)\).

Now by induction

\[
\text{Ddet}(WUT) = \text{Ddet}(WU \prod_{i=1}^{k} J_i) = \text{Ddet}(WU(J \prod_{i=2}^{k} J_i)) \\
= \text{Ddet}(C \prod_{i=2}^{k} J_i) = \text{Ddet}(C) \text{Ddet}(\prod_{i=2}^{k} J_i) \\
= -\text{sgn}(W)(-1)^{k-1} = \text{sgn}(W)\text{sgn}(T),
\]

as desired. \(\square\)

We let \(\text{SL}_n(D)\) denote the kernel of the Dieudonné determinant, the special linear group.

6.4 \((B,N)\)-pairs

The pair of subgroups \(B\) and \(N\) of the group \(G\) is a \((B,N)\)-pair provided:

\((BN1)\) \(\langle B, N \rangle = G\) and \(H = B \cap N \leq N\).

\((BN2)\) \(N/H = W = \langle S \rangle\) and \(s^2 = 1 \neq s\) for each \(s \in S\).

\((BN3)\) For \(w \in W\) and \(s \in S\) we have \(BwB BsB \subseteq BwB \cup BwsB\).

\((BN4)\) For each \(s \in S\) we have \(sBs \neq B\).

This is an important unifying concept (due to Tits), since many of the classical and Lie type groups possess a \((B,N)\)-pair. We already saw in Theorem \([6.15]\) that \(G = \text{GL}_n(D)\) is a group with a \((B,N)\)-pair consisting of \(B\), the upper triangular subgroup, and \(N\), the monomial subgroup. We shall find below in Theorem \([6.32]\) that its normal subgroup \(\text{SL}_n(D)\) does as well.

The subgroup \(B\) of \(G\) is a Borel subgroup of \(G\). The subgroup \(H\) is a Cartan subgroup, and the quotient \(W = N/H\) is the Weyl group of \(G\). These terms are usually extended to include any \(G\)-conjugates of \(B\) and \(H\). The subgroup \(N\) does not seem to have a common name. Note that the generating subset \(S\) of \(W\) is part of the data required to define a \((B,N)\)-pair. When we need to emphasize the specific generating set \(S\) being considered, we may write \(P_S\) in place of \(G\); see Lemma \([6.21]\) and the remarks that follow it.

\footnote{This notation and terminology are not used uniformly in the literature; see Hahn and O’Meara \([HaO89]\ p. 84].}
The (BN) axioms, as presented above, vary somewhat from the properties seen under Theorem (6.15). The most significant variance is that the group \( W \) is not required to be a subgroup of \( G \) but is instead defined to be the section \( N/H \), where by (BN1) the subgroup \( H \), now defined as \( B \cap N \), is normal in \( N \). This also means that we have abused notation under (BN3) and (BN4) by writing elements \( w, s \) of \( W \) as though they belong to \( G \). In both places this is unambiguous since the elements of \( W \) are actually cosets of the normal subgroup \( H \) in \( N \) whereas the subgroup \( B \) contains \( H \). The distinction is important. In particular in Theorem (6.32), where we see that the Dieudonné kernel \( \text{SL}_n(D) \) inherits a \((B,N)\)-pair \( B_0, N_0 \) from \( \text{GL}_n(D) \), it is not always the case that the extension of \( H_0 \) by \( W \) splits within \( N_0 \); see Problem (6.42).

As we shall see, the axiom (BN3) is very powerful. The double coset product \( BxB_0ByB = BxByB \) is always a union of double cosets, one of them clearly being \( BxyB \). We saw in Problem (2.39) that the product is always this one coset if and only if the subgroup \( B \) is normal. Axiom (BN3) then says that a significant portion of the time, the double coset product includes at most one further coset.

Axiom (BN3) appears to say more about right multiplication by members of \( S \) than left. However when we invert (BN3) and set \( u = w^{-1} \) we find an equivalent and lefthanded version:

\[(BN3^{-1}) \text{ For } u \in W \text{ and } s \in S \text{ we have } BsB.BuB \subseteq BuB \cup BsB.\]

Although (BN4) is usually presented in the form given here, there are at least two alternative and equivalent formulations (given (BN2) and (BN3)) that are of interest:

\[(BN4') \text{ For each } s \in S \text{ we have } s^{-1}Bs \neq B.\]
\[(BN4'') \text{ For each } s \in S \text{ we have } BsB.BsB = B \cup BsB.\]

Both of these state emphatically that \( B \) is not normal in \( G \). Were \( B \) to be normal, then we would always have \( BsBs = s^{-1}Bs = B \) and \( BsB.BsB = B \) with \( G/N = BN/B \approx N/B \cap N = W \).

\[ (6.20). \text{ Lemma. Let } B \text{ and } N \text{ form a } (B,N)\text{-pair in } G. \]
\[ (a) \text{ If } K = \ker_G(B), \text{ the core of } B \text{ in } G, \text{ then } B/K \text{ and } NK/K \text{ form a } (B,N)\text{-pair in } G/K. \]
\[ (b) \text{ For arbitrary } K, \text{ the subgroups } K \times B \text{ and } K \times N \text{ form a } (B,N)\text{-pair in } K \times G. \]

The last change from Theorem (6.15) to here is in (BN1) where \( G = BNB \) has been weakened to \( G = \langle B,N \rangle \); however:

\[ (6.21). \text{ Lemma. Let } B \text{ and } N \text{ form a } (B,N)\text{-pair in } G. \]
\[ (a) \text{ } G = BNB. \]
\[ (b) \text{ For the subset } T \text{ of } S \text{ set } W_T = (T) \leq W \text{ and then let } N_T \text{ be the preimage of } W_T \text{ in } N \text{ and } P_T = BNP_T. \text{ Then } P_T \text{ is a subgroup of } G \text{ within which } B \text{ and } N_T \text{ form a } (B,N)\text{-pair.} \]
6.4. \((B,N)\)-PAIRS

Proof. The first part follows from the second, since \(P_S = BNB = BNB\) is then a subgroup of \(G\) that contains the generating set \(\{B,N\}\).

The double coset union \(BN_TB\) is nonempty as it contains \(B\); it is closed under multiplication by \((\text{BN3})\) and induction; and it is closed under inverses as \(BtB = (BtB)^{-1}\) for all \(t \in T\). Therefore \(P_T\) is a subgroup, and all \(P_T\) contain \(B = P_0\). The \((B,N)\)-pair axioms for \(P_T\) follow directly from those for \(G\). □

The subgroups \(P_T\) of the lemma are the \textit{parabolic subgroups} containing \(B\), with the conjugates \(P_T^g\) being the parabolic subgroups containing the Borel subgroup \(B^g\). In Theorem \((6.28)\) below we shall find various properties of the parabolic subgroups including their characterization as the only subgroups of \(G\) containing a Borel subgroup. Observe that \(B = P_0\) and \(G = P_S\) (as promised above).

Throughout the rest of this section we will consider a specific nontrivial group \(G\) with \((B,N)\)-pair as given above.

In the Weyl group \(W\) generated by the elements of \(S\), we define the \textit{length} \(\ell_S(w)\) (sometimes just \(\ell(w)\)) of the element \(w\) to be the minimal \(l\) with \(w = \prod_{i=1}^l s_i\) for \(s_i \in S\). For instance \(\ell_S(1) = 0\) and \(\ell_S(s_i) = 1\). The length function has already made a cameo appearance in our proof of Theorem \((6.19)\).

(6.22). Lemma. If \(w, u \in W\) with \(BW = BuB\) then \(w = u\).

Proof. Assume \(\ell(w) \leq \ell(u)\). We induct on \(\ell(w)\). If this is 0, then \(w = 1_W\) and \(B = BW = BuB\). A coset representative \(w_u\) then belongs to \(B \cap N = H\), so also \(u = 1_W\).

Now assume \(\ell(w) \geq 1\) and write \(w = us\) with \(\ell(v) = \ell(w) - 1\) and \(s \in S\). Then

\[
BwB \subseteq BwBsB = BwBsB \subseteq BuB \cup BusB
\]

by \((\text{BN3})\). That is, the double coset \(BwB\) is either \(BuB\) or \(BusB\). By induction either \(v = u\) or \(v = us\). We cannot have \(v = u\) as

\[
\ell(v) = \ell(w) - 1 < \ell(u).
\]

Therefore \(v = us\), which is to say \(w = vs = (us)s = u\), as desired. □

(6.23). Proposition. Let \(w \in W\) and \(s \in S\).

(a) If \(\ell(ws) \geq \ell(w)\) then \(BwB.BsB = BwsB\).

(b) If \(\ell(ws) \leq \ell(w)\) then \(BwB.BsB = BwB \cup BwsB\).

Proof. Let \(w = \prod_{i=1}^m s_i\) with \(m = \ell(w)\) and all \(s_i\) in \(S\).

(a) We use induction on \(m\), the case \(m = 0\) being clear. Assume \(m \geq 1\), then set \(r = s_1\) and \(u = \prod_{i=2}^m s_i\) so that \(w = ru\) with \(\ell(u) = m - 1\).

We cannot have \(\ell(us) < \ell(u) = m - 1\) as then we would also have

\[
\ell(ws) = \ell(rus) \leq m - 1 < m = \ell(w),
\]
which is not the case by hypothesis. Therefore \( \ell(us) \geq \ell(u) = m - 1 \), so by induction \( BuBsB = BusB \) hence \( uBs \subseteq BusB \). Thus by (BN3⁻¹)

\[
BwBsB = Br(uBs)B \subseteq BrBusB \subseteq BrusB \cup BusB = BwsB \cup BusB.
\]

On the other hand, by (BN3)

\[
BwBsB \subseteq BwB \cup BwsB.
\]

Suppose \( BwBsB \cap BwB \neq \emptyset \) (that is, \( BwBsB \supseteq BwB \)). Then we must have \( BwB = BwsB \) or \( BwB = BusB \). Lemma (6.22) tells us that \( w = ws \) or \( w = us \), the first clearly false as \( s \neq 1 \) by (BN2). On the other hand, if \( w = us \), then \( ws = u \), and

\[
\ell(ws) = \ell(u) = m - 1 < m = \ell(w),
\]

against hypothesis. We conclude that \( BwBsB \cap BwB = \emptyset \) and so \( BwBsB = BwsB \).

(b) Here \( m = 0 \) is not possible. We now set \( s = sm \) and \( v = \prod_{i=1}^{m-1} s_i \) so that \( w = vs \) with \( \ell(v) = m - 1 \).

By (BN4⁰) \( BsBsB \cap BsB \neq \emptyset \), hence \( sBs \cap BsB \neq \emptyset \) and \( vsBs \cap vBsB \neq \emptyset \); so indeed

\[
BwBsB \cap BvBsB = BwBsB \cap BvBsB \neq \emptyset.
\]

As \( w = vs \),

\[
\ell(vs) = \ell(w) = m - 1 = \ell(v);
\]

so by (a), \( BuBsB = BwsB = BwB \) meets \( BwBsB \) nontrivially, hence is contained in \( BwBsB \).

(6.24). Corollary. For \( w \in W \) and \( s \in S \), we have \( \ell(ws) = \ell(w) \pm 1 \).

Proof. As \( (ws)s = w \), also \( \ell(w) - 1 \leq \ell(ws) \leq \ell(w) + 1 \). By the Proposition we cannot have \( \ell(w) = \ell(ws) \).

Recall that \( s \) is a coset of \( H \) in \( G \).

(6.25). Corollary. If \( \ell(ws) < \ell(w) \) then \( s \subseteq B^{-1}wB \).

Proof. We have \( wBs \cap BwB \neq \emptyset \), so \( Bs \cap w^{-1}BwB \neq \emptyset \) hence \( s \subseteq Bw^{-1}BwB \).

(6.26). Proposition.

Let \( w = \prod_{i=1}^{m} s_i \) with \( m = \ell_S(w) \), and set \( T = \{ s_i \mid 1 \leq i \leq m \} \). (Note that we may have \( |T| < m \).) Then \( \langle B,B^w \rangle = \langle B,w \rangle = P_T \).

Proof. Set \( s = sm \) and \( v = \prod_{i=1}^{m-1} s_i \) so that \( w = vs \) and \( ws = v \) with \( \ell(v) = m - 1 \).

By induction \( s_1, \ldots, s_{m-1} \subseteq \langle B,B^v \rangle \), so

\[
P_T = \langle B,s_1,\ldots,s_{m-1},s_m \rangle \leq \langle B,B^v,s \rangle.
\]
As \( \ell(ws) = \ell(v) = m - 1 = \ell(w) \), by Corollary (6.25)
\[
s \subseteq Bw^{-1}BwB \subseteq \langle B, B^w \rangle.
\]
Therefore as \( v = ws \)
\[
P_T \leq \langle B, B^w, s \rangle \leq \langle B, B^w \rangle \leq \langle B, w \rangle \leq P_T,
\]
and we have equality throughout. \( \square \)

(6.27). Corollary. If \( w \in W \) with \( w = \prod_{i=1}^{\ell_S(w)} s_i \) and \( w \subseteq P_T \) then \( s_i \in T \) for all \( i \). In particular \( \ell_T(w) = \ell_S(w) \), and for \( s \in S \) we have \( s \subseteq P_T \) if and only if \( s \in T \).

Proof. As \( T \subseteq S \) we must have \( \ell_T(w) \leq \ell_S(w) \). Write \( w = \prod_{i=1}^{\ell_S(w)} s_i \) with \( S_0 = \{ s_i \mid 1 \leq i \leq \ell_S(w) \} \subseteq S \) and \( w = \prod_{j=1}^{\ell_T(w)} t_j \) for \( T_0 = \{ t_j \mid 1 \leq j \leq \ell_T(w) \} \subseteq T \). Then by the proposition applied within \( G = P_S \), we have
\[
\langle B, w \rangle = P_{S_0} = \bigcup_{h \in W_{S_0}} BhB.
\]
On the other hand, the parabolic subgroup \( P_T \) also has a \( (B, N) \)-pair by Lemma (6.21)(b), and applied within \( P_T \) the proposition gives
\[
\langle B, w \rangle = P_{T_0} = \bigcup_{k \in (W_T)_{T_0}} BkB = \bigcup_{k \in W_{T_0}} BkB.
\]
In particular, for every \( s_i \in S_0 \), we have
\[
Bs_iB \subseteq \bigcup_{k \in W_{T_0}} BkB.
\]
By Lemma (6.22) we must have \( s_i \in W_{T_0} \) for all \( i \).

Now write \( s_i = \prod_{l=1}^{\ell_T(s_i)} r_l \) with \( r_l \in T \). Then by the proposition again (in \( P_T \) and in \( G \))
\[
Br_1B \subseteq \langle B, r_1, \ldots \rangle = \langle B, s_i \rangle = B \cup Bs_iB.
\]
Lemma (6.22) also applies again, now telling us that \( \ell_T(s_i) = 1 \) and \( s_i = r_1 \in T \).

We conclude that any minimal \( S \)-factorization of \( w \in P_T \) is in fact a minimal \( T \)-factorization. Especially \( \ell_T(w) = \ell_S(w) \). \( \square \)

(6.28). Theorem.

(a) If \( B \leq P \leq G \), then there is a \( T \subseteq S \) with \( P = P_T \).

(b) The maps \( T \mapsto W_T \) and \( T \mapsto P_T \) give isomorphisms of the lattice of subsets of \( S \) with, respectively, the lattice of subgroups of \( W \) generated by subsets of \( S \) and the lattice of subgroups \( P \) of \( G \) with \( B \leq P \leq G \).
Proof. (a) Let $B \leq P \leq G$ so that $P = \bigcup_{u \in U} BuB$ for some subset $U$ of $W$. As $P$ is a subgroup of $G$, we have $U^{-1} = U$ and $1 \in U$. Furthermore, for all $u, v \in U$ with $BuvB \subseteq BuB.BvB \subseteq P$, so $U$ is a subgroup of $W$.

For each $u \in U$ write $u = \prod_{i=1}^{\ell(u)} s_{u,i}$. Then set $S_u = \{ s_{u,i} \mid 1 \leq i \leq \ell(u) \}$ and $T = \bigcup_{u \in U} S_u$. From Proposition (6.26) we learn

$$P_T \supseteq P = \bigcup_{u \in U} BuB = \langle B, u \mid u \in U \rangle = \langle P_{S_u} \mid u \in U \rangle = P_T.$$ 

That is, $P = P_T$ and $U = W_T$.

(b) By Lemma (6.21) and Corollary (6.27) the map $W_T \mapsto P_T = BW_TB$ is a lattice isomorphism. By definition $P_{R \cup T} = \langle P_R, P_T \rangle$, and certainly $P_{R \cup T} \leq P_R \cap P_T$. But if $w \in P_R \cap P_T$, then $w \in P_R$ and $w \in P_T$, again by Corollary (6.27). Thus we have in turn a lattice isomorphism $T \mapsto P_T$ of the set of subsets of $S$ with the set of parabolic subgroups containing $B$.

(6.29). Theorem. Assume that $S$ is indecomposable; that is, it is not possible to write $S$ as the disjoint union of two nonempty subsets $S_1$ and $S_2$ for which $(s_1,s_2)^2 = 1$ for all $s_1 \in S_1$ and $s_2 \in S_2$. If $X \leq G$ then either $X \leq \ker_G(B)$ or $G = BX$.

Proof. By Theorem (6.28) the subgroup $BX$ is $P_T$ for some $T \subseteq S$. Here $T \supseteq \{ t \in S \mid BtB \cap X \neq \emptyset \}$ by Corollary (6.27). Indeed we have equality since $P_T = BX = BXB$ implies that every $t \in T$ is represented in $N_T$ by some $n_t \in X$. We have $T = \emptyset$ if and only if $X \leq \ker_G(B)$. Assume this is not the case.

Let $t \in T$ and $s \in S$ with $(st)^2 \neq 1$. By Corollary (6.27) $\ell_{\{s,t\}}(w) = \ell_S(w)$ for all $w$ in the nonabelian dihedral group $P_{\{s,t\}} = \langle s,t \rangle$. Especially

$$3 = \ell_S(sts) > \ell_S(st) > \ell_S(s) = 1.$$ 

Let $n_s$ be a representative for $s$ in $N = N_S$. As $X$ is normal in $G$ we have $n_s^{-1} n_t n_s \in X$ hence $Bn_s^{-1} n_t n_s B = BstsB \subseteq P_T$. Thus $sts \subseteq P_T$ and $\ell(s) = 3$, so Corollary (6.27) give $s \in T$. Indecomposability of $S$ now forces $T = S$, hence $BX = P_T = P_S = G$, as claimed.

A frequent application of this is the following:

(6.30). Corollary. Assume that $S$ is indecomposable. If $G$ is perfect and $B$ is solvable, then $G/\ker_G(B)$ is simple.

Proof. By the theorem, any normal $X$ not contained in $\ker_G(B)$ has $G = BX$. Then $G/X = BX/X \simeq B/B \cap X$, which is solvable. As $G$ is perfect, we conclude $B/B \cap X = 1$ hence $G = X$. Therefore $G/\ker_G(B)$ is simple.

6.5 Simplicity

Let $R_n(D)$ be the subgroup of nonzero scalar matrices in $GL_n(D)$. Next $Z_n(D)$ consists of those nonzero scalar matrices whose diagonal entries are from the
Theorem. Let $D$ be a division ring and $n \geq 2$ such that $(n, |D|) \neq (2, 2), (2, 3)$. Then all proper normal subgroups of $\text{SL}_n(D)$ are contained in $\text{Z}_n(D)$. Especially $\text{PSL}_n(D)$ is simple provided $(n, |D|) \neq (2, 2), (2, 3)$.

The two excluded cases are genuine exceptions with $\text{PSL}_2(\mathbb{F}_2) \simeq \text{Sym}(3)$ and $\text{PSL}_2(\mathbb{F}_3) \simeq \text{Alt}(4)$; see Corollary [8.8].

(6.32). Theorem. Let $D$ be a division ring and $n \geq 2$. Set $G_0 = \text{SL}_n(D)$, $U = U_n(D)$, and $H_0 = H_n(D) \cap G_0$. Next let $B_0 = H_0U = UH_0$ and $N_0$ be the subgroup of all monomial matrices having Dieudonné determinant 1. Finally set $S = \{s_j = (j, j + i) \mid 1 \leq j \leq n - 1\} \subseteq \text{Sym}(n) = W$, which we identify with the quotient $N_0/H_0$. Then $B_0$ and $N_0$ form a $(B, N)$-pair in the group $G_0$ with the same Weyl group $W = \langle S \rangle \simeq \text{Sym}(n)$.

Proof. This should be compared with the proof of Theorem [6.15].

Certainly $H_0 = B_0 \cap N_0 \leq N_0$. By Theorem [6.11] $\text{GL}_n(D) = UNU$. Since each element $u$ of $U$ has $\text{Det}(u) = 1$, those matrices with Dieudonné determinant 1 are precisely those of $UN_0U = B_0N_0B_0$, so we have (BN1).

Again (BN2) is a known property from Theorem [5.2]b) for the symmetric group. Within $\text{GL}_n(D)$ we have $N = N_0H$, so that coset representatives for elements of $W$ can always be chosen from $N_0$. To prove (BN4) of Theorem [6.15] we noted that $s_jU_s_j \neq U$, and with a suitable choice of coset representative for $s_j$ in $N_0$ (say $(j, j + 1)h_j(-1)$) this remains true in $G_0$.

It remains to check (BN3). By Lemma [6.14]

$$wUs \subseteq UwHU \cup UwsU$$

in $\text{GL}_n(D)$. Multiplying by $H_0$ we get

$$wB_0s \subseteq B_0wHU \cup B_0wsB_0,$$

at which point we can choose our coset representatives for $w$, $s$, and $ws$ all within $N_0$. As everything else then has Dieudonné determinant 1, this becomes

$$wB_0s \subseteq B_0wH_0U \cup B_0wsB_0,$$

hence

$$B_0wB_0, B_0sB_0 = B_0wB_0sB_0 \subseteq B_0wB_0 \cup B_0wsB_0,$$

as desired. □

It must be emphasized that the Weyl group $\text{Sym}(n)$ is given as a section of $\text{SL}_n(D)$, not a subgroup. The transpositions $(j, j + 1)$ are not in $\text{SL}_n(D)$. The coset representatives $(j, j + 1)h_j(-1)$ generate a supplement to $H_0 = H_n(D) \cap \text{SL}_n(D)$ in $N_0$, but the extension does not always split (see Problem [6.42]).
(6.33). Lemma. For \( n \geq 2 \) and \( B_0 \) as in Theorem (6.32) the core \( \ker_{\text{SL}_n(D)}(B_0) \) is equal to \( Z_n(D) \cap \text{SL}_n(D) \).

Proof. The Whitehead Lemma (6.6)(d) shows that any subgroup of \( B_0 \) (indeed of \( B \)) that is normalized by \( \text{SL}_n(D) \) must consist of scalar matrices. If the scalar \( u \) is not central, then Lemma (6.6)(f) with \( u = v \) and \( a \) an element of \( D \) not commuting with \( u \) tells us that the matrix \( uI \) does not belong to a normal subgroup of diagonal matrices. On the other hand, the subgroup \( Z_n(D) \) is indeed normal in \( \text{GL}_n(D) \).

(6.34). Proposition. For \( n \geq 2 \), \( \text{SL}_n(D) \) is the normal closure of \( U_n(D) \) in \( \text{SL}_n(D) \).

Proof. By the Whitehead Lemma (6.6)(d) the subgroup \( U_n^{-}(D) \) of lower unitriangular matrices is in the normal closure of \( U = U_{n}^{+}(D) = U_n(D) \) in \( \text{SL}_n(D) \). Therefore by Lemma (6.6)(a,b,c) the normal closure also contains generators for \( N_0 \), the subgroup of monomial matrices with Dieudonné determinant \( 1 \). Theorem (6.32) and (BN1) then tell us that the normal closure contains \( \langle U, N_0 \rangle = \langle B_0, N_0 \rangle = \text{SL}_n(D) \), as desired.

(6.35). Proposition. For \( n \geq 2 \), \( \text{SL}_n(D) = \text{SL}_{n}(D)' = \text{GL}_n(D)' \) provided \( (n, |D|) \neq (2, 2), (2, 3) \).

Proof. For \( n \geq 3 \), this is immediate by the previous proposition, Lemma (6.3)(b), and Proposition (6.7). For \( n = 2 \), let \( b \) be arbitrary in \( D \) and choose \( u \in D \) that commutes with \( b \) but \( u \notin \{0, 1, -1\} \). If \( b \) is not in \( Z(D) \), the center of the division ring, then we can choose \( u = b \). If \( b \) is in the center then everything commutes with \( b \), and we only need an element \( u \) of \( D \) that is not 0, 1, or -1. As long as \( |D| > 3 \), such \( u \) exist.

Then, for \( a = b(u^2 - 1)^{-1} \), by the Whitehead Lemma (6.6)(f)

\[
\begin{pmatrix}
0 & b \\
1 & 0
\end{pmatrix}
= \begin{pmatrix}
1 & -a + uau \\
0 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & a \\
0 & 1
\end{pmatrix} \cdot \begin{pmatrix}
u^{-1} & 0 \\
0 & u
\end{pmatrix}
\]

Therefore \( U_2(D) \leq \text{SL}_2(D)' \) provided \( |D| > 3 \). The previous proposition then shows that \( \text{SL}_2(D) = \text{SL}_2(D)' \).

Proof of Theorem (6.31).

Let \( G_0 = \text{SL}_n(D) \), and let \( X \) be a normal subgroup of \( G_0 \) not contained in \( \ker_{G_0}(B_0) \leq Z_n(D) \) (using Lemma (6.33)).

By Theorem (6.32) the subgroups \( B_0 \) and \( N_0 \) form a \((B, N)\)-pair in \( G_0 \), so by Theorem (6.29) we have \( G_0 = B_0X \). As \( U \leq B_0 \), we then find \( UX \leq G_0 \).

But \( G_0 \) is the normal closure of \( U \) within \( G_0 \) by Proposition (6.34). Therefore \( G_0 = UX \), and \( G_0/X = UX/X \simeq U/U \cap X \), a nilpotent hence solvable group by Proposition (6.5). By Proposition (6.35) the group \( G_0 = G_0' \) is perfect provided \((n, |D|) \neq (2, 2), (2, 3) \). In those cases we must have \( G_0/X \) trivial hence \( G_0 = X \). That is, any normal subgroup of \( G_0 \) not contained in \( \ker_{G_0}(B_0) \) is all of \( G_0 \). In particular \( G_0/\ker_{G_0}(B_0) \) is simple.
6.6 Problems

(6.36). Problem. Let \( a \) and \( b \) be noncommuting elements of the division ring \( D \).

(a) Prove that \( \begin{pmatrix} 1 & a \\ b & ab \end{pmatrix} \) is invertible in \( \text{Mat}_2(D) \).

(b) Prove that the transpose \( \begin{pmatrix} 1 & b \\ a & ab \end{pmatrix} \) is not invertible in \( \text{Mat}_2(D) \) but is invertible in \( \text{Mat}_2(D^{\text{op}}) \).

(6.37). Problem. Let \( G = \text{GL}_2(R) \), the group of \( 2 \times 2 \) invertible matrices with entries from the ring with identity \( R \). Set \( B = \{ (a \ b) \mid a,d \in U(R) \} \) and \( n = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). We have seen that for division rings \( R \) we have \( G = B \cup BnB \). Prove that \( G \neq B \cup BnB \) when \( R \) is not a division ring.

(6.38). Problem. Let \( R \) be a ring with identity. Let \( G \leq U_n(R) \) be block upper unitriangular with \( k \) blocks. This problem outlines a proof that \( G \) is nilpotent of class at most \( k - 1 \). In particular \( U_n(R) \) itself has class \( n - 1 \).

Suppose the blocks have dimensions, respectively, \( d_1, d_2, \ldots, d_k \), so that \( \sum_{i=1}^k d_k = n \). Set \( d_0 = 0 \). The “corners” of \( G \) are then the positions

\[ C = \{ (d_1, d_1 + 1), (d_1 + d_2, d_1 + d_2 + 1), \ldots, \\
(d_1 + \cdots + d_i, d_i + \cdots + d_i + 1), \ldots, \\
(d_1 + \cdots + d_{k-1}, d_1 + \cdots + d_{k-1} + 1) \} \]

Let \( U \) be the full block diagonal group with these corners. In a sequence of steps we show that \( U \) is nilpotent of class \( k - 1 \). Verify the following.

(a) By Gaussian elimination \( U \) is generated by the elementary subgroups

\[ E_{ij} = \{ I + \alpha e_{ij} \mid \alpha \in R \} \]

it contains. (Here \( e_{ij} \) is the standard matrix unit.) That is

\[ U = \langle E_{ij} \mid i \leq a \text{ and } b \leq j, \text{ for some } (a,b) \in C \rangle . \]

(b) For each corner \((a,b) \in C\),

\[ U_{ab} = \langle E_{ij} \mid a \leq i \text{ and } j \leq b \rangle \]

is abelian and normal in \( U \).

(c) By the previous two parts, \( U = \langle U_{ab} \mid (a,b) \in C \rangle \) is nilpotent of class at most \( |C| \); and so \( U \geq G \), nilpotent of class at most \( k - 1 \), as claimed. HINT: Problem [2.45]

(d) Set

\[ I_i = [d_0 + \cdots + d_{i-1}, d_0 + \cdots + d_i + 1] \]

and

\[ E^{ab} = \langle E_{ij} \mid i \in I_a, j \in I_b \rangle \leq U, \]

for \( 1 \leq a < b \leq k \). Then \([E^{ab}, E^{bc}] = E^{ac}\), and so

\[ [E^{1,2}, E^{2,3}, E^{3,4}, \ldots, E^{k-2,k-1}, E^{k-1,k}] = E^{1,k}. \]

In particular, \( U \) is not nilpotent of class less than \( k - 1 \); so it is nilpotent of class exactly \( k - 1 \).
(6.39). Problem. Let $R$ be a ring with identity. For $n \leq m$, we consider the group $\text{GL}_n(R)$ as embedded in the upper lefthand corner of $\text{GL}_m(R)$:

$$\text{GL}_n(R) \cong \begin{pmatrix} \text{GL}_n(R) & 0 \\ 0 & I_{m-n} \end{pmatrix} \leq \text{GL}_m(R).$$

We then let the stable linear group $\text{GL}(R)$ be the directed limit of the various $\text{GL}_n(R)$ for $n = 1, 2, 3, \ldots$. (so $\text{GL}(R)$ can be thought of as $\mathbb{N} \times \mathbb{N}$ invertible matrices, each of which differs from the identity matrix only in some finite dimensional upper lefthand corner.)

Always $E_n(R) \leq \text{GL}_n(R)$, and we let $E(R)$ be the corresponding directed limit subgroup of $\text{GL}(R)$. Prove:

(a) $E_n(R) = E_n(R)'$ for $n \geq 3$;
(b) $\text{GL}_n(R)' \leq E_{2n}(R)$ for all $n$;
(c) (The Whitehead Lemma) $\text{GL}(R)' = E(R) = E(R)'$.

Remark. Along the spectrum of things referred to as the Whitehead Lemma this is probably at the top while our Lemma (6.6) is probably at the bottom. But Whitehead’s insight here was that the simple calculations of that earlier lemma readily lead to this important result.

The abelian group quotient $\text{GL}(R)/E(R)$ is the Whitehead group of $R$ and is denoted $K_1(R)$. It is of central interest in the field of algebraic K-theory.

(6.40). Problem. In the group $E(R)$ of Problem (6.39), let $U^+(R)$ be the subgroup that is the directed limit of the upper unitriangular subgroups $U_n^+(R)$. Prove that $U^+(R)$ is a locally nilpotent group with trivial center.

(6.41). Problem. Let $D$ be a division ring and $A \in \text{GL}_n(D)$ with $\text{mon}(A) = HP$ for diagonal $H \in H_n(D)$ and permutation matrix $P$. Set

$$U_n^+(D)_P = \{ t_{i,j}(a) \mid a \in D, i < j, t^{P-1} > j^{P-1} \}.$$

Prove that $A = U_1 H P U_2$ with $U_1 \in U_n(D)$, $H \in H_n(D)$, $P \in \text{Sym}(n)$, and $U_2 \in U_n^+(D)_P$ all uniquely determined.

Hint: The permutation matrix $P$ is $\pi_{P-1}$, where $\rho$ is the permutation found while carrying through the algorithm of our proof for Theorem (6.11). That is, $P^{-1} = \pi_{\rho}$; so the condition $t^{P-1} > j^{P-1}$ is equivalent to $\rho(i) > \rho(j)$.

(6.42). Problem. Consider the group $N_0$ of monomial matrices of (Dieudonné) determinant 1 in $\text{GL}_{2m}(\mathbb{F}_3)$, and let its normal subgroup of diagonal matrices of determinant 1 be $H_0 \cong \mathbb{Z}_2^{2m-1}$. The quotient is then $N_0/H_0 \cong \text{Sym}(2m)$. Prove that this extension is nonsplit.

Hint: In each of $N_0$ and the split extension $H_0 \rtimes \text{Sym}(2m)$ (with the same action), let $A$ be the preimage of the subgroup $\langle (1,2) \rangle \ltimes \text{Alt}(3, \ldots, 2m)$ of $\text{Sym}(2m)$, and let $S$ be the preimage of the subgroup $\langle (1,2) \rangle$. Thus the normal subgroup $H_0$ has index 2 in $S$ which is itself normal in $A$. Consider the action of $A$ on the elements of order 2 in the coset $S \setminus H_0$.

(6.43). Problem. If $B$ and $N$ form a $(B, N)$-pair in the group $G$, prove that $Z(G)$ is contained in the core of $B$. 
Chapter 7

Projective Spaces

7.1 Projective spaces

For a vector space \( V \) over the division ring \( D \), the projective space \( \mathbb{P}_0V \) is the lattice of subspaces of \( V \) (excluding \( \{0\} \) and \( V \)). The rank of \( \mathbb{P}_0V \) is one less than the \( D \)-dimension of \( V \).

For any vector subspace \( W \) of \( V \), the projective space \( \mathbb{P}W \) is naturally contained in \( \mathbb{P}_0V \). Somewhat abusing terminology, we refer to both \( W \) and \( \mathbb{P}W \) as subspaces (members, elements) of \( \mathbb{P}V \) of rank \( d - 1 \), where \( d = \dim_D(W) \). Lemma (7.1) below allows this abuse. (The other deleted subspace \( \{0\} \) is the unique element of rank \(-1\).) The subspaces of \( \mathbb{P}V \) of rank 0 are projective points; those of rank 1 are projective lines, and those of rank 2 are projective planes, usually abbreviated to points, lines, and planes.\(^1\) If \( W \) has codimension 1 in \( V \), then \( \mathbb{P}W \) is a hyperplane of \( \mathbb{P}V \) (just as \( W \) is a hyperplane of \( V \)).

Two members \( u, w \) of \( \mathbb{P}_0V \) are incident, written \( u \sim w \), if one contains the other. (That is, subspaces \( U \) and \( W \) are incident if either \( U \leq W \) or \( U \geq W \).) In particular, two members of the same rank are incident if and only if they are equal.

There is a great deal of redundant information in the incidence relations of the projective space. For \( w \in \mathbb{P}V \) and \( 0 \leq i \leq \text{rank}(V) \), let

\[
\mathbb{P}_iV_w = \{ p \in \mathbb{P}_iV | p \sim w \}
\]

the shadow of \( w \) in \( \mathbb{P}_iV \). Once we realize that (b) follows directly from (a), we have

(7.1). Lemma.

(a) For \( w, v \in \mathbb{P}V \), \( \mathbb{P}_0V_w = \mathbb{P}_0V_v \) if and only if \( w = v \).

\(^1\)We avoid a common vector space terminology that identifies vectors as points, 1-spaces or 1-flats as lines, and 2-spaces or 2-flats as planes.
(b) For $0 \leq i \leq \text{rank}(V)$ and $w, v \in P_i V$, $P_i V = P_i V_v$ if and only if $w = v$.

(c) A subset $P$ of $P_0 V$ is equal to $P_0 V w$, for some subspace $w$, if and only if, for every projective line $\ell \in P_1 V$, we have either $|\ell \cap P| \leq 1$ or $P_0 V \ell \subseteq P$.

Part (a) of the lemma allows us, without much confusion, to abuse notation by identifying a subspace with the set of projective points contained within it. Then (b) says that $P$ is a subspace if and only if, for all lines $\ell$, either $|\ell \cap P| \leq 1$ or $\ell \subseteq P$; the subspaces are exactly the line-closed subsets of $P_0 V$.

For any subset $P$ of $P V$, the subspace generated by $P$, denoted $\langle P \rangle$, is the intersection of all subspaces containing $P$. So $\langle P \rangle$ is the smallest subspace that contains $P$. As mentioned above, we typically identify $\langle P \rangle$ with its shadow in $P_0 V$.

It is an easy consequence of Lemma (7.1) that every automorphism of the incidence system $\Pi(V) = (P_0 V, P_1 V)$ extends uniquely to a lattice automorphism of the projective space $P V$ and, conversely, any lattice automorphism of $P V$ restricts to an automorphism of $\Pi(V)$. For this reason, the automorphisms of $P V$ are usually called collineations and the full lattice automorphism group of $P V$ is called the collineation group of $P V$, denoted $\text{Coll}(P V)$.

### 7.2 The Fundamental Theorem of Projective Geometry

Recall that the morphisms in $\text{Vec}$ are semilinear maps. Thus $\Sigma = [\sigma, s]$ is a semilinear map from $D V$ to $E W$ provided:

(i) $\sigma$ is a homomorphism of $D$ into $E$;

(ii) $s$ is an additive homomorphism from $(V, +)$ to $(W, +)$;

(iii) for all $a \in D$ and $v \in V$ we have $(av)^\Sigma = a^\sigma v^s$.

Especially a semilinear map $[1_D, s]$ is a linear transformation from $D V$ to $D W$. Since $D$ is a division ring, $\sigma$ always realizes an isomorphism of $D$ with a subdi- vision ring of $E$.

**Theorem.** (Fundamental Theorem of Projective Geometry)

Let $D$ and $E$ be division rings with $V$ a $D$-space of dimension at least 3 and $W$ an $E$-space. Let $S : P_0 V \rightarrow P_0 W$ be a map on projective points with the “small rank” property that:

(\text{SmRk}) if $p, q, r \in P_0 V$, then $\text{rank}(p, q, r) = \text{rank}(p^S, q^S, r^S)$.

Then there is a semilinear transformation $\Sigma = [\sigma, s] : V \rightarrow W$ with $D^\sigma$ a subfield of $E$ isomorphic to $D$ (via $\sigma$) and $(v)^S = (v^s)$, for all vectors $v \in V$.

**Lemma.** Let $p, q \in P_0 V$. 

7.2. THE FUNDAMENTAL THEOREM OF PROJECTIVE GEOMETRY

(a) \( S : \mathbb{P}_0 V \rightarrow \mathbb{P}_0 W \) is injective.

(b) For \( t \in \mathbb{P}_0 W \) we have \( t \in [p^S, q^S] \cap \text{im}(S) \) if and only if there is an \( r \in \langle p, q \rangle \) with \( r^S = t \).

**Proof.**

\( \square \)

(7.4). Corollary.

(a) \( S : \mathbb{P}_1 V \rightarrow \mathbb{P}_1 W \) given by \( \langle p, q \rangle S = \langle p^S, q^S \rangle \) is injective.

(b) If \( \langle p, q \rangle \), and \( \langle r, s \rangle \) are lines of \( \mathbb{P}_1 V \) with \( t = \langle p, q \rangle \cap \langle r, s \rangle \), then \( t^S = \langle p, q \rangle^S \cap \langle r, s \rangle^S \).

**Proof.**

We further extend our definition of the map \( S \) by defining \( \langle u, v \rangle S \) to be \( \langle \langle u \rangle, \langle v \rangle \rangle S \) for \( u, v \in V \).

**Proof of the Fundamental Theorem of Projective Geometry** (7.2).

The proof is accomplished in a series of steps. We will use Property \((\text{SmRk})\), the lemma, and the corollary often and usually without reference.

Let \( \{x_0\} \cup \{ x_i \mid i \in \mathcal{I} \} \) be a \( D \)-basis for \( V \). Choose \( x_0' \in W \) with \( \langle x_0 \rangle S = [x_0'] \) and then for each \( i \in \mathcal{I} \) choose \( x_i' \in W \) such that:

1. \( \langle x_i \rangle^S = [x_i'] \) and
2. \( \langle x_0 + x_i \rangle^S = [x_0' + x_i'] \).

By Property \((\text{SmRk})\), any subset of \( \{x_0' \} \cup \{ x_i' \mid i \in \mathcal{I} \} \) of size up to three is linearly independent in \( W \) since its preimage in \( V \) is. This is not necessarily the case for subsets of size greater than three.

**Step (i).** For each \( i \in \mathcal{I} \) and \( d \in D \), define \( d^{(i)} \) by \( \langle x_0 + dx_i \rangle S = [x_0' + d^{(i)} x_i'] \). Then for all \( i, j \in \mathcal{I} \) and all \( d \in D \) we have \( d^{(i)} = \frac{[x_i']}{[x_0'] - [x_j']} \).

**Proof.** We first note that \( d \rightarrow d^{(i)} \) is well-defined. As \( \langle x_0 + dx_i \rangle S \in [x_0', x_i'] \), this only fails if \( \langle x_0 + dx_j \rangle S = [x_j'] \); but in that case \( \langle x_0, x_i \rangle^S = \langle x_0 + dx_i, x_i \rangle^S = [x_i'] \), which is not the case (by Property \((\text{SmRk})\)).

The claim of the step is obvious for \( i = j \) and true by choice (see above, in particular (2)) for \( d = 0, 1 \). Now assume \( i \neq j \) and \( 0 \neq d \neq 1 \).

Consider the three distinct lines

\[ \langle x_i, x_j \rangle, \langle x_0 + x_i, x_0 + x_j \rangle, \langle x_0 + dx_i, x_0 + dx_j \rangle, \]

all intersecting in the common point \( \langle x_i - x_j \rangle = \langle dx_i - dx_j \rangle \).
CHAPTER 7. PROJECTIVE SPACES

Step (ii). Consider the map \( \sigma : D \to E \) given by \( d^\sigma = d^{(i)} \), for any \( i \in I \). Then \( \sigma \) is a well-defined injection \( \sigma : D \to E \) with \( 0^\sigma = 0 \) and \( 1^\sigma = 1 \).

Proof.

By (i) the map \( \sigma \) is well-defined.

Step (iii). For all finite \( I \subseteq I \) and all \( d_i \in D \) for \( i \in I \), we have
\[
\langle x_0 + \sum_{i \in I} d_i x_i \rangle^S = \left[ x'_0 + \sum_{i \in I} d^\sigma_i x'_i \right].
\]

Proof.

Step (iv). For all finite \( I \subseteq I \) and all \( d_i \in D \) for \( i \in I \), we have
\[
\langle \sum_{i \in I} d_i x_i \rangle^S = \left[ \sum_{i \in I} d^\sigma_i x'_i \right].
\]

Proof.

Step (v). For all \( d,e \in D \) we have \( (de)^\sigma = d^\sigma e^\sigma \).

Proof.

Step (vi). For all \( d,e \in D \) we have \( (d+e)^\sigma = d^\sigma + e^\sigma \).

Proof.

Step (vii). For all finite \( H \subseteq \{0\} \cup I \) and all \( d_i \in D \) for \( i \in H \), we have
\[
\langle \sum_{i \in H} d_i x_i \rangle^S = \left[ \sum_{i \in H} d^\sigma_i x'_i \right].
\]

Proof.

Define the map \( s : (V,+) \to (W,+) \) by \( \left( \sum_{i \in I} d_i x_i \right)^s = \sum_{i \in I} d^\sigma_i x'_i \).

Step (viii). \( S \) is induced by the semilinear map \( \Sigma = [\sigma,s] : \text{for all } \langle v \rangle \in \mathbb{P}_0 V \text{ we have } \langle v \rangle^S = [v^\sigma] \).

Proof.

This completes our proof of the Fundamental Theorem of Projective Geometry (7.2).
Linear transformations

We often consider a matrix ring or group in terms of action on its natural module. Rings and groups of linear transformations provide the appropriate level of generality.

Many of the arguments are reminiscent of earlier arguments about the symmetric and alternating groups but are usually somewhat more difficult.

8.1 The dual space

For a vector space, the dual space $V^*$ is $\text{Hom}_D(V, D)$. Under pointwise action it is an abelian group. Indeed, assuming $V$ is a left $D$-space, the dual $V^*$ is a right $D$-vector space with operations given by

$$v(\lambda + \mu) = v\lambda + v\mu \quad \text{and} \quad v(\lambda k) = (v\lambda)k,$$

for all $\lambda, \mu \in V^*$, $v \in V$, and $k \in D$. The dual of a right $D$-space is in turn a left $D$-space.

(8.1). Lemma. Let $V$ be a $D$-space with basis $\{v_i \mid i \in I\}$. For $\lambda \in V^*$, set $\lambda_i = v\lambda$. Then, for each $v = \sum_{i \in I} a_i v_i \in V$, we have $v\lambda = \sum_{i \in I} a_i \lambda_i$. Indeed, the map $\lambda \mapsto (\lambda_i)_{i \in I}$ is an isomorphism of $V^*$ and $\prod_{i \in I} D$ as right $D$-spaces.

Proof. We have

$$v\lambda = \left(\sum_{i \in I} a_i v_i\right) \lambda = \sum_{i \in I} a_i (v_i \lambda) = \sum_{i \in I} a_i \lambda_i.$$

The map is directly checked to be a right $D$-space injection. Conversely, for any $(\lambda_i)_{i \in I} \in \prod_{i \in I} D$,

$$\left(\sum_{i \in I} a_i v_i\right) \lambda = \sum_{i \in I} a_i \lambda_i$$

defines a member $\lambda$ of $V^*$, since all but a finite number of the $a_i$ equal 0. \qed
CHAPTER 8. LINEAR TRANSFORMATIONS

(8.2). COROLLARY. If $V$ is finite dimensional, then
\[ \dim(V^*_D) = \dim_D(V^*_D) = \dim_D(DV) = \dim(DV). \]
In any event $|V^*| = |D|^\dim_D(V)$. \qed

While $V$ is a direct product of $|I|$ copies of $D$, the dual $V^*$ is a cartesian product of $|I|$ copies of $D$. For infinite $I$, we therefore expect the dual to bigger than the original space; and this is indeed the case. Especially, if $V$ is finite dimensional as left $D$-space, then $V^*$ has the same dimension as right $D$-space.

(8.3). PROPOSITION. Let $V$ be infinite dimensional over the division ring $D$.

(a) $|V| = \max(\dim_D(V), |D|)$.
(b) If $D$ is a field, then $\dim_D(V^*) = |D|^\dim_D(V) > \dim_D(V)$.
(c) $\dim_D(V^*) > \dim_D(V)$.
(d) $\dim_D(V^*) = |D|^\dim_D(V) > \dim_D(V)$.

Proof. \qed

On the other hand, for finite $|I|$ the dimensions of $V$ and $V^*$ are equal. Nevertheless there is no canonical isomorphism of $V$ and $V^*$, a fact most easily appreciated by remembering that $V$ is a left $D$-space while $V^*$ is a right $D$-space.

With each basis $B = \{v_i \mid i \in I\}$ of $V$, we can associate a nice subset $B^* = \{v^*_i \mid i \in I\}$ of $V^*$, given by
\[ v_i.v^*_i = 1 \quad \text{and} \quad v_j.v^*_i = 0 \quad \text{for} \quad i \neq j. \]
The dual set $B^*$ is always linearly independent. In particular, for finite $I$, it is a basis of $V^*$, the dual basis to $B$.

In the proof of Proposition [8.3] we have used the fact that there is little difference in properties between right $D$-spaces and left $D$-spaces. In particular, if $W$ is a right $D$-space, then we may equally well consider its dual $\text{Hom}_D(W,D) = W^*$ (which perhaps should be $^*W$). Similar properties hold but with right and left reversed, so $W^*$ is now naturally a left $D$-space. It is then natural to consider the double dual of $V$, the left $D$-space $V^{**} = (V^*)^*$.

Here there is a canonical embedding.

(8.4). LEMMA. $V$ is isomorphic to its image in $V^{**}$ under the map
\[ v \rightarrow v^{**} \quad \text{where} \quad v^{**}(\lambda) = v\lambda, \]
for all $v \in V$ and $\lambda \in V^*$. 

Proof. \qed
8.2 Matrix representation

The automorphism group of the division ring $D$ acts as a group of automorphisms on $GL_n(D)$ via

$$A \mapsto A^\alpha \text{ with } (A^\alpha)_{i,j} = (A_{i,j})^\alpha,$$

for each $\alpha \in \text{Aut}(D)$. This gives the semidirect product

$$\Gamma L_n(D) = \text{Aut}(D) \rtimes GL_n(D).$$

(8.5). Theorem. Let $V$ be a $D$-space of dimension $n$.

(a) $\text{End}_D(V) \simeq \text{Mat}_n(D)$.

(b) $\Gamma L_D(V) \simeq \Gamma L_n(D)$.

(c) $\Gamma L_D(V) \simeq GL_n(D)$.

Proof. As $GL_n(D)$ is the group of units in $\text{Mat}_n(D)$ and a normal subgroup of $\Gamma L_n(D)$, the last part is a consequence of either one of the preceding parts.

The result remains true for $V$ a free $R$-module of rank $n$. Furthermore, when matrices of infinite degree are defined appropriately, the result further extends to infinite $n$.

(8.6). Proposition. For $0 \neq r \in D$

(a) $r \mapsto R_r = (1, rI) \in GL_n(D)$ is an isomorphic embedding of $D^\times$ as the normal subgroup $R_n(D)$ of $GL_n(D)$.

(b) $r \mapsto L_r = (r, r^{-1}I) \in \Gamma L_n(D)$ is an isomorphic embedding of $D^\times$ as a normal subgroup $L_n(D)$ of $\Gamma L_n(D)$.

(c) $L_n(D) \cap R_n(D) = Z_n(D)$ consists of the nonzero central scalars. It is the center of $\Gamma L_n(D)$ and the centralizer of $\text{SL}_n(D)$ in $\Gamma L_n(D)$.

Proof.

Just as $\text{PSL}_n(D)$ was defined to be $\text{SL}_n(D)$ modulo its normal scalar subgroups, so $\text{PGL}_n(D)$ is $\Gamma L_n(D)$ modulo the group of scalars $L_n(D)$ and $\text{PGL}_n(D)$ is the image of its subgroup $GL_n(D)$.

8.3 The finite linear groups

(8.7). Theorem. Let $q = p^a$ for $p$ a prime and $a$ a positive integer.

(a) $|GL_n(q)| = N_{n,q} = \prod_{i=0}^{n-1} (q^n - q^i) = q^n \prod_{i=1}^{n} (q^i - 1)$. 


(b) \(|\text{SL}_n(q)| = |\text{PGL}_n(q)| = N_{n,q}/q - 1.\)

(c) \(|\text{PSL}_n(q)| = |\text{SL}_n(q)|/\gcd(n, q - 1).\)

(d) \(|\text{GL}_n(q)| = a|\text{GL}_n(q)|.\)

**Proof.** The group \(\text{GL}_n(q)\) is regular on the set of (ordered) bases of \(\mathbb{F}_q^n\), essentially by definition. But the number of such ordered bases is \(N_{n,q}\). The rest of the theorem follows directly. \(\square\)

(8.8). **Corollary.**

(a) \(\text{PSL}_2(2) = \text{GL}_2(2) \simeq \text{Sym}(3)\).

(b) \(\text{PGL}_2(3) \simeq \text{Sym}(4)\).

(c) \(\text{PSL}_2(3) \simeq \text{Alt}(4)\).

(d) \(\text{PSL}_2(4) \simeq \text{Alt}(5)\).

(e) \(\text{PSL}_2(5) \simeq \text{Alt}(5)\).

**Proof.** \(\text{PGL}_2(q)\) acts faithfully on the projective line, which consists of \(q + 1\) points. Its subgroup \(\text{PSL}_2(q)\) is generated by its Sylow \(p\)-subgroups (elementary transvections), where \(q = p^a\). In the last two parts \(\text{PSL}_2(q)\) is simple (by Theorem (6.31)) of order 60. For the last part, see also Problem (5.20). \(\square\)

### 8.4 Finitary linear transformations

The linear transformation \(g \in \text{GL}_D(V)\) is **finitary** provided the dimension of its commutator subspace \([V,g] = V(g - 1)\) is finite.

Let \(\text{FGL}_D(V)\) be the set of all finitary elements of \(\text{GL}_D(V)\).

(8.9). **Lemma.**

(a) \(g \in \text{GL}_D(V)\) is finitary if and only if its fixed point space \(C_V(g)\) has finite codimension in \(V\).

(b) For finitary \(g\), the codimension of \(C_V(g)\) is equal to the dimension of \([V,g]\).

(c) \(\text{FGL}_D(V)\) is a normal subgroup of \(\text{GL}_D(V)\).

**Proof.** The subspace \([V,g]\) is the image of the endomorphism \(g - 1\) while its kernel \(\ker(g - 1)\) is equal to \(C_V(g)\). This gives the first two parts immediately.

If \(C_V(g)\) and \(C_V(h)\) both have finite codimension, then so does \(C_V([g,h]) = C_V(g) \cap C_V(h)\). Thus \(\text{FGL}_D(V)\) is a subgroup. It is normal as \([V,g]^h = [V,g]^h\). \(\square\)
8.5. Transvections

A *transvection* is a linear transformation of $V$ with $V(t - 1)$ of dimension 1 and $V(t - 1)^2 = 0$.

**(8.10). Lemma.** Every transvection has the form

$$t(\lambda, x): v \rightarrow v + (v\lambda)x$$

for nonzero $\lambda \in V^*$ and $x \in V$ with $x\lambda = 0$.

**Proof.**

The *center* of $t(\lambda, x)$ is the 1-space $\langle x \rangle$, and its *axis* is the hyperplane $\ker \lambda = \ker(\lambda)$. (We allow the abuse of notation $t(0, x) = 1 = t(\lambda, 0)$, but we do not consider the identity to be a transvection.)

**(8.11). Proposition.** For $\lambda, \lambda_1, \lambda_2 \in V^*, x, x_1, x_2 \in V$, and $d \in D$:

(a) $t(\lambda d, x) = t(\lambda, dx)$. Indeed if the transvection $t(\lambda_1, x_1)$ is equal to $t(\lambda_2, x_2)$, then there is an $e \in D$ with $\lambda_1 e = \lambda_2$ and $e^{-1}x_1 = x_2$.

(b) $t(\lambda_1, x)t(\lambda_2, x) = t(\lambda_1 + \lambda_2, x)$.

(c) $t(\lambda_1, x_1)t(\lambda_2, x_2) = t(\lambda_1 x_1 + x_2)$.

(d) For $g = [\gamma, \theta] \in \Gamma L_D(V)$, we have $g^{-1}t(\lambda, x)g = t(g^{-1}\lambda, xg)$.

**Proof.** (a) comes from the previous lemma.

For (b) and (c) consider $t_1 = t(\lambda_1, x_1)$, $t_2 = t(\lambda_2, x_2)$ and $s = t_1t_2$. We have

$$v.s = v.t_1t_2 = v + (v\lambda_1)x_1 + (v\lambda_2)x_2 + (v\lambda_1)(x_1\lambda_2)x_2.$$  

In (b) and (c) we always have $x_1\lambda_2 = 0$, giving the results.

For (d), let $[\tau, h] \in \Gamma L(V)$ with associated automorphism $\tau$ of $D$. Then $[\tau, h]$ acts (semilinear on the left) on $\mu \in V^*$ via $v(h\mu) = ((vh)\mu)^{-1}$. (Check that this is a valid action!) Thus, for a $[\gamma, \theta]$ associated with, we have

$$v(g^{-1}t(\lambda, x)g) = ((vg^{-1})t(\lambda, x))g$$

$$= (vg^{-1} + ((vg^{-1})\lambda x))g$$

$$= vg^{-1}g + (v(g^{-1}\lambda))g^{-1}x$$

$$= v + (v(g^{-1}\lambda))xg$$

$$= v(t(g^{-1}\lambda, xg)).$$

Let $V$ be a $D$-spaces with subspaces $U$ of $V$ and $W$ of $V^*$. We let $T(W, U)$ be the subgroup of $\Gamma L_D(V)$ generated by all the $t(\lambda, v)$ with $\lambda \in W$, $v \in V$, and $u\lambda = 0$. In particular if $W$ is a 1-space of $V^*$ and $U$ a 1-space of $V$ with $UW = 0$, then $T(W, U)$ is a *transvection subgroup* of $\Gamma L_D(V)$. We will abuse this notation somewhat by writing $T(\lambda, u)$ for the transvection subgroup $T(W, U)$ when $\lambda$ spans the 1-space $W$ and $u$ spans the 1-space $U$. 
(a) If $W$ is a 1-space of $V^*$ and $U$ a 1-space of $V$, then $T(W, U) = \{ t(\lambda, u) \mid \lambda \in W, u \in U \}$ is a subgroup of $GL_D(V)$ that is isomorphic to $(D, +)$.
(b) The transvection subgroups $T(W, U)$ for $UW = 0$ are all conjugate in the group $T(V^*, V)$.

Proof. The first part follows immediately from the previous proposition.
We wish to prove $T(\lambda, x)$ and $T(\gamma, y)$ are conjugate. First assume that $\langle x \rangle \neq \langle y \rangle$, and choose a basis $\{x, y, z_1, z_2, \ldots\}$ for $V$. The hyperplane $\langle x - y, z_1, z_2, \ldots \rangle$ is $\ker \eta$, for some $\eta \in V^*$ with $\alpha = y\eta \neq 0$. Then, for $t = t(\eta, \alpha^{-1}(x - y))$, we have
$$y.t = y + (y\eta)\alpha^{-1}(x - y) = y + \alpha(\alpha^{-1}(x - y)) = x$$
Especially $T(\lambda, x)t = T(\delta, y)$, for some $\delta \in V^*$.
So it is enough to prove $T(\lambda, y)$ and $T(\gamma, y)$ conjugate in $T(V^*, V)$. We may assume $\lambda$ and $\gamma$ span different 1-spaces of $V^*$. Let $\{y = y_0, y_1, \ldots\}$ be a basis of $K = \ker \lambda \cap \ker \gamma$, and choose $u$ and $v$ with $\ker \lambda = \langle u, K \rangle$ and $\ker \gamma = \langle v, K \rangle$.
For $\mu \in V^*$ with $\ker \mu = \langle v - u, K \rangle$ and $\beta = v\mu \neq 0$, set $s = t(\mu, \beta^{-1}(v - u))$.
Then
$$u.s = u + (u\mu)\beta^{-1}(v - u) = u + \beta\beta^{-1}(v - u) = v.$$ Therefore $T(\lambda, y) = T(\gamma, y)^s$, as desired. \qed

(8.13). Lemma.
(a) If $t_1 = t(\lambda_1, x_1)$ and $t_2 = t(\lambda_2, x_2)$ with $\langle \lambda_1 \rangle \neq \langle \lambda_2 \rangle$ and $\langle x_1 \rangle \neq \langle x_2 \rangle$, then for $s = t_1t_2$, we have $V(s - 1) = \langle x_1, x_2 \rangle$. In particular, $s$ is not a transvection.
(b) Let $T$ be a subgroup of $GL_D(V)$ with $T^\# = T \setminus \{1\}$ completely composed of transvections. Then either there is a 1-space $W$ in $V^*$ with $T \leq T(W, V)$ or there is a 1-space $U$ in $V$ with $T \leq T(V^*, U)$.

Proof. In equation (*) from the proof of Proposition [8.11], if we first choose $v \in \ker \lambda_1 \setminus \ker \lambda_2$ then we find $x_2 \in V(s - 1)$. Next with $v \notin \ker \lambda_1$ we also have $x_1 \in V(s - 1)$.

The second part follows directly from the first. \qed

8.6 Problems

(8.14). Problem. This problem will (among other things) show again that the sign homomorphism on finite $\Sym(\Omega)$ (and hence on arbitrary $FSym(\Omega)$) is well-defined. Let $F$ be a field and $V$ the $\Sym(\Omega)$ permutation module $F\Omega$ with basis $\{e_\omega \mid \omega \in \Omega\}$ and action given by $e_\omega s = e_{\omega s}$. Let $n \geq 2$ and set $\Omega = \{1, 2, \ldots, n\}$ so that $\Sym(\Omega) = \Sym(n)$.

(a) Recall that for $g \in GL_F(V)$, we have defined $[V, g] = V(g - 1)$. Prove:
   (i) The subspace $W$ of $V$ is $g$-invariant with $g$ trivial on $V/W$ if and only if $W \geq [V, g]$.
   (ii) $[V, gh] \leq [V, g] + [V, h]$.

8.6. PROBLEMS

(b) For $g \in \text{Sym}(n)$, let $\ell(g)$ be the smallest number of transpositions with product $g$. Prove that $\dim_{\mathbb{D}}[V, g] \leq \ell(g)$.

(c) Prove that $\dim_{\mathbb{D}}[V, g] = \ell(g) = n - n_k = |\text{Supp}(g)| - c_k$ where $n_k$ is the number of cycles in $g$ (including cycles of length 1) and $c_k$ is the number of cycles in $g$ of length greater than 1. ( Hint: First prove that if $g$ is a $k$-cycle, then $\dim_{\mathbb{D}}[V, g] = \ell(g) = k - 1$.)

(d) For a transposition, prove that $\ell(gt) = \ell(g) \pm 1$.

(e) Prove that $\text{sgn}: g \mapsto (-1)^{\ell(g)} = (-1)^{\dim_{\mathbb{D}}[V, g]}$ is a homomorphism from $\text{Sym}(n)$ onto the multiplicative group $\pm 1$. (This is the sign homomorphism.)

(8.15). Problem. Let $(I, \leq)$ a totally ordered set. For the field $K$, let $\{ e_i \mid i \in I \}$ be the canonical basis of the $I$-tuple space $K^{(I, \leq)}$, defined to be $\oplus_{i \in I} Ke_i$. The upper triangular group $U_K(K^{(I, \leq)}) \leq \text{FGL}_K(K^{(I, \leq)})$ then consists of all linear transformations $g$ given by $e_i^g = e_i + \sum_{i<j} \alpha_{ij} e_j$ for all $i$, where for each $i$ only a finite number of the $\alpha_{ij}$ are nonzero. For instance, in Problems (6.38) and (6.40), we discussed $U_n(K) = U_K(K^{(\{1, n\}, \leq)})$ and $U^+(K) = U_K(K^{(\mathbb{Z}, \leq)})$.

(a) For infinite $I$, prove that $U_K(K^{(I, \leq)})$ is locally nilpotent with trivial center.

(b) Prove that $U_K(K^{(\mathbb{Q}, \leq)})$ is a perfect locally nilpotent group with trivial center.

(c) If $K$ is a field of characteristic $p > 0$, prove that $U_K(K^{(I, \leq)})$ is locally finite.

Remark. The group $U_K(K^{(\mathbb{Q}, \leq)})$ is in fact characteristically simple and is called a McLain group.
Chapter 9

Pairings, Isometries, and Automorphisms

The classical groups are linear groups that are isomorphism (isometry) groups of forms defined on the underlying space. The underlying concept is that of pairings of spaces.

9.1 Pairings

As before, \( D \) is a division ring. We let \( V = D V \), a left \( D \)-space, and \( W = W_D \), a right \( D \)-space. A pairing of \( V \) and \( W \) is a bilinear map \( m: V \times W \to D \). That is, for all \( u, v \in V \), \( w, y \in W \), and \( a, b \in D \):

(i) \( m(u + v, w) = m(u, w) + m(v, w) \);
(ii) \( m(u, w + y) = m(u, w) + m(u, y) \);
(iii) \( m(av, wb) = am(v, w)b \).

The motivating example is the canonical pairing \( m^{\text{can}} \) of \( V \) with its dual \( W = V^* \), where

\[ m^{\text{can}}(v, \lambda) = v\lambda, \]

for all \( v \in V \) and \( \lambda \in V^* \). If instead we start with a right \( D \)-space \( W \), then the canonical pairing is \( m^{\text{can}}: W^* \times W \to D \) given by \( m^{\text{can}}(\mu, w) = \mu w \).

Let \( U \) be a subspace of \( V \) and \( Y \) a subspace of \( W \). Then

\[ U^\perp = \{ w \in W \mid m(u, w) = 0, \text{ for all } u \in U \} \]

and

\[ Y^\perp = \{ v \in V \mid m(v, y) = 0, \text{ for all } y \in Y \}. \]

The pairing \( m \) is nondegenerate if \( V^\perp = 0 \) and \( W^\perp = 0 \). If \( U \leq V \) and \( Y \leq W \) with \( m|_{U \times Y} \) identically 0, then we call the pair \((U, Y)\) totally isotropic.
9.1. Lemma.

(a) For a pairing \( m: V \times W \rightarrow D \), the map \( \rho: w \mapsto m(\cdot, w) \) is a \( D \)-homomorphism of \( W \) into \( V^* \) and the map \( \lambda: v \mapsto m(v, \cdot) \) is a \( D \)-homomorphism of \( V \) into \( W^* \). Here \( \ker \rho = W^\perp \) and \( \ker \lambda = \perp W \).

(b) The pairing \( m: V \times W \rightarrow D \) is nondegenerate if and only if the map \( \rho: w \mapsto m(\cdot, w) \) is an injection of \( W \) into \( V^* \) and the map \( \lambda: v \mapsto m(v, \cdot) \) is an injection of \( V \) into \( W^* \).

Proof.

9.2. Corollary. For the pairing \( m: V \times W \rightarrow D \), set \( V^0 = V/\perp W \) and \( W^0 = W/V^\perp \). Then \( m^0: V^0 \times W^0 \rightarrow D \) given by \( m^0(v + \perp W, w + V^\perp) = m(v, w) \) is a well-defined nondegenerate pairing.

9.3. Lemma. Let \( m: V \times W \rightarrow D \) be a nondegenerate pairing. Let finite dimensional \( U \leq V \) and finite dimensional \( Y \leq W \).

(a) The codimension of \( U^\perp \) in \( W \) equals the dimension of \( U \), and \( \perp (U^\perp) = U \).

(b) The codimension of \( \perp Y \) in \( V \) equals the dimension of \( Y \), and \( \perp (\perp Y) = Y \).

(c) \( m|_{U \times Y} \) is nondegenerate if and only if \( \dim_D(U) = \dim_D(Y) \), \( V = U \oplus \perp Y \), and \( W = Y \oplus U^\perp \).

Proof.

9.4. Lemma. Let \( m: V \times W \rightarrow D \) be a nondegenerate pairing. Let finite dimensional \( U_0 \leq V \) and finite dimensional \( Y_0 \leq W \). Then there are \( U \) and \( Y \) with \( U_0 \leq U \leq V \), \( Y_0 \leq Y \leq W \), \( m|_{U \times Y} \) nondegenerate, and \( \dim_D(U) = \dim_D(Y) \leq \dim_D(U_0) + \dim_D(Y_0) \).

Proof. Let \( \dim_D(U_0) = k \) and \( \dim_D(Y_0) = l \).

Let \( Y_1 \) be a complement to \( (U_0 \cap \perp Y_0)^\perp \) in \( W \), so \( Y_1 \) has dimension \( d = \dim(U_0 \cap \perp Y_0) \leq k \) by Lemma [9.3]. Similarly let \( U_1 \) be a complement to \( \perp (Y_0 \cup U_0^\perp) \) in \( V \) of dimension \( e = \dim(Y_0 \cap U_0^\perp) \leq l \). We then set

\[ U = U_0 \oplus U_1 \quad \text{and} \quad Y = Y_0 \oplus Y_1, \]

both of dimension at most \( k + l \). We claim that \( m|_{U \times Y} \) is nondegenerate.

Let \( u = u_0 + u_1 \in U \) be a nonzero element with \( u_0 \in U_0 \) and \( u_1 \in U_1 \). We will find a \( y \in Y \) with \( m(u, y) \neq 0 \), and so demonstrate \( U^\perp \cap Y = 0 \). If \( u_1 \neq 0 \) then there is a \( y \in U_0^\perp \cap Y_0 \) with \( 0 \neq m(u_1, y) = m(u_0, y) + m(u_1, y) = m(u, y) \), so we may assume \( u = u_0 \in U_0 \).
9.1. PAIRINGS

If \( u_0 \notin U_0 \cap Y_0 \), then there is a \( y \in Y_0 \) with \( m(u,y) = m(u_0,y) \neq 0 \). Finally if \( 0 \neq u_0 \in U_0 \cap Y_0 \), then by nondegeneracy of \( m \) there is a \( y \in Y_1 \) with \( m(u,y) \neq 0 \).

We conclude that \( U_\perp \cap Y = 0 \) and similarly \( U \cap Y_\perp = 0 \), thus \( m|_{U \times Y} \) is nondegenerate. In particular \( \dim U = \dim Y \leq k + l = \dim U_0 + \dim Y_0 \).

A particular consequence of Lemma (9.3) is that for the finite dimensional space \( V = U \) there is an essentially unique nondegenerate pairing, the canonical one \( m^{\text{can}} \) with \( W = Y = V^* \). This is not the case for infinite dimensional \( V \).

As in Section 8.1, to each basis \( B \) of \( V \), we associate the dual subset \( B^* = \{ \lambda_y \mid y \in B \} \) of \( V^* \) given by \( x \lambda_y = \delta_{x,y} \) for \( x, y \in B \). Then \( B^* \) is linearly independent, and we let \( V^B \) be the subspace of \( V^* \) with basis \( B^* \). The restriction of the canonical pairing, \( m^B = m^{\text{can}}|_{V^B} \), is a nondegenerate pairing of \( V \) and \( V^B \).

For finite dimensional \( V \), the space \( V^B \) is all of \( V^* \) (by Corollary (8.2)) and so \( m^B = m^{\text{can}} \). For \( \dim_D(V^*) > \dim_D(V) = \dim_D(V^B) \)

by Proposition (8.3)(c); so the two nondegenerate pairings \( m^{\text{can}} \) and \( m^B \) of \( V \) are different in an essential way.

In general, we say that a pairing \( m: V \times W \rightarrow D \) is hyperbolic provided it admits dual bases: there are a basis \( V = \{ v_i \mid i \in I \} \) for \( V \) and basis \( W = \{ w_i \mid i \in I \} \) for \( W \) such that

\[
m(v_i, w_j) = \delta_{i,j}, \quad \text{for all } i, j \in I.\]

Thus each \( m^B \) is hyperbolic, essentially by definition. Clearly a necessary condition for the pairing to be hyperbolic is that it be nondegenerate with \( \dim V = |I| = \dim W \). This is not, in general, sufficient, although it is in in certain cases. We have remarked above that all nondegenerate pairings in finite dimension are hyperbolic. More surprising is that this remains true in countable dimension. The proof is a nice combination of a “back-and-forth” argument and a Gram-Schmidt style calculation.

(9.5). Theorem. If \( D \) and \( W \) both have countable dimension, then every nondegenerate pairing \( m: V \times W \rightarrow D \) is hyperbolic.

Proof. Choose the bases \( U = U_0 = \{ u_1, u_2, \ldots \} \) for \( V \) and \( X = X_0 = \{ x_1, x_2, \ldots \} \) for \( W \). We construct bases \( V = \{ v_1, v_2, \ldots \} \) for \( V \) and \( W = \{ w_1, w_2, \ldots \} \) for \( W \). At Step \( n \) we replace some \( u_i \in U \) by the vector \( v_n \in V \) and some \( x_j \in X \) by \( w_n \in W \). We do this in such a way that:

(i) \( U_n = \{ v_n \} \cup U_{n-1} \setminus \{ u_i \} \) is still a basis for \( V \) and \( X_n = \{ w_n \} \cup X_{n-1} \setminus \{ x_j \} \) is still a basis for \( W \);
(ii) \( m(v_a, w_b) = \delta_{a,b} \) for \( a, b \leq n \);
(iii) all \( u_i \) of \( U \) and \( x_j \) of \( X \) are eventually replaced.
The result of this process is then a pair of dual bases $\mathcal{V} = U_\infty$ for $V$ and $\mathcal{W} = X_\infty$ for $W$ that reveal $m$ as hyperbolic.

We describe Step $n$ precisely. If $n$ is odd, let $i$ be the smallest index $i$ with $u_i$ not yet replaced. Set

$$v_n = u_i - \sum_{k=1}^{n-1} m(u_i, w_k)v_k,$$

and let $V_n = \langle v_1, \ldots, v_n \rangle$ of dimension $n$. By Lemma [9.4] every element of $V_n^*$ can be induced by some element of $W$. Let $j$ be minimal subject to the condition that the linear functional $\rho_j: V_n \rightarrow D$, given by $\rho_j(v) = m(v, x_j)$, is not induced by any element of $W_{n-1} = \langle w_1, \ldots, w_{n-1} \rangle$. Set

$$w_n = x_j - \sum_{k=1}^{n-1} w_km(v_k, x_j).$$

If instead $n$ is even, we first replace $x_j$ and only then replace $u_i$. That is, we first choose $j$ to be the smallest index for which $x_j$ has not already been replaced. We then define $w_n$ according to the formula given above. Next we set

$$W_n = \langle w_1, \ldots, w_n \rangle$$

and choose $u_i$ with $i$ minimal subject to the linear functional $\lambda_i: W_n \rightarrow D$, given by $\lambda_i(w) = m(u_i, w)$, not being induced by any element of $V_{n-1}$. (Again Lemma [9.4] guarantees that such an $i$ exists.) The element $v_n$ is then defined as above.

Whether $n$ is even or odd, these choices of $v_n$ and $w_n$ certainly give (i). Also Step $n - 1$ provides us with (ii) for $a, b < n$.

For $b < n$

$$m(v_n, w_b) = m(u_i - \sum_{k=1}^{n-1} m(u_i, w_k)v_k, w_b)$$

$$= m(u_i, w_b) - \sum_{k=1}^{n-1} m(u_i, w_k)m(v_k, w_b) = 0.$$

Similarly, for $a < n$

$$m(v_a, w_n) = m(v_a, x_j - \sum_{k=1}^{n-1} w_km(v_k, x_j))$$

$$= m(v_a, x_j) - \sum_{k=1}^{n-1} m(v_a, w_k)m(v_k, x_j) = 0.$$

Depending upon whether $n$ is odd or even, our choice of $j$ or $i$ guarantees that $m(v_n, w_n) = d$ is nonzero, so to complete (ii) at Step $n$ we only need to replace one of $v_n$ or $w_n$ with its multiple by the scalar $d^{-1}$.

Finally, the element $u_i$ will be replaced by the $i^{th}$ odd step if not earlier, while $x_j$ will have been replaced by the $j^{th}$ even step. Thus both $u_k$ and $x_k$ are replaced by the time we have completed Step $2k$, giving (iii) and the theorem.

$\square$
9.2. THE ISOMETRY GROUPS OF PAIRINGS

(9.6). **Proposition.** For spaces $D V$ and $W_D$ there exists a nondegenerate pairing $m: V \times W \rightarrow D$ if and only if $\dim W \leq \dim V^*$ and $\dim V \leq \dim W^*$.

**Proof.** Necessity follows from Lemma (9.1)(b).

For the other direction, we may assume $\dim V \leq \dim W$. Choose a basis $B$ of $V$, and let $V^B$ be the subspace of the same dimension in $V^*$ that was constructed above. By hypothesis there is a vector space injection $\theta: W \rightarrow V^*$ with $V^B \leq W^\theta$. Define $m: V \times W \rightarrow D$ by $m(v,w) = v(w^\theta)$. Then $V^\perp = 0$ as $\theta$ is injective and $W^\perp = 0$ as $m^B: V \times V^B \rightarrow D$ is nondegenerate.

9.2 The isometry groups of pairings

Let $g$ be an isomorphism in $\text{Hom}_D(V,V')$ and $h$ an isomorphism in $\text{Hom}_D(W,W')$. Then for every pairing $m: V \times W \rightarrow D$ we have a pairing $m^{(g,h)}: V' \times W' \rightarrow D$ given by $m^{(g,h)}(v',w') = m(v,g^{-1}h^{-1}w')$.

The pair $(g,h)$ is then an equivalence of the pairings $(V,W,m)$ and $(V',W',n)$ (for $n = m^{(g,h)}$), which are said to be isometric. Again, this is a formalization of the feeling that there is no essential difference between the pairings $(V,W,m)$ and $(V',W',n)$.

As a direct consequence of Lemma (9.1) we have:

(9.7). **Lemma.** Let $m: V \times W \rightarrow D$ be a nondegenerate pairing. Then there are subspaces $W^\rho$ of $V^*$ and $V^\lambda$ of $W^*$ with $(V,W,m)$ isometric to $(V^\rho,W^\rho,m^\rho)$ and $(V^\lambda,W,m^\lambda)$, where $m^\rho$ and $m^\lambda$ are the restrictions to $W^\rho$ and $V^\lambda$ of the canonical pairings $(V,V^*,m^\text{can})$ and $(W^*,W,m^\text{can})$.

An isometry (rather than self-isometry) of the pairing $m: V \times W \rightarrow D$ is then a self-equivalence—an element

$$(g,h) \in \text{GL}(D V) \times \text{GL}(W_D)$$

with $m(v,w) = m(v,g,h,w)$,

for all $(v,w) \in V \times W$. This can be viewed as the stabilizer of $m$ in the (right) action of $\text{GL}(D V) \times \text{GL}(W_D)$ on the abelian group of pairings $\text{Pair}_D(V,W)$ ($\simeq \text{Hom}_D(V,W^*)$) given by $m \mapsto m^{(g,h)}$. Under our convention of right action we have

$$(g_1,h_1)(g_2,h_2) = (g_1g_2,h_2h_1)$$

in $\text{GL}(D V) \times \text{GL}(W_D)$. The subgroup of this group consisting of all isometries of $m$ (with this product) will be denoted $\text{GL}_D(V,W,m)$.

(9.8). **Lemma.** Let $m: V \times W \rightarrow D$ be a nondegenerate pairing, and let $(g,h) \in \text{GL}_D(V,W,m)$.
(a) \( C_W(h) = V(g - 1)^\perp \) and \( C_V(g) = (h - 1)W \).

(b) \( g = 1 \) if and only if \( h = 1 \).

(c) \( g \in \text{FGL}_D(V) \) if and only if \( h \in \text{FGL}_D(W) \). In this case \( \deg_V(g) = \deg_W(h) \).

**Proof.** For all \( v \in V \) and fixed \( w \),
\[
m(v(g - 1), w) = m(vg, w) - m(v, w) = m(vg, hw) = m(vg, (1 - h)w).
\]
Therefore \( w \in V(g - 1)^\perp \) if and only if \( w \in C_W(h) \). This gives (a).

Part (b) is an immediate consequence of (a). For (c) assume that \( \deg_V(g) \) is finite. Then
\[
\deg_V(g) = \dim_D(V(g - 1)) = \text{codim}_D(V(g - 1)^\perp) = \text{codim}_D(C_W(h)) = \dim_D((h - 1)W) = \deg_W(h),
\]
as desired.

**Corollary.** Let \( m: V \times W \rightarrow D \) be a nondegenerate pairing, and \( G = \text{GL}_D(V, W, m) \) its isometry group.

(a) The restriction map \( (g, h) \mapsto g \) is an injection of \( G \) into \( \text{GL}_D(V) \).

(b) The restriction map \( (g, h) \mapsto h^{-1} \) is an injection of \( G \) into \( \text{GL}_D(W) \).

**Proof.** Given that \((g_1, h_1)(g_2, h_2) = (g_1g_2, h_2h_1)\) in \( G \), this is immediate from Lemma \([9.8]\) b). □

Each element \( g \in \text{GL}_D(V) \) acts naturally on \( V^* \) via
\[
v(g\mu) = (vg)\mu,
\]
for all \( v \in V \) and \( \mu \in V^* \). In particular, for all \( g \in \text{GL}_D(V) \) we have \((g, g^{-1}) \in \text{GL}_D(V, V^*, m_{\text{can}})\). This remark and the previous two results immediately give

**Corollary.**

(a) \( \text{GL}_D(V) = \text{GL}_D(V, V^*, m_{\text{can}})|_V \).

(b) \( \text{FGL}_D(V) = \text{FGL}_D(V, V^*, m_{\text{can}})|_V \).

**Proof.** □
9.2. THE ISOMETRY GROUPS OF PAIRINGS

(9.11). **Proposition.** If \( m: U \times Y \rightarrow D \) is a nondegenerate pairing with \( U \) and \( Y \) finite dimensional, then

\[
\text{GL}_D(U, Y, m) \cong \text{GL}_D(U, Y, m)_{|U} = \text{GL}_D(U) \cong \text{GL}_D(U)
\]

and

\[
\text{GL}_D(U, Y, m) \cong \text{GL}_D(U, Y, m)_{|Y} = \text{GL}_D(Y) = \text{GL}_D(Y).
\]

**Proof.** We have

\[
\text{GL}_D(U, Y, m) \cong \text{GL}_D(U, Y, m)_{|U} \quad \text{by Corollary (9.9)}
\]

\[
\cong \text{GL}_D(U, Y^\vee, m_{\text{can}}|_{U \times Y})_{|U} \quad \text{by Lemma (9.7)}
\]

\[
= \text{GL}_D(U, U^\perp, m_{\text{can}}|_U) \quad \text{by Corollary (8.2)}
\]

\[
= \text{GL}_D(U) \quad \text{by Corollary (9.10)}.
\]

Similarly \( \text{GL}_D(U, Y, m) \cong \text{GL}_D(Y) \). \( \Box \)

By Theorem (8.5) there is an isomorphism of \( \text{GL}_n(D) \) and \( \text{GL}_D(U) \) for \( n = \dim_D(U) \). Different isomorphisms are related by a change of basis. In particular, via any such isomorphism the Dieudonné determinant is well-defined on \( \text{GL}_D(U) \) and so also on \( \text{GL}_D(U, Y, m) \) (using the proposition). Let \( \text{SL}_D(U) \) and \( \text{SL}_D(U, Y, m) \) be the images in \( \text{GL}_D(U) \) and \( \text{GL}_D(U, Y, m) \) of \( \text{SL}_n(D) \), the kernel of the Dieudonné determinant. Especially by Theorem (6.31) we have \( \text{SL}_D(U, Y, m) \) quasisimple and equal to \( \text{GL}_D(U, Y, m)' \) provided \( (n, |D|) \neq (2, 2), (2, 3) \).

Let the *finitary general linear group* \( \text{FGL}_D(V, W, m) \) consist of those elements \((g, h) \in \text{GL}_D(V, W, m)\) with \( g \in \text{FGL}_D(V) \) and \( h \in \text{FGL}_D(W) \).

(9.12). **Proposition.** For the nondegenerate pairing \( m: V \times W \rightarrow D \), the group \( \text{FGL}_D(V, W, m) \) is the directed limit of its subgroups

\[
G_{U, Y} \cong \text{GL}_D(U, Y, m|_{U \times Y}) \cong \text{GL}_D(U)
\]

for \( U \) finite dimensional in \( V \), \( Y \) finite dimensional in \( W \), and \( m|_{U \times Y} \) non-degenerate. Here the element of \((g, h) \in G_{U, Y}\) corresponding to \((g_0, h_0) \in \text{GL}_D(U, Y, m|_{U \times Y})\) is defined to act on \( V = U \oplus U^\perp \) according to

\[
g|_U = g_0 \quad \text{and} \quad U^\perp (g - 1) = 0
\]

and on \( W = Y \oplus U^\perp \) via

\[
h|_Y = h_0 \quad \text{and} \quad (h - 1)U^\perp = 0.
\]

**Proof.** By Lemma (9.3)(c), the groups \( G_{U, Y} \) with \( g \) and \( h \) acting as described are subgroups of \( \text{FGL}_D(V, W, m) \) and are isomorphic to \( \text{GL}_D(U) \) by the previous proposition.
Each \((g,h) \in \text{FGL}_D(V,W,m)\) is in some \(G_{U,Y}\) by Lemma \((9.4)\) with \(U_0 = V(g-1)\) and \(Y_0 = (h-1)W\).

Furthermore, if \(U_1, U_2, Y_1, Y_2\) are finite dimensional with both \(m|_{U_1 \times Y_1}\) and \(m|_{U_2 \times Y_2}\) nondegenerate, then a second application of Lemma \((9.4)\) now with \(U_0 = U_1 + U_2\) and \(Y_0 = Y_1 + Y_2\), provides a finite dimensional and nondegenerate pairing \(m|_{U \times Y}\) with \((G_{U_1,Y_1},G_{U_2,Y_2}) \leq G_{U,Y}\). Therefore the set of all \(G_{U,Y}\) is indeed directed with \(\text{FGL}_D(V,W,m)\) as its directed limit.

\((9.13)\) Theorem. For the nondegenerate pairing \(m: V \times W \rightarrow D\) with 
\((\dim_D(V), |D|) \neq (2,2), (2,3)\). For \((\dim_D(U), |D|) \neq (2,2)\) let \(S_{U,Y}\) be the derived group of the group \(G_{U,Y}\) defined in Proposition \((9.12)\).

The group \(\text{FSL}_D(V,W,m) = \text{FGL}_D(V,W,m)^{\prime}\) is the directed limit of its subgroups

\[ S_{U,Y} \simeq \text{SL}_D(U,Y,m|_{U \times Y}) \simeq \text{SL}_D(U) \]

for \(U\) finite dimensional in \(V\), \(Y\) finite dimensional in \(W\), and \(m|_{U \times Y}\) nondegenerate.

This group \(\text{FSL}_D(V,W,m)\) is quasisimple if \(V\) and \(W\) have finite dimension and simple if \(V\) and \(W\) have infinite dimension.

Proof. We have \(G_{U,Y}^{\prime} = S_{U,Y} \simeq \text{SL}_D(U)\).

By the proposition, for each \(g, h \in \text{FGL}(V,W,\cdot)\) there is a \(G_{U,Y}^{\prime}\) containing both \(g\) and \(h\) hence \([g,h] \in S_{U,Y}\).

Furthermore, for finite dimensional nondegenerate \(m: U_1 \times Y_1\) and \(m: U_2 \times Y_2\), there is a finite dimensional and nondegenerate \(m: U \times Y\) with

\[ \langle G_{U_1,Y_1}, G_{U_2,Y_2} \rangle \leq G_{U,Y} \]

hence

\[ \langle S_{U_1,Y_1}, S_{U_2,Y_2} \rangle = \langle G_{U_1,Y_1}^{\prime}, G_{U_2,Y_2}^{\prime} \rangle \leq G_{U,Y}^{\prime} = S_{U,Y} \, . \]

Therefore the subgroup of \(\text{FGL}_D(V,W,m)\) generated by all commutators is the directed limit of the various quasisimple subgroups \(S_{U,Y}\). By Problem \((4.19)\) the groups itself must then be quasisimple.

If \(V\) has finite dimension, then \(\text{FSL}_D(V,W,m) = S_{V,W}\) is quasisimple. Assume \(V\) has infinite dimension, and let \(z \in \text{Z}(\text{FSL}_D(V,W,m))\). Then there is some \(S_{U,Y}\) with \(z \in S_{U,Y}\), hence \(z\) scalar is on \(U\) (and \(Y\)). Thus either \(z = 1\) of \(\deg_U(z) = \deg_U(z) = \dim_D(U)\). Since \(V\) has infinite dimension, we may find finite dimensional \(U^\prime\) and \(Y^\prime\) with \(U < U^\prime, Y < Y^\prime\) and \(m|_{U^\prime \times Y^\prime}\) nondegenerate. But then \(z\) is in the center \(S_{U,Y}\), having degree strictly less than \(\dim_D(U^\prime)\). We conclude that \(z = 1\), and so \(\text{FSL}_D(V,W,m)\) is simple.

Here we have defined the finitary special linear group \(\text{FSL}_D(V,W,m)\) to be the derived group of the finitary general linear group \(\text{FGL}_D(V,W,m)\). Instead we could have observed, using Proposition \((9.12)\) that the Dieudonné determinant has a well-defined and unique extension from the finite dimensional to the finitary groups \(\text{FGL}_D(V,W,m)\) (with \(m\) nondegenerate) and that \(\text{FSL}_D(V,W,m)\) is the corresponding kernel. Thus the finitary special linear
9.2. THE ISOMETRY GROUPS OF PAIRINGS

groups FSL relate to the finitary general linear groups FGL in the same way that the alternating groups Alt relate to the finitary symmetric groups FSym.


(a) For \( m : V \times W \rightarrow D \) a nondegenerate pairing, we have

\[
\text{FSL}_D(V, W, m) \cong T_D(W^\rho, V) \cong T_D(W, V^\lambda),
\]

the isomorphisms given by restriction.

(b) Let \( V \) have infinite dimension and \( W \) be a subspace of \( V^* \) with \( \perp W = 0 \). Then \( m = m^{\text{can}}|_{V \times W} \) is nondegenerate. Furthermore

\[
\text{FSL}_D(V, W, m) \cong T(W, V)
\]

is simple. Especially

\[
\text{FSL}_D(V, V^*, m^{\text{can}}) \cong \text{FSL}_D(V) = T(V^*, V)
\]

is simple.

(c) Let \( B \) be the canonical basis of the \( D \)-vector space \( V = D^N \). Then the finitary linear group \( \text{FGL}_D(V, V^B, m^B) \) is isomorphic to the stable linear group \( \text{GL}(D) \) of Problem \([6.39]\) and that isomorphism restricts to an isomorphism of \( \text{FSL}_D(V, V^B, m^B) = \text{FGL}_D(V, V^B, m^B)' \) with the elementary stable linear group \( E(D) = \text{GL}(D)' \), which is simple.

Proof. (a) For \((\dim_D(V), |D|) = (2, 2)\) this is clear, and in finite dimensions the result is immediate from Proposition \([9.11]\).

In general, there are many ways of seeing the isomorphisms, but perhaps the most elegant is to observe that all three groups are (isomorphic to) the directed limit of the subgroups \( S_{U,Y} \) of the previous theorem. Simplicity then follows from the theorem as well.

(b) As \( W \subseteq V^* \) we have \( V^\perp = 0 \), so \( m \) is nondegenerate. Then (a) and Theorem \([9.13]\) apply.

(c) The dual bases \( B \) of \( V \) and \( B^* \) of \( V^B \) can be used to represent the group \( \text{FGL}_D(V, V^B, m^B) \) by infinite matrices that differ from the identity only in a finite dimensional upper-lefthand corner, as in Problem \([6.39]\). That is, if \( V_n \) is the span in \( V \) of the first \( n \) vectors of the basis \( B \) and \( V^B_n \) the subspace of \( V^* \) spanned by the corresponding initial segment of \( B^* \), then \( \text{FGL}_D(V, V^B, m^B) \) is the ascending directed limit of the groups \( \text{GL}_D(V_n) \) \((\cong \text{GL}_D(V_n, V^B_n, m^B|_{V_n \times V^B_n})\) with respect to the natural embedding.

Simplicity again comes from the theorem.

\[\square\]

1This points up a notational inconsistency. Because the alternating groups only make sense in the finitary context, we did not refer to them as finitary alternating Alt but only as alternating Alt. Here we can only make sense of the Dieudonné determinant in the finitary linear context, but nevertheless we maintain the finitary terminology and notation FSL rather than SL, even though the finitary attribute is redundant.
CHAPTER 9. PAIRINGS, ISOMETRIES, AND AUTOMORPHISMS

(9.15). Theorem. For \( m : V \times W \rightarrow D \) nondegenerate and infinite dimensional, the unique minimal normal subgroup of \( \text{GL}_D(V,W,m) \) is \( \text{FSL}_D(V,W,m) \).

\[ \text{Proof.} \]

\[ \square \]

9.3 Elations and automorphisms

An elation \( e \) is the image in \( \text{PSL}_D(V) \) of a transvection of \( \text{SL}_D(V) \). The image \( \bar{T}(\varphi,x) \) of the transvection subgroup \( T(\varphi,x) \) is an elation subgroup.

(9.16). Lemma.

(a) Every elation has a unique transvection preimage.

(b) Set \( \bar{T}(\varphi) = \bar{T} \) for each nonzero \( \varphi \in V^* \) and \( v \in V \). If \( T(a) \cap T(b) \neq 1 \) for nonzero \( a, b \in V^* \cup V \) with \( \langle a \rangle \neq \langle b \rangle \), then there are \( \varphi \in V^* \) and \( v \in V \) with \( \{a, b\} = \{\varphi, v\} \), \( v \in \ker \varphi \), and \( \bar{T}(\varphi, x) = \bar{T}(\varphi) \cap \bar{T}(v) \) isomorphic to \( (D,+) \). For \( \dim V \geq 3 \), \( \bar{T}(\varphi) \neq \bar{T}(v) \).

(c) Every abelian subgroup that is maximal subject to containing only the identity and elations is either \( \bar{T}(\varphi) \), for some \( \varphi \in V^* \), or is \( \bar{T}(v) \), for some \( v \in V \).

\[ \text{Proof.} \]

\[ \square \]

\( \text{Aut}_0(\text{PSL}_D(V)) \) will denote that subgroup of \( \text{Aut}(\text{PSL}_D(V)) \) composed of automorphisms that take elation subgroups to elation subgroups.

(9.17). Theorem. Let \( n \geq 3 \).

(a) \( \text{Aut}_0(\text{PSL}_n(D)) \) has \( \text{PGL}_n(D) \) as a normal subgroup of index at most 2.

(b) \( \text{Aut}_0(\text{PSL}_n(D)) \neq \text{PGL}_n(D) \) if and only if \( D \) is isomorphic to \( D^{op} \).

\[ \text{Proof.} \]

\[ \square \]

(9.18). Corollary. For \( n \geq 3 \),

\[ \text{Aut}(\text{PSL}_n(q)) = \text{PGL}_n(q) \langle \tau \rangle . \]

\[ \text{Proof.} \] Let \( q \) be a power of the prime \( p \). An automorphism of finite \( \text{PSL}_n(q) \) must take Sylow \( p \)-subgroups to Sylow \( p \)-subgroups. But the center of a Sylow \( p \)-subgroup of \( \text{PSL}_n(q) \) is an elation subgroup. \[ \square \]
9.4. PROBLEMS

(9.19). Problem. The matrix “inverse-transpose” map \( g \mapsto (g^{-1})^\top \) induces an automorphism of \( \text{PSL}_n(F) \), for any field \( F \). For \( n \geq 3 \) this automorphism is not induced by any semilinear map.

Find a semilinear \( \Sigma = (\sigma, S) \in \Gamma L_2(F) \) with \( g^\Sigma = (g^{-1})^\top \) on \( \text{PSL}_2(F) \).

Remark. The next problem implies that this automorphism must be semilinear when \( n = 2 \), but the direct calculation is more elementary.

(9.20). Problem. Let \( F \) be a field. This problem approaches Theorem (9.20)(a). \( \text{Aut}(\text{PSL}_2(F)) = \text{PGL}_2(F) \).

We actually prove the slightly easier

Theorem (9.20)(b). \( \text{Aut}_0(\text{PSL}_2(F)) = \text{PGL}_2(F) \).

As in Corollary (9.18) we get the important:

Corollary (9.20)(c). For finite fields \( F \), we have \( \text{Aut}(\text{PSL}_2(F)) = \text{PGL}_2(F) \).

The proofs are presented through a sequence of parts.

Let \( V = F^2 \), the two dimensional \( F \)-space of row vectors, admitting the group \( \Gamma L_2(F) = \text{Aut}(F) \rtimes \text{GL}_2(F) \) acting via

\[
(a, b)^{(\sigma, S)} = (a^\sigma, b^\sigma)S .
\]

Thus \( \text{PGL}_2(F) \) (and its various subgroups) acts on the associated projective line \( \mathbb{P}V = \mathbb{P}F^2 \).

For the vectors \( (a, b) \in V \) and 1-spaces \( \langle (a, b) \rangle \), define the transvections

\[
t_{\langle (0,1) \rangle}(d) = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}
\]

and

\[
t_{\langle (1,0) \rangle}(d) = \begin{pmatrix} 1 - ad & -a^2d \\ d & 1 + ad \end{pmatrix}
\]

for each \( d \in F \); so in particular

\[
t_{\langle (1,0) \rangle}(d) = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} .
\]

Also define the transvection subgroup

\[
T_{\langle v \rangle} = \{ t_{\langle v \rangle}(d) \mid d \in F \} ,
\]

for each 1-space \( \langle v \rangle \) in \( V \).

(a) (i) For fixed \( \langle v \rangle \), prove that \( T_{\langle v \rangle} \) is a subgroup of \( \text{SL}_2(F) \) and that \( d \mapsto t_{\langle v \rangle}(d) \) is an isomorphism of the additive group \( (F, +) \) with \( T_{\langle v \rangle} \).

(ii) For each \( t \in T_{\langle v \rangle} \) with \( t \neq 1 \), prove that \( V(t - 1) = \langle v \rangle \) and \( V(t - 1)^2 = \langle v \rangle \).

Conversely, show that any \( t \in \text{GL}_2(F) \) that has these two properties is \( t_{\langle v \rangle}(d) \), for some non-zero \( d \in F \).
CHAPTER 9. PAIRINGS, ISOMETRIES, AND AUTOMORPHISMS

(REMARK. Once you have proved this characterization of transvections and transvection subgroups, in the rest of the problem you should not need to do much calculation with the complicated matrices above.)

(iii) For each \( g \in \text{GL}_2(F) \), prove that \( g^{-1}T_{(x)}g = T_{(x)} \). (Make sure you get the correct inverse for \( g \). You may want to use the characterization of (ii) for this.)

(iv) Prove that \( g \in \text{GL}_2(F) \) normalizes \( T_{(x)} \) if and only if \( (v^g) = (v^g) \).

(v) If finite \( |F| = p^k \), for some prime \( p \), prove that the set of the various \( T_{(x)} \) is precisely the set of Sylow \( p \)-subgroups of \( \text{GL}_2(F) \).

Each transvection subgroup \( T_{(x)} \) meets the group \( Z_2(F) \) of scalars trivially and contains all transvections of the subgroup \( T_{(x)} \times Z_2(F) \) (as

\[
\begin{pmatrix}
    r - 1 & 0 \\
    d & r - 1
\end{pmatrix}
\]

has rank 2 for central \( r \neq 1 \). Thus the image \( \tilde{T}_{(x)} \) of \( T_{(x)} \) in the quotient group \( \text{PSL}_2(F) \) inherits the properties of part (a). The subgroups \( \tilde{T}_{(x)} \) are the elation subgroups of \( \text{PSL}_2(F) \).

\( \text{Aut}_0(\text{PSL}_2(F)) \) is defined to be the subgroup of \( \text{Aut}(\text{PSL}_2(F)) \) that takes elation subgroups to elation subgroups. That is, for each \( r \) in \( \text{Aut}_0(\text{PSL}_2(F)) \) and each nonzero \( v \in V \), we have \( \tilde{T}_r(T_{(v)}) = T_{r(\tilde{v})} \), for some \( \tilde{v} \). By part (a)(iii), \( \text{PGL}_2(F) \) is at least contained in \( \text{Aut}_0(\text{PSL}_2(F)) \).

(b) Show that if \( |F| \) is finite, then \( \text{Aut}_0(\text{PSL}_2(F)) = \text{Aut}(\text{PSL}_2(F)) \).

We now commence with the proof of Theorem (9.20)(b). Set \( G = \text{PSL}_2(F) \), and choose an arbitrary \( S \in \text{Aut}_0(G) \).

We want to show that there is a semilinear map \( \Sigma \) such that \( g^S = g^\Sigma \), for each \( g \in \text{PSL}_2(F) \), for then \( \Sigma \mapsto S \) describes a homomorphism of \( \text{GL}_2(F) \) onto \( \text{Aut}_0(\text{PSL}_2(F)) \) with kernel the group of scalar maps \( Z_2(F) \), proving Theorem 2.

There are vectors \( \bar{x}, \bar{y}, \bar{z} \in V \) with \( \tilde{T}_{(1,0)}(\bar{x}) = \tilde{T}_{(1,1)}(\bar{y}) = \tilde{T}_{(0,0)}(\bar{z}) = \tilde{T}_{(1,1)}(\bar{z}) \). Set \( \bar{x}_0 = \bar{x} \). Then we can find a scalar \( e \in F \) with so that \( \bar{z} = \bar{x}_0 + \bar{x}_1 \) upon setting \( \bar{x}_1 = e \bar{y} \). Hence

\[
\tilde{T}_{(1,0)} = \tilde{T}_{(x_0)}, \quad \tilde{T}_{(1,1)} = \tilde{T}_{(x_1)}, \quad \text{and} \quad \tilde{T}_{(0,0)} = \tilde{T}_{(x_0 + x_1)}.
\]

Next, for every \( a \in F \), there is a uniquely determined \( a^\sigma \in F \) with

\[
\tilde{T}_{(a)} = \tilde{T}_{(x_0 + a^\sigma x_1)}.
\]

Notice that \( 0^\sigma = 0 \) since \( \tilde{T}_{(0,0)} = \tilde{T}_{(x_0)} \), and \( 1^\sigma = 1 \) since \( \tilde{T}_{(1,1)} = \tilde{T}_{(x_0 + x_1)} \).

(c) Prove that for all \( a, b \in F \):

(i) \( (a + b)^\sigma = a^\sigma + b^\sigma \);

(ii) \( (ab)^\sigma = a^\sigma(b^\sigma) \);

(iii) \( (a^r)^{-1} = (a^{-1})^\sigma \);

(HINT: For (i) let \( g \in \tilde{T}_{(0,0)} \) be represented by \( \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \). Therefore \( g^S \in \tilde{T}_{(0,0)} \). Thus there is a \( b' \in F \) for which \( g^S \) is represented by the transvection \( t \) with

\[
t: \bar{x}_0 \mapsto \bar{x}_0 + b' \bar{x}_1 \quad t: \bar{x}_1 \mapsto \bar{x}_1.
\]
9.4. PROBLEMS

Now calculate both sides of
\[
(g^{-1}\bar{T}_{(1, a)})^S g = (g^{-1})^S \bar{T}_{(1, a)} g^S
\]
to conclude that, for all \(a \in F\), \((a + b)^\sigma = a^\sigma + b\). Using this, complete (i).

For (ii) and (iii) consider the action of elements represented by \[
\begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix}
\]
as well as their images under \(S\).

(d) Prove that \(\sigma\) is in fact an automorphism of \(F\).

( Remark. More generally, any bijection \(\sigma: F \to F\) with (i), (ii), and (iii) of (c) is an automorphism of \(F\).)

(e) Prove that \(\Sigma: (a, b) \mapsto a^\sigma \bar{x}_0 + b^\sigma \bar{x}_1\) is a semilinear map on \(V\) with \(\bar{T}_{(v)}^\Sigma = \bar{T}_{(v)}^S\), for all 1-spaces \(\langle v \rangle\) of \(V\).

(f) Prove that \(g^\Sigma = g^S\), for all \(g \in G\).

( Hint: Let \(I \in \text{Aut}_0(G)\) be the automorphism \(\Sigma S^{-1}\), where \(\Sigma\) is the image of \(\Sigma\) in \(\text{PGL}_2(F)\). Then \(I\) fixes each transvection subgroup of \(G\). For arbitrary \(g \in G\), calculate \((g^{-1}\bar{T}_{(v)} g)^I = (g^{-1})^I \bar{T}_{(v)}^I g^I\) to prove that \(\bar{T}_{(v)}^g = \bar{T}_{(v)}^g\), for all 1-spaces \(\langle v \rangle\). Therefore \(g^I g^{-1}\) fixes all 1-spaces \(\langle v \rangle\) and so is the identity element of \(G = \text{PSL}_2(F)\).)

Part (f) completes the proof of Theorem (9.20)(b) and together with part (b) completes the proof of Corollary (9.20)(c).
Bibliography


<table>
<thead>
<tr>
<th>Reference</th>
<th>Author(s)</th>
<th>Title</th>
<th>Series</th>
<th>Publisher</th>
<th>Location</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shu11</td>
<td>E.E. Shult</td>
<td>“Points and Lines. Characterizing the Classical Geometries”</td>
<td>Universitext</td>
<td>Springer</td>
<td>Heidelberg</td>
<td>2011</td>
</tr>
</tbody>
</table>
Index

(B, N)-pair, 81
0-dummy index 2015-02-16, 116
2-cycle, 59
2-transitive, 33
2^2-elements, 59
3-cycles, 59
3-transposition group, 67
3-transpositions, 67
A-invariant, 14
D-linear representations, 6
FC-group, 57
G-decomposable, 41
G-invariant, 6
G-module, 39
G-orbit, 30
G-space, 29
K-linear representation, 39
K-permutation module, 40
[V, g], 98
Aut(G), 13
H_n(R), 70
Col(ΩV), 92
FGL_D(V, W, m), 109
GL_D(V), 6
GL_D(V, W, m), 107
Inn(G), 13
U^-n(R), 70
Out(G), 13
PGL_n(D), 97
PTL_n(D), 97
PSL_n(D), 87
R_n(D), 86
E_n(R), 70
SL_D(U), 109
SL_n(D), 81
SL_D(U, Y, m), 109
U_n(R), 70
U_n^+(R), 70
Z_n(D), 86
mon(A), 75
pmon(A), 75
k-homogeneous, 34
k-transitive, 34
p-Sylow subgroups, 23
p-group, 22
C-automorphisms, 5
C-endomorphisms, 5
C-representation, 5
C_G(H), 14
C_V(g), 98
F(X), 49
K_1(R), 90
N_G(H), 14
Sym(A), 6
Z(G), 13
axis, 99
A Frattini argument, 32
absolutely irreducible, 42
act via ρ, 5
action, 5
acts on A via ρ, 5
additive categories, 5
alternating group, 62
ascending chain condition, 55
automorphisms, 5
INDEX

B. Fischer, 67
bar convention, 16
block, 34
block lower unitriangular, 44
block of imprimitivity, 34
Borel subgroup, 81
braid group, 68
Breys-Iwasawa-Wilson Lemma, 35
Bruhat decomposition, 77
canonical pairing, 103
Cartan subgroup, 81
Cartesian product, 25
category, 3
category equivalence, 5
category isomorphic, 5
Cayley graph, 38
Cayley’s Theorem, 30
center, 13
central series, 21
centralizer, 14
characteristic, 14
characteristic series, 19
characteristically simple, 14
chief factors, 56
chief series, 56
Chinese Remainder Theorem, 24
Classification of finite simple groups (CFSG), 1983, 2004, 2
Clifford’s Theorem, 43
collineation group, 92
collineations, 92
column pivot, 73
column pivot form, 73
column pivot location, 73
column pivot value, 73
commutator, 15
completely reducible, 42
composition map, 3
composition series, 56
comultiplication, 46
concrete, 4
concrete category, 4
conjugate, 3
connected, 38
core, 32
coset, 11
countably directed limit, 51
Coxeter group, 60
cycle type, 32
D.G. Higman, 38
decomposable, 41
defect, 19
degree, 39
dense, 4
dense subcategory, 4
derived length, 19
derived series, 19
derived subgroup, 16
descending chain condition, 55
Dieudonné determinant, 78
direct product, 23, 24
direct sum, 25
directed limit, 51
directed limit, finite, 51
division ring, 4
division rings, 4
double cosets, 11
double dual, 96
doubly transitive, 33
dual basis, 96
dual space, 95
eletion, 112
eletion subgroup, 112
elementary matrices, 69
elementary operations, 71
equipartition, 35
equivalence, 107
equivalent, 6, 39
even permutations, 63
extension, 17
external direct product, 24
external directed limit, 51
factor group, 12
faithful, 5, 29
finitary, 98
finitary general linear group, 109
finitary linear group, 55
INDEX

finitary special linear group, 110
finitary symmetric group, 54
finite dimensional linear groups, 39
finite generation, 49
finite presentation, 49
finite series, 19
finitely directed limit, 51
finitely generated, 49
finitely presented, 49
First Isomorphism Theorem, 12
Fischer, B., 67
Fitting subgroup, 22
free group, 49
full, 4
full subcategory, 4
functor, 5
Fundamental Theorem of Projective Geometry, 92
Fundamental Theorem of Set Geometry, 65
general linear group, 6
global stabilizer, 31
group automorphisms, 6
group of operators, 5

homogeneous component, 42
Hopf algebras, 46
hyperbolic, 105
hyperbolic pairing, 105
hyperplane, 91
identity functor, 5
imprimitive, 24, 43
indecomposable, 41
index, 11
inner automorphism, 13
inner automorphism group, 13
internal direct product, 25
internal directed limit, 51
internal representation theory, 15
intransitive, 30
invariant, 6
invariant relation, 33
irreducible, 41
isometric, 107

isometry, 107
isomorphic, 3, 5
isomorphic G-modules, 39
isomorphic G-spaces, 39
isomorphic modules, 39
isomorphic objects, 3
Iwasawa’s Lemma, 55

Jordan-Hölder, 1
K-permutation representation, 40
kernel, 12

Lagrange’s Theorem, 11
length, 83
linear group, 39, 54
linear representation, 6, 39
lines, 91
local linearity, 54
local system, 51
locally finite group, 52
locally small, 4
locally small category, 4
locally-A’, 52
lower central series, 20
lower unitriangular group, 14

maximal condition, 55
McLain group, 101
minimal condition, 55
minimal normal subgroup, 56
monomial form, 75
monomial matrix, 73
morphisms, 3

nilpotence class, 21
nilpotent, 21
nilpotent group, 21
normal series, 19
normal subgroup, 12
normalizer, 14

objects, 3
odd permutations, 63
orbit, 30
orbital, 33
outer automorphism group, 13
INDEX

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>P. Hall</td>
<td>51, 52</td>
</tr>
<tr>
<td>paired orbital</td>
<td>83</td>
</tr>
<tr>
<td>pairing</td>
<td>103</td>
</tr>
<tr>
<td>parabolic subgroups</td>
<td>83</td>
</tr>
<tr>
<td>partial monomial form</td>
<td>75</td>
</tr>
<tr>
<td>partial monomial matrix</td>
<td>73</td>
</tr>
<tr>
<td>perfect group</td>
<td>17</td>
</tr>
<tr>
<td>permutation group</td>
<td>29</td>
</tr>
<tr>
<td>permutation isomorphism</td>
<td>30</td>
</tr>
<tr>
<td>permutation matrix</td>
<td>40</td>
</tr>
<tr>
<td>permutation module</td>
<td>40</td>
</tr>
<tr>
<td>permutation representation</td>
<td>6, 29</td>
</tr>
<tr>
<td>permutation representations</td>
<td>6</td>
</tr>
<tr>
<td>permutation space</td>
<td>29</td>
</tr>
<tr>
<td>pivot matrix</td>
<td>73</td>
</tr>
<tr>
<td>pivots</td>
<td>73</td>
</tr>
<tr>
<td>planes</td>
<td>91</td>
</tr>
<tr>
<td>points</td>
<td>91</td>
</tr>
<tr>
<td>pointwise stablizer</td>
<td>31</td>
</tr>
<tr>
<td>primitive</td>
<td>34, 43</td>
</tr>
<tr>
<td>pro-$p$ groups</td>
<td>53</td>
</tr>
<tr>
<td>profinite topology</td>
<td>53</td>
</tr>
<tr>
<td>projective lines</td>
<td>91</td>
</tr>
<tr>
<td>projective planes</td>
<td>91</td>
</tr>
<tr>
<td>projective points</td>
<td>91</td>
</tr>
<tr>
<td>projective representation</td>
<td>39</td>
</tr>
<tr>
<td>projective space</td>
<td>91</td>
</tr>
<tr>
<td>projective special linear group</td>
<td>87</td>
</tr>
<tr>
<td>quasisimple</td>
<td>17</td>
</tr>
<tr>
<td>quotient group</td>
<td>12</td>
</tr>
<tr>
<td>rank</td>
<td>33, 91</td>
</tr>
<tr>
<td>reducible</td>
<td>41</td>
</tr>
<tr>
<td>regular</td>
<td>31</td>
</tr>
<tr>
<td>Reidermeister Quadrangle Condition</td>
<td>26</td>
</tr>
<tr>
<td>Reidermeister-Schreier</td>
<td>49</td>
</tr>
<tr>
<td>representation</td>
<td>9</td>
</tr>
<tr>
<td>residually finite</td>
<td>53</td>
</tr>
<tr>
<td>residually-$\mathcal{X}$</td>
<td>52</td>
</tr>
<tr>
<td>restricted direct product</td>
<td>25</td>
</tr>
<tr>
<td>right regular representation</td>
<td>30</td>
</tr>
<tr>
<td>row echelon form</td>
<td>72</td>
</tr>
<tr>
<td>row pivot</td>
<td>73</td>
</tr>
<tr>
<td>row pivot form</td>
<td>73</td>
</tr>
<tr>
<td>Schmidt’s Theorem</td>
<td>52</td>
</tr>
<tr>
<td>Schreier</td>
<td>49, 53</td>
</tr>
<tr>
<td>Second Isomorphism Theorem</td>
<td>13</td>
</tr>
<tr>
<td>section</td>
<td>15</td>
</tr>
<tr>
<td>semidirect product</td>
<td>18</td>
</tr>
<tr>
<td>semiequivalent</td>
<td>7</td>
</tr>
<tr>
<td>semilinear</td>
<td>4, 6</td>
</tr>
<tr>
<td>semilinear map</td>
<td>40</td>
</tr>
<tr>
<td>semilinear maps</td>
<td>92</td>
</tr>
<tr>
<td>semiregular</td>
<td>31</td>
</tr>
<tr>
<td>shadow</td>
<td>91</td>
</tr>
<tr>
<td>sign</td>
<td>63</td>
</tr>
<tr>
<td>simple group</td>
<td>14</td>
</tr>
<tr>
<td>small category</td>
<td>9</td>
</tr>
<tr>
<td>solvable</td>
<td>19</td>
</tr>
<tr>
<td>solvable radical</td>
<td>20</td>
</tr>
<tr>
<td>special linear group</td>
<td>81</td>
</tr>
<tr>
<td>split</td>
<td>41</td>
</tr>
<tr>
<td>split extension</td>
<td>18, 41</td>
</tr>
<tr>
<td>stability group</td>
<td>43</td>
</tr>
<tr>
<td>stabilizer</td>
<td>31</td>
</tr>
<tr>
<td>stable linear group</td>
<td>90</td>
</tr>
<tr>
<td>stably linear</td>
<td>55</td>
</tr>
<tr>
<td>strongly connected</td>
<td>58</td>
</tr>
<tr>
<td>subcategory</td>
<td>4</td>
</tr>
<tr>
<td>subdirect product</td>
<td>24</td>
</tr>
<tr>
<td>subnormal</td>
<td>19</td>
</tr>
<tr>
<td>subnormal series</td>
<td>19</td>
</tr>
<tr>
<td>subspace generated</td>
<td>92</td>
</tr>
<tr>
<td>support</td>
<td>54</td>
</tr>
<tr>
<td>Sylow $p$-subgroup</td>
<td>35</td>
</tr>
<tr>
<td>Sylow $p$-subgroups</td>
<td>23</td>
</tr>
<tr>
<td>Sylow subgroups</td>
<td>23</td>
</tr>
<tr>
<td>Sylow’s First Theorem</td>
<td>23, 36</td>
</tr>
<tr>
<td>Sylow’s Second Theorem</td>
<td>36</td>
</tr>
<tr>
<td>Sylow’s Third Theorem</td>
<td>36</td>
</tr>
<tr>
<td>symmetric group</td>
<td>9</td>
</tr>
<tr>
<td>symmetric group</td>
<td>29</td>
</tr>
<tr>
<td>The Class Equation</td>
<td>14</td>
</tr>
<tr>
<td>The Frattini argument</td>
<td>36</td>
</tr>
<tr>
<td>The Whitehead Lemma</td>
<td>90</td>
</tr>
<tr>
<td>Third Isomorphism Theorem</td>
<td>13</td>
</tr>
<tr>
<td>Thompson Transfer</td>
<td>67</td>
</tr>
</tbody>
</table>
Three subgroups lemma, \footnote{16}
transitive, \footnote{30}
transposition, \footnote{59}
transvection, \footnote{99}
transvection subgroup, \footnote{99}
trivial equivalence relations, \footnote{34}
type \(A_k\), \footnote{60}

unipotent element, \footnote{44}
unipotent subgroup, \footnote{44}
unitriangular matrices, \footnote{70}
universal locally finite group, \footnote{68}
unrestricted direct product, \footnote{25}
upper central series, \footnote{20}

Weyl group, \footnote{60} \footnote{81}
Whitehead group, \footnote{90}
Whitehead Lemma, \footnote{71}