Definitions

Algebra qualifying course
MSU, Spring 2017

Joshua Ruiter

October 15, 2019

This document was made as a way to study the material from the spring semester algebra qualifying course at Michigan State University, in spring of 2017. It serves as a companion document to the "Theorems" review sheet for the same class.

Contents

1 Modules over Rings

1.1 Homomorphism Group and Hom Functor

Definition 1.1. Let A be a ring and X, X' be A-modules. We define $\mathbf{Hom}_{\boldsymbol{A}}\boldsymbol{(X, X')}$ to be the set of A-module homomorphisms from X to X'. It is a group under pointwise addition of maps. We define an action $A \times \mathrm{Hom}_A(X, X') \to \mathrm{Hom}_A(X, X')$ by

$$(a \cdot \phi)(x) = a \cdot (\phi(x))$$

for $a \in A, \phi \in \mathrm{Hom}_A(X, X')$, and $x \in X$. This makes $\mathrm{Hom}_A(X, X')$ an A-module.

Definition 1.2. Let A be a ring and Y an A-module. We define the functor $\mathbf{Hom}_{\boldsymbol{A}}\boldsymbol{(Y, -)}$ from the category of A-modules to itself by sending an A-module X to the A-module $\mathrm{Hom}_A(Y, X)$ and sending $f \in \mathrm{Hom}_A(X, X')$ to

$$\begin{aligned} \mathrm{Hom}_A(Y, f) : \mathrm{Hom}_A(Y, X) &\to \mathrm{Hom}_A(Y, X') \\ \phi &\mapsto f \circ \phi \end{aligned}$$

The identity is preserved, because $\mathrm{Hom}_A(Y, \mathrm{Id}_X)$ is given by $\phi \mapsto \mathrm{Id} \circ \phi = \phi$. It also preserves composition: let $f \in \mathrm{Hom}_A(X, X')$ and $g \in \mathrm{Hom}_A(X', X'')$. Then for $\phi \in \mathrm{Hom}_A(Y, X)$,

$$\begin{aligned} \mathrm{Hom}_A(Y, g \circ f)(\phi) &= (g \circ f) \circ \phi = g \circ (f \circ \phi) = g \circ \mathrm{Hom}_A(Y, f)(\phi) \\ &= \mathrm{Hom}_A(Y, g) \circ \mathrm{Hom}_A(Y, f)(\phi) \\ \implies \mathrm{Hom}_A(Y, g \circ f) &= \mathrm{Hom}_A(Y, g) \circ \mathrm{Hom}_A(Y, f) \end{aligned}$$

so it is covariant.

Definition 1.3. Let A be a ring and Y an A-module. We define the functor $\mathbf{Hom}_{\boldsymbol{A}}\boldsymbol{(-, Y)}$ from the category of A-modules to itself by sending an A-module X to the A-module $\mathrm{Hom}_A(X, Y)$ and sending $f \in \mathrm{Hom}_A(X, X')$ to

$$\begin{aligned} \mathrm{Hom}_A(f, Y) : \mathrm{Hom}_A(X', Y) &\to \mathrm{Hom}_A(X, Y) \\ \phi &\mapsto \phi \circ f \end{aligned}$$

The identity is preserved, because $\mathrm{Hom}_A(\mathrm{Id}_X, Y)$ is given by $\phi \mapsto \phi \circ \mathrm{Id}_X = \phi$. Unlike the above, this is a contravariant functor: let $f \in \mathrm{Hom}_A(X, X')$ and $g \in \mathrm{Hom}_A(X', X'')$. Then for $\phi \in \mathrm{Hom}_A(X'', Y)$,

$$\begin{aligned} \mathrm{Hom}_A(Y, g \circ f)(\phi) &= \phi \circ (g \circ f) = (\phi \circ g) \circ f = \mathrm{Hom}_A(g, Y)(\phi) \circ f \\ &= \mathrm{Hom}_A(f, Y) \circ \mathrm{Hom}_A(g, Y)(\phi) \\ \implies \mathrm{Hom}_A(Y, g \circ f) &= \mathrm{Hom}_A(f, Y) \circ \mathrm{Hom}_A(g, Y) \end{aligned}$$

so it is contravariant.

Definition 1.4. Let A be a ring and let

$$X' \xrightarrow{f} X \xrightarrow{g} X''$$

be a sequence of A-modules. Let Y be an A-module. The **induced sequence** is

$$\mathrm{Hom}_A(X', Y) \xleftarrow{\mathrm{Hom}_A(f,Y)} \mathrm{Hom}_A(X, Y) \xleftarrow{\mathrm{Hom}_A(g,Y)} \mathrm{Hom}_A(X'', Y)$$

Definition 1.5. Let A-Mod and B-Mod be the categories of $A-$ and $B-$modules respectively and let $F : A\text{-Mod} \to B\text{-Mod}$ be a functor. F is **exact** if for every exact sequence

$$\ldots \xrightarrow{f} X \xrightarrow{f'} X' \xrightarrow{f''} X'' \xrightarrow{f'''} \ldots$$

the induced sequence

$$\ldots \xrightarrow{F(f)} F(X) \xrightarrow{F(f')} F(X') \xrightarrow{F(f'')} F(X'') \xrightarrow{F(f''')} \ldots$$

is exact.

1.2 Free Modules

Definition 1.6. Let M be a module over a ring A and let $S \subset M$. A **linear combination** of elements of S is a sum

$$\sum_{s \in S} a_s s$$

where $a_s \in A$ and there are only finitely many nonzero terms.

Definition 1.7. Let M be a module over a ring A and let $S \subset M$. S **generates** $\boldsymbol{S}$ **over** $\boldsymbol{A}$ if every $x \in M$ can be written as a linear combination of elements of S. That is,

$$M = \left\{ \sum_{s \in S} a_s s : a_s \in A, \text{ finitely many nonzero terms} \right\}$$

Definition 1.8. Let M be a module over a ring A and let $S \subset M$. S is **linearly independent** over A if

$$\sum_{s \in S} a_s s = 0 \implies \forall s \; a_s = 0$$

That is, the only linear combination of elements of S that is zero is the trivial linear combination.

Definition 1.9. Let M be a module over a ring A and let $S \subset M$. S is a **basis** of M if $S \neq \emptyset$ and S generates M and S is linearly independent over A. Note that if M has a basis and $M \neq \{0\}$ and $A \neq \{0\}$, then every element of M has a unique expression as a linear combination of elements of S.

Definition 1.10. A **free module** is a module that has a basis. (Note: The zero module is considered free.)

Definition 1.11. After fixing a ring A, a free module is determined (up to isomorphism) by the size of a basis. Thus the size of a basis is invariant (this is a theorem). Thus we can define the **rank** of a free A-module to be the size of any basis for that module.

Definition 1.12. A **finite free module** is a free module of finite rank.

1.3 Dual Module

Definition 1.13. Let A be a commutative ring and let E be a free A-module. The **dual module**, denoted $\boldsymbol{E}^\vee$ is the A-module $\operatorname{Hom}(E, A)$. Elements of $E^\vee$ are called **linear functionals**. For $x \in E$ and $f \in E^\vee$, we define $\langle \boldsymbol{x}, \boldsymbol{f} \rangle = f(x)$. Note that for a fixed x, the map $E^\vee \to A$ defined by $f \mapsto f(x)$ is an injective A-module homomorphism.

Definition 1.14. Let A be a commutative ring and let E be a free A-module with basis $\{x_i\}_{i \in I}$. For each i, define $f_i : E \to A$ by $f_i(x_j) = \delta_{ij}$. Note that $\{f_i\}_{i \in I}$ is not always a basis of $E^\vee$. When E has finite rank, $\{f_i\}_{i \in I}$ is called the **dual basis**. (It is called the dual basis because it is in fact a basis for $E^\vee$.)

1.4 Modules over Principal Ideal Domains

Definition 1.15. An R-module M is **cyclic** if there exists $x \in M$ so that $M = Rx = \{rx : r \in R\}$.

Definition 1.16. A **torsion module** is an R-module M such that for any $x \in M$, there exists $r \in R$ such that $r \neq 0$ and $rx = 0$.

Definition 1.17. An element x of an R-module M is a **torsion element** if there exists $r \in R$ that is not a zero divisor so that $rx = 0$.

Definition 1.18. Let M be an R-module. The **torsion submodule** of M, denoted M_{tor}, is the submodule of M consisting of all torsion elements of M.

Definition 1.19. Let R be a PID and let E be an R-module. For a fixed $x \in E$, the map $R \to E$ defined by $r \mapsto rx$ is a homomorphism. The kernel of this homomorphism is a principal ideal, since R is a PID. Any generator m of that ideal is a **period** of x.

Definition 1.20. Let R be a PID and let E be an R-module. An **exponent** of E is an element $c \in R$ with $c \neq 0$ such that $cE = 0$.

Definition 1.21. Let R be a PID and let E be an R-module. Let $p \in R$ be a prime. We define $\boldsymbol{E(p)}$ to be the submodule of E consisting of all elements $x \in E$ so that x has an exponent that is a power of p^n for $n \geq 1$. A $\boldsymbol{p}$**-submodule** of E is a submodule of $E(p)$.

Recall that in a PID, a **prime** element is a non-unit one that cannot be expressed as a product of two non-unit elements.

1.5 Euler-Poincare Maps

Definition 1.22. Let A be a ring, let $\mathcal{C}$ be a collection of A-modules such that $0 \in \mathcal{C}$ and if $0 \to M' \to M \to M'' \to 0$ is exact, then

$$M \in \mathcal{C} \iff M' \in \mathcal{C} \text{ and } M'' \in \mathcal{C}$$

Let G be an abelian group. An **Euler-Poincare mapping** is map $\phi : \mathcal{C} \to G$ such that if $0 \to M' \to M \to M'' \to 0$ is exact, then

$$\phi(M) = \phi(M') + \phi(M'')$$

and $\phi(0) = 0$. (Note that a consequence of this definition is that ϕ is well-defined up to isomorphism, that is, ϕ maps isomorphic A-modules to the same element of G.)

Motivating example of Euler-Poincare maps: Assigning each finitely-generated $\mathbb{Z}$ module to its rank as an abelian group. Another example: Assigning each finite dimensional vector space over k to its dimension.

1.6 Tensor Products

Definition 1.23. Let R be a commutative ring. Let $E_1, \dots, E_n, F$ be R-modules. Then $\boldsymbol{L^n(E_1, \dots, E_n; F)}$ is the R-module of multilinear maps $f : E_1 \times \ldots \times E_n \to F$. Addition and scalar multiplication of maps are defined as follows:

$$(f+g)(e_1, \dots, e_n) = f(e_1, \dots, e_n) + g(e_1, \dots, e_n) \qquad (rf)(e_1, \dots, e_n) = r(f(e_1, \dots, e_n))$$

Definition 1.24. Let R be a commutative ring and $E_1, \dots, E_n$ be R-modules. Let M be the free R-module generated by $E_1 \times \ldots \times E_n$. Let N be the submodule of M generated by elements of the form

$$(x_1, \dots, x_i + x_i', \dots, x_n) - (x_1, \dots, x_i, \dots, x_n) - (x_1, \dots, x_i', \dots, x_n)$$
$$(x_1, \dots, ax_i, \dots, x_n) - a(x_1, \dots, x_n)$$

The module M/N is the **tensor product** of $E_1, \dots, E_n$. This is denoted

$$E_1 \otimes_R E_2 \otimes_R \ldots \otimes_R E_n \quad \text{or} \quad \bigotimes_{i=1}^n E_i$$

Elements of $\bigotimes_{i=1}^n E_i$ are written as $x_1 \otimes \ldots \otimes x_n$ where $x_i \in E_i$. There is a canonical map

$$\otimes : \prod_{i=1}^n E_i \to \bigotimes_{i=1}^n E_i$$

given by

$$(x_1, \dots, x_n) \mapsto x_1 \otimes \ldots \otimes x_n$$

which is R-multilinear.

Definition 1.25. Let $\phi : E' \to E$ be an R-module homomorphism and let F be an R-module. Then **induced map** $\phi_* : F \otimes E' \to F \otimes E$ is the linear map defined on the generators $y \otimes x'$ by

$$\phi_*(y \otimes x') = y \otimes \phi(x')$$

where $y \in F$ and $x' \in E'$. Note that not every element of $F \otimes E'$ can be written as $y \otimes x'$, but every element can be written as a linear combination of such elements, and there is a unique linear map that satisfies this. Note that ϕ_* is the image ϕ under the tensor functor $F \otimes -$.

1.7 Flat Modules

Definition 1.26. Let F be an R-module. F is **flat** if the functor $E \mapsto E \otimes_R F$ is exact. (It is always right exact, so this is equivalent to it being left exact.)

1.8 Homology

Definition 1.27. Let R be a ring. A **chain complex** of R-modules is a sequence of R-modules E^i and R-module homomorphisms $d^i : E^i \to E^{i+1}$ for $i \in \mathbb{Z}$, such that $d^i \circ d^{i-1} = 0$.

$$\dots \longrightarrow E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \longrightarrow \dots$$

(Note: The sequence is not necessarily exact. Every exact sequence is a complex, but the reverse is not true.)

Definition 1.28. A chain complex of R-modules is **bounded on the left** if there exists $n \in \mathbb{Z}$ so that $E^i = 0$ for all $i \leq n$. Similarly, it is **bounded on the right** if there exists n so that $E^i = 0$ for $n \geq i$. It is **bounded** or **finite** if it bounded on both sides.

Definition 1.29. Let M be an R-module. A **resolution** of M is an exact sequence

$$\dots \to E_2 \to E_1 \to E_0 \to M \to 0$$

Definition 1.30. A **free resolution** is a resolution where each E_i is free.

Definition 1.31. A **projective resolution** is a resolution where each E_i is projective.

Definition 1.32. Let R be a ring, and let (E_i, d_i) and (E'_i, d'_i) be complexes of R-modules. A **morphism of complexes of degree r** is a sequence of R-module homomorphisms $f_i : E'_i \to E_{i+r}$ so that for all i the following diagram commutes.

$$\begin{array}{ccc} E'_i & \xrightarrow{f_i} & E_{i+r} \\ {\scriptstyle d'_i}\downarrow & & \downarrow{\scriptstyle d_{i+r}} \\ E'_{i+1} & \xrightarrow[f_{i+1}]{} & E_{i+r+1} \end{array}$$

(Chain complexes along with morphisms form a category. Also, most important morphisms have degree zero.)

Definition 1.33. Let (E_i, d_i) be a chain complex of R-modules. The module $\ker d^i$ is called the ***i*-cycles**, and the module $\operatorname{im} d^{i-1}$ is called the ***i*-boundaries**. The quotient $\ker d^i / \operatorname{im} d^{i-1}$ is the i-th **homology** of the complex, and is denoted $H_i(E)$. The homology forms its own chain complex,

$$\dots \longrightarrow H_{i-1}(E) \longrightarrow H_i(E) \longrightarrow H_{i+1}(E) \longrightarrow \dots$$

(I think all the maps in this complex are just the zero map.)

Definition 1.34. Let R be a ring and let (E_i, d_i) and (E'_i, d'_i) be chain complexes of R-modules. Let $f_i : E_i \to E'_i$ be a morphism of degree zero, so we have the commutative diagram

$$\begin{array}{ccc}
E'_{i-1} & \xrightarrow{f_{i-1}} & E_{i-1} \\
{\scriptstyle d'_{i-1}}\big\downarrow & & \big\downarrow{\scriptstyle d_{i-1}} \\
E'_i & \xrightarrow{f_i} & E_i \\
{\scriptstyle d'_i}\big\downarrow & & \big\downarrow{\scriptstyle d_i} \\
E'_{i+1} & \xrightarrow[f_{i+1}]{} & E_i
\end{array}$$

By commutativity of the top square, $\operatorname{im} f_i \subset \operatorname{im} d_{i-1}$, so we can think of f_i as a map $f_i : \operatorname{im} d'_{i-1} \to \operatorname{im} d_{i-1}$. By commutativity of the bottom square, $f(\ker d'_i) \subset \ker d_i$, so we can also think of f_i as a map $f_i : \ker d'_i \to \ker d_i$. Thus there is an induced map $H_i(f) : \ker d'_i / \operatorname{im} d'_{i-1} \to \ker d_i / \operatorname{im} d_{i-1}$, that is, $H_i(f) : H_i(E') \to H_i(E)$. $H_i(f)$ is the **induced map on homology**. The sequence of maps $H_i(f)$ is a morphism of chain complexes between $H(E')$ and $H(E)$, and this map is denoted $f_* : H(E') \to H(E)$.

1.9 Projective Modules

For the following, let A be a ring. We work in the category of A-modules, so all homomorphisms are homomorphisms of A-modules.

Definition 1.35. Let A be a ring. An A-module P is **projective** if any of the following hold:
(1) Given a homomorphism $f : P \to M''$ and a surjective homomorphism $g : M \to M''$, there exists a homomorphism $h : P \to M$ so that $g \circ h = f$. That is, given a commutative diagram as below, the dotted line can be filled in.

$$\begin{array}{ccccc}
 & & P & & \\
 & {\scriptstyle h}\swarrow & \big\downarrow{\scriptstyle f} & & \\
M & \xrightarrow{g} & M'' & \longrightarrow & 0
\end{array}$$

(2) Every exact sequence $0 \to M' \to M'' \to P \to 0$ splits.
(3) There exists a module M so that $P \oplus M$ is free.
(4) The functor $M \mapsto \operatorname{Hom}_A(P, M)$ is exact.
(This is both a definition and a theorem. The needed theorem states that these definitions are in fact equivalent.)

1.10 Injective Modules

Definition 1.36. Fix a ring R, and let I be an R-module. An R-module I is **injective** if any of the following hold.
(1) Given an exact sequence $0 \to M' \to M$ of R-modules and a homomorphism $f : M' \to I$, there exists h so that the following diagram commutes.

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \big\downarrow f & \swarrow h & \\ & & I & & \end{array}$$

(2) The functor $M \mapsto \mathrm{Hom}_R(M, I)$ is exact.
(3) Every exact sequence $0 \to I \to M \to M'' \to 0$ splits.
(This is both a definition and a theorem. The theorem says that these things are in fact equivalent. So this complex is trivial, but still sometimes useful to think about.)

1.11 Homotopies of Morphisms of Complexes

Definition 1.37. Let R be a ring, and let (E_n, d_n) and (E'_n, d'_n) be chain complexes of R-modules. Let $f, g : E \to E'$ be morphisms of complexes of degree zero. Then f is **homotopic** to g if there exist homomorphisms $h_n : E_n \to E'_{n-1}$ so that

$$f_n - g_n = d'_{n-1}h_n + h_{n+1}d_n$$

2 Field Theory

2.1 Review of Rings and Polynomials

Definition 2.1. Let A be an integral domain. An element $a \neq 0$ is **irreducible** if it is not a unit and the equation $bc = a$ implies that one of b, c is a unit.

Definition 2.2. Let A be a subring of a commutative ring B. For $b \in B$, the **evaluation homomorphism** $\mathrm{ev}_b : A[x] \to B$ is defined by $f \mapsto f(b)$. (It is a ring homomorphism.)

2.2 Algebraic Extensions

Definition 2.3. Let F be a field. An **extension field** of F is a field E such that $F \subset E$. This is also denoted $\boldsymbol{E/F}$. (This latter notation, though similar looking, is unrelated to the notation for quotients of groups and rings.)

Definition 2.4. Let F be a field and E a field extension. The dimension of E as a vector space over F is denoted $\boldsymbol{[E : F]}$.

Definition 2.5. Let E be a field extension of F. This is a **finite extension** if $[E : F]$ is finite, and an **infinite extension** if $[E : F]$ is infinite.

Definition 2.6. Let F be a subfield of a field E. An element $\alpha \in E$ is **algebraic over F** if it is the solution to a polynomial equation with coefficients in F. That is, there exist $a_0, \ldots, a_n \in F$ so that

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$$

where not all a_i are zero. Equivalently, α is algebraic over F if the evaluation homomorphism $F[x] \to E$ given by $f \mapsto f(\alpha)$ has nontrivial kernel.

Definition 2.7. Let E be a field extension of F. If every element of E is algebraic over F, then E is an **algebraic extension** of F.

Definition 2.8. Let F be a subfield of a field E. An element $\alpha \in E$ is a **variable** over F or **transcendental** over F if it is not algebraic.

Definition 2.9. Let E be a field extension of a field F, and let $\alpha \in E$ be algebraic. Let $\text{ev}_\alpha : F[x] \to E$ be the evaluation homomorphism $f \mapsto f(\alpha)$. Since $F[x]$ is a principal ideal domain, the kernel is generated by a monic polynomial $p(x)$. Then

$$F[x]/\langle p(x)\rangle \cong F[\alpha]$$

Because $F[\alpha]$ is an integral domain, $\langle p(x)\rangle$ is prime, so $p(x)$ is irreducible. We can always divide p by a unit so to get a monic polynomial. This monic polynomial is uniquely determined by α and F, so it is called the **irreducible polynomial of $\boldsymbol{\alpha}$ over $\boldsymbol{F}$**, and denoted $\text{Irr}(\alpha, F)$.

Definition 2.10. A **tower of fields** is a sequence

$$F_1 \subset F_2 \subset \ldots \subset F_n$$

of extension fields.

Definition 2.11. A tower of fields is **finite** if each extension is finite

Definition 2.12. Let $k \subset E$ be a field extension and $\alpha \in E$. Then $\boldsymbol{k(\alpha)}$ is the smallest subfield of E containing k and α.

Definition 2.13. Let $k \subset E$ be a field extension and $\alpha_1, \ldots, \alpha_n \in E$. Then $\boldsymbol{k(\alpha_1, \ldots, \alpha_n)}$ is the smallest subfield of E containing k and $\alpha_1, \ldots, \alpha_n$. Note that

$$k(\alpha_1, \alpha_2) = \Big(k(\alpha_1)\Big)(\alpha_2)$$

Also note that

$$k(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in k[x_1, \ldots, x_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

Definition 2.14. Let $k \subset E$ be a field extension. E is **finitely generated** over k if there exist $\alpha_1, \ldots, \alpha_n \in E$ so that $E = k(\alpha_1, \ldots, \alpha_n)$.

Definition 2.15. Let E, F, L be fields such that $E, F \subset L$. The **compositum** of E and F, denoted $\boldsymbol{EF}$, is the smallest subfield of L containing both E and F. More precisely, we should refer to EF as the compositum of E and F **in $\boldsymbol{L}$**.

Definition 2.16. Let $\{F_i\}_{i \in I}$ be a family of subfields of L. The **compositium** of the family is the smallest subfield of L containing each F_i.

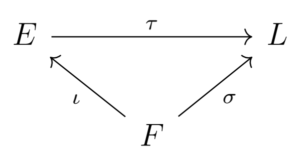
Definition 2.17. Let $\mathcal{C}$ be a class of extension fields $F \subset E$. $\mathcal{C}$ is **distinguished** if it satisfies

1. For any tower $k \subset F \subset E$, the extension $k \subset E$ is in $\mathcal{C}$ if and only if $k \subset F$ and $F \subset E$ are in $\mathcal{C}$.
2. If $k \subset E$ is in $\mathcal{C}$, and $k \subset F$ is any extension, and E, F are both contained in some field, then $F \subset EF$ is in $\mathcal{C}$.
3. If $k \subset F$ and $k \subset E$ are in $\mathcal{C}$ and E, F are contained in some field, then $k \subset EF$ is in $\mathcal{C}$.

Note that (3) is a consequence of (1) and (2), so to check that a class is distinguished it suffices to prove that (1) and (2) hold.

2.3 Algebraic Closure

Definition 2.18. Let E, F, L be fields with $F \subset E$ and $\sigma : F \to L$ be an embedding. An embedding $\tau : E \to L$ is **over** σ if $\tau|_F = \sigma$. This is equivalent to saying that τ **extends** σ. If $L = F$ and $\sigma = \mathrm{Id}_F$, then τ is an **embedding of E over F**. That is, the following diagram commutes.



where $\iota : F \hookrightarrow E$ is the inclusion.

Definition 2.19. A field k is **algebraically closed** if every polynomial $k[x]$ of degree ≥ 1 has a root in k.

Definition 2.20. Let k be a field. Let $\overline{k}$ be the unique algebraically closed field such that $k \subset \overline{k}$ is an algebraic extension (existence and uniqueness are theorems). The field $\overline{k}$ is the **algebraic closure** of k.

2.4 Splitting Fields and Normal Extensions

Definition 2.21. Let k be a field and let $f \in k[x]$ with degree ≥ 1. A **splitting field** of f is an extension K of k such that f splits into linear factors in $K[x]$ and K is generated over k by the roots of f.

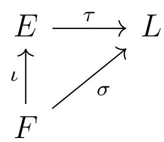
Definition 2.22. Let k be a field. An extension $k \subset K$ is **normal** if K is the splitting field of a family of polynomials in $k[x]$.

2.5 Separable Extensions

Definition 2.23. Let F, E, L be fields with L algebraically closed and $F \subset E$ and let $\sigma : F \to L$ be an embedding. Define

$$S_\sigma = \{\tau : E \to L : \tau|_F = \sigma\}$$

That is, S_σ is the set of possible extensions of σ to E.



The size of S_σ is the **separable degree** of the extension $F \subset E$, and denote $[E : F]_s$. (It is a theorem that the size of S_σ is independent of σ.)

Definition 2.24. Let $k \subset E$ be a finite extension. It is **separable** if $[E : k]_s = [E : k]$.

Definition 2.25. Let k be a field with algebraic closure $\overline{k}$. An element $\alpha \in \overline{k}$ is **separable over** k if $k(\alpha)$ is separable over k. Equivalently, α is separable if $\operatorname{Irr}(\alpha, k)$ has no repeated roots.

Definition 2.26. Let k be a field. A polynomial $f \in k[x]$ is **separable** if it has no multiple roots. (Any root of a separable polynomial is separable.)

Definition 2.27. Let $k \subset E$ be an extension. E is **separable** over k if every extension $k(\alpha_1, \ldots, \alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in E$ is separable over k.

Definition 2.28. Let k be a field with algebraic closure $\overline{k}$. The **separable closure** of k is the compositum of all separable extension of k in $\overline{k}$.

Definition 2.29. Let k be a field and $\alpha \in \overline{k}$ be algebraic over k. Let $\sigma_1, \ldots, \sigma_r$ be the distinct embeddings of $k(\alpha)$ into $\overline{k}$ over k. The **conjugates** of α in $\overline{k}$ are the elements $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$. (These are the distinct roots of $\operatorname{Irr}(\alpha, k)$.)

Definition 2.30. Let $k \subset E$ be a field extension. If there exists $\alpha \in E$ so that $E = k(\alpha)$, then α is a **primitive element** of E over k.

Definition 2.31. A field k is **perfect** if $k^p = k$ or k has characteristic zero.

2.6 Finite Fields

Definition 2.32. Let F_q be a finite field with $q = p^n$ elements. The **Frobenius map** is the map $F_q \to F_q$ given by $x \mapsto x^p$. (It is an automorphism of fields.)

2.7 Inseparable Extensions

Definition 2.33. Let k be a field, and $f \in k[x]$. Given $\alpha \in \overline{k}$, we can write f as $(x-\alpha)^m g(x)$ where α is not a root of g. The **multiplicity** of α as a root of f is m.

Definition 2.34. Let $k \subset E$ be a finite extension. The **inseparable degree** is the quotient

$$\frac{[E : k]}{[E : k]_s}$$

which is also denoted $[E : k]_i$.

2.8 Galois Theory

Definition 2.35. Let K be a field and let G be a group of automorphisms of K. The **fixed field** of G is the set

$$K^G = \{x \in K : \sigma(x) = x, \ \forall \sigma \in G\}$$

(Note that this set is in fact always a field.)

Definition 2.36. A **Galois extension** is an algebraic, normal, and separable field extension.

Definition 2.37. Let $k \subset K$ be a Galois extension. The **Galois group** of K over k is the group of automorphisms of K that fix k,

$$\textbf{Gal}\,(\boldsymbol{K/k}) = \{\sigma : K \to K \ : \ \sigma|_k = \mathrm{Id}_k\}$$

Definition 2.38. Let $k \subset K$ be a Galois extension, and let F be an intermediate field $k \subset F \subset K$. The group **associated** to F is $\mathrm{Gal}(K/F)$. (It is a subgroup of $\mathrm{Gal}(K/k)$.)

Definition 2.39. Let $k \subset K$ be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. A subgroup $H \subset G$ **belongs** to an intemediate field F (where $k \subset F \subset K$) if $H = \mathrm{Gal}(K/F)$.

Definition 2.40. A Galois extension is **cyclic** if the Galois group is cyclic.

Definition 2.41. A Galois extension is **abelian** if the Galois group is abelian.

2.9 Computing Galois Groups of Polynomials

Definition 2.42. Let k be a field and let $f \in k[x]$ be a separable polynomial of degree ≥ 1. Let K be the splitting field of k, and let $G = \mathrm{Gal}(K/k)$. Then G is the **Galois group** of f.

Definition 2.43. Let $f(x) = x^3 + ax + b \in k[x]$. The **discriminant** of f is $\Delta(f) = -4a^3 - 27b^2$.

2.10 Roots of Unity

Definition 2.44. Let k be a field. A **root of unity** is an element $\zeta \in \overline{k}$ that is a root of $x^n - 1$ for some $n \in \mathbb{N}$. Note that if $\operatorname{char} k = p$, then $x^{p^m} - 1$ has a unique root (1) and thus there is no p^mth root of unity except 1. However, if $n > 1$ is not divisible by $\operatorname{char} k$, then $x^n - 1$ is separable (look at the derivative) so there are exactly n distinct nth roots of unity.

Definition 2.45. Note that nth roots of unity form a cyclic group under multiplication. This group is denoted $\boldsymbol{\mu}_n$. A generator for this group is a **primitive $\boldsymbol{n}$th root of unity**.

Definition 2.46. Let k be a field of characteristic zero, and let $\zeta_n \in \overline{k}$ be a primitive nth root of unity. We can factor $x^n - 1$ into linear factors in $k(\zeta_n)$ as

$$x^n - 1 = \prod_{\zeta}(x - \zeta)$$

An nth root of unit ζ has **period** d if $\zeta^d = 1$. The dth **cyclotomic polynomial** is $\Phi_d(x)$ defined by

$$\Phi_d(x) = \prod_{\text{period } \zeta = d} (x - \zeta)$$

Note that we can also write $\Phi_n(x)$ as

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} \Phi_d(x)}$$

Note that the roots of $\Phi_n(x)$ are precisely the primitive nth roots of unity, so $\deg \Phi_n(x) = \phi(n)$ (Euler totient function). Note also that Φ_n is irreducible.

Definition 2.47. Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, where p is an odd prime. For $v \in \mathbb{Z}\backslash\{0\}$ not divisible by p, we define the **Legendre symbol**, also called the **quadratic symbol**,

$$\left(\frac{v}{p}\right) = \begin{cases} 1 & v \equiv x^2 \pmod{p} \text{ for some } x \\ -1 & v \not\equiv x^2 \pmod{p} \text{ for all } x \end{cases}$$

2.11 Linear Independence of Characters

Definition 2.48. Let G be a monoid and k a field. A **character** of G in k is a monoid homomorphism $G \to k^\times$ (into the multiplicative group of nonzero elements of k). The **trivial character** is the character $x \mapsto 1$. (Note: Groups are monoids, so $k^\times$ is a monoid.)

Definition 2.49. Let G be a monoid and k a field. A set of characters $f_i : G \to k$ are **linearly independent** if the only linear combination of the f_i over k equal to zero is the trivial one. That is,

$$\sum_i a_i f_i = 0 \implies a_i = 0 \; \forall i$$

where $a_i \in k$.

2.12 Norm and Trace

Definition 2.50. Let E/k be a finite field extension, with $[E : k]_s = r$ and $[E : k]_i = p^\mu$. (If $\operatorname{char} k = 0$ then $[E : k]_i = 1$.) Let $\sigma_1, \ldots, \sigma_r$ be the distinct embeddings of E into $\overline{k}$. For $\alpha \in E$, the **norm** of α is

$$N_{E/k}(\alpha) = N_k^E(\alpha) = \prod_{m=1}^{r} \sigma_m\left(\alpha^{p^\mu}\right) = \left(\prod_{m=1}^{r} \sigma_m\left(\alpha\right)\right)^{[E:k]_i}$$

Note that if E/k is separable, then $[E : k]_i = 1$ so the norm can be written much more simply as

$$N_{E/k}(\alpha) = \prod_{m=1}^{r} \sigma_m(\alpha)$$

Definition 2.51. Let E/k be a finite field extension, with $[E:k]_s = r$ and $[E:k]_i = p^\mu$. (If $\operatorname{char} k = 0$ then $[E:k]_i = 1$.) Let $\sigma_1, \ldots, \sigma_r$ be the distinct embeddings of E into $\overline{k}$. For $\alpha \in E$, the **trace** of α is

$$\operatorname{Tr}_{E/k}(\alpha) = \operatorname{Tr}_k^E(\alpha) = [E:k]_i \sum_{m=1}^{r} \sigma_m(\alpha)$$

Note that if E/k is not separable, then $[E:k]_i$ is divisible by $p = \operatorname{char} k$, so $[E:k]_i = 0$, so the trace is zero. If E/k is separable, then

$$\operatorname{Tr}_{E/k}(\alpha) = \sum_{m=1}^{r} \sigma_m(\alpha)$$

2.13 Solvable and Solvable by Radicals

Definition 2.52. A finite separable extension E/k is **solvable** if there exists a finite Galois extension K/k with $k \subset E \subset K$ such that $\operatorname{Gal}(K/k)$ is a solvable group.

$$\begin{array}{c} K \\ | \\ E \\ | \\ F \end{array}$$

Definition 2.53. A finite separable extension E/k is **solvable by radicals** if there is a finite extension K/k such that $k \subset E \subset K$ and there is a tower

$$k = K_0 \subset K_1 \subset \ldots \subset K_m = K$$

where each step of the tower K_{i+1}/K_i is one of the following types:

1. It is formed by attaching a root of unity.
2. It is formed by attaching a root of $x^n - a$ with $a \in K_i$ where $\gcd(n, \operatorname{char} k) = 1$.
3. (Only when $\operatorname{char} k = p > 0$) It is formed by attaching a root of $x^p - x - a$ with $a \in K_i$.