Algebra I&II – Summary
Source Code at
https://github.com/kimhanm/kimhanm.github.io

Han-Miru Kim

June 18, 2021

1 Rings

Definition

An element $a \in R \setminus \{0\}$ is called a **zero divisor** (Nullteiler), if there exists a $b \in R \setminus \{0\}$ with $ab = 0$. A ring $R \neq \{0\}$ is called an **integral domain** (Integritätsbereich), if it has no zero divisors. This is equivalent to asking that the following holds

$$ab = ac \wedge a \neq 0 \implies b = c$$

Proposition

- Every subring of an integral domain is again an integral domain.
- Every field is an integral domain.
- $Z/n\mathbb{Z}$ is an integral domain $\iff$ n is prime.

Definition

In a commuative ring R, $a, b \in R$ we say that a **divides** b, (write $a|b$) if there exists a $c \in R$ with $b = ac$. Define the **group of units** (Einheitengruppe)

$$R^\times := \{a | a \text{ divides } 1\}$$

If $b = ac$ for some unit $c \in R^\times$, write $b \sim a$ and we say that a and b are **associated**.

Proposition

- $a \sim b \implies a|b$ and $b|a$

- If R is an integral domain, then $a \sim b \Leftarrow a|b$ and $b|a$.

Definition

Let R be an integral domain. It's **quotient field** (Quotientenkörper) is the field

$$\mathrm{Quot}(R) := {}^{R \times (R \setminus \{0\})}\!/\!_{\sim}, \quad (a,b) \sim (p,q) \iff aq = bp$$

and write $\frac{a}{b} = [(a,b)]_\sim$. There is a canonical inclusion

$$\iota : R \hookrightarrow \mathrm{Quot}(R), \quad x \mapsto \frac{x}{1}$$

- $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$
- Because $i^2, \sqrt{2}^2 \in \mathbb{Z}$ we have $\mathrm{Quot}(\mathbb{Z}[i]) = \mathrm{Quot}(Z)[i]$, $\mathrm{Quot}(\mathbb{Z}[\sqrt{2}]) = \mathrm{Quot}(\mathbb{Z})[\sqrt{2}]$

Definition

For a commutative ring R, the **polynomial ring** (with variable X) is the collection of finite power series

$$R[X] := \left\{ \sum_{k=0}^{n} a_k X^k | a_k \in R n \in \mathbb{N} \right\}$$

with coefficient-wise addition and Cauchy-multiplication

$$\left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{k=0}^{m} b_k X^k\right) = \sum_{k=0}^{n+m} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j$$

To construct this ring, we start with the set of all sequences $(a_n)_{n\in\mathbb{N}} \in R^{\mathbb{N}}$ and identify $(0,1,0,\ldots) =: X$. Every polynomial $f \in R[X]$ induces a function $f : R \to R, x \mapsto f(x)$, but the mapping

$$R[X] \to \mathrm{End}_{\mathsf{Set}}(R), f \mapsto (x \mapsto f(x))$$

is not injective. (i.e $X^2 + X \in \mathbb{F}_2[X]$)
The ring of formal power series is denoted by $R[\![X]\!]$

Definition

For $f \in R[X]$ define its **degree**

$$\deg(f) = \sup\{n \in \mathbb{N} | a_n = 0\}$$

in particular $\deg(0) = -\infty$.

Proposition

If R is an integral domain, then so is $R[X]$ and

- $\deg(fg) = \deg(f) + \deg(g)$
- $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
- $(R[X])^\times = R^\times$. (In general, only $R^\times \subseteq R[X]^\times$, For example $2X+1 \in \mathbb{Z}/4\mathbb{Z}[X]$ is invertible.)

Definition

For $n \in \mathbb{N}$, define the polynomial ring in n-variables inductively as

$$R[X_1, \dots, X_n] = \begin{cases} R & n = 0 \\ R[X_1, \dots, X_{n-1}][X_n] & n > 0 \end{cases}$$

This ring has multiple degree functions, $\deg_{X_1}, \dots, \deg_{X_n}$ or $\deg_{\text{tot}}$.
For a field K, define the field of **rational functions** in n-variables as

$$\begin{aligned} K(X1, \dots, X_n) &:= \text{Quot}(K[X_1, \dots, X_n]) \\ &= \{\frac{f}{g} | f, g \in K[X_1, \dots, X_n], g \neq 0\} \end{aligned}$$

Theorem

For the canonical inclusion $\iota : R \to R[X_1, \dots, X_n]$, n-elements $x_1, \dots, x_n \in S$, any ringhomormophism $\varphi : R \to S$ induces a unique ringhomomorphism $\overline{\varphi} : R[X_1, \dots, X_n] \to S$ such that the following diagram commutes

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\iota"'] & & S \\ & R[X_1, \dots, X_n] \arrow[ur, dotted, "\exists! \overline{\varphi}"'] & \end{tikzcd}$$

and $\overline{\varphi}(X_i) = x_i$.

This ringhomomorphism is given by

$$\begin{aligned} &\overline{\varphi}\left(\sum_{k_1, \dots, k_n = 0}^{m} a_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n}\right) \\ &= \sum_{k_1, \dots, k_n = 0}^{m} \varphi(a_{k_1, \dots, k_n}) x_1^{k_1} \dots x_n^{k_n} \in S \end{aligned}$$

2 Ideals

Definition

Let R be a commutative ring. A subset $\mathfrak{a} \subseteq R$ is called an **ideal** if

(a) $\mathfrak{a} \neq 0$

(b) $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$

(c) $\forall a \in \mathfrak{a}, r \in R : ra \in \mathfrak{a}$

Trivially, R itself and $\{0\}$ are ideals. The kernel of a ring homomorphism is an ideal.

Definition

For a commutative ring R and elements $a_1, \ldots, a_n$, define the **ideal generated by** $a_1, \ldots, a_n$ as

$$(a_1, \ldots, a_n) = \{\sum_{k=1}^{n} a_i x_i | x_i \in R\}$$

An ideal $\mathfrak{a}$ is called a **principal ideal** (Hauptideal), if it can be generated by a single element $\mathfrak{a} = (a)$. If every ideal in R is a principal ideal, then R is called a **principal ideal domain** (PID).

A non-principal ideal is $(X, Y) \subseteq Z[X, Y]$

Definition

For ideals $\mathfrak{a}, \mathfrak{b}$ and an element $r \in R$ define

(a) $r \cdot \mathfrak{a} := \{ra | a \in \mathfrak{a}\} \subseteq \mathfrak{a}$

(b) $\mathfrak{a} + \mathfrak{b} := \{a + b | a \in \mathfrak{a}, b \in \mathfrak{b}\} \subseteq \mathfrak{a}, \mathfrak{b}$

(c) $\mathfrak{a}\mathfrak{b} := \{\sum_{k=1}^{n} a_k b_k | a_k \in \mathfrak{a}, b_k \in \mathfrak{b}\} \subseteq \mathfrak{a}, \mathfrak{b}$.

Theorem

The relation $a \sim b \iff a - b \in \mathfrak{a}$ defines an equivalence relation on R and we write $a \equiv b \mod \mathfrak{a}$. The quotient $R/\mathfrak{a}$ is called the **factor ring** (Faktorring) "R modulo $\mathfrak{a}$" with induced addition and multiplication. It allows a surjective ring homomorphism called the canonical projection

$$\rho : R \to R/\mathfrak{a}, \quad x \mapsto x + \mathfrak{a}$$

Lemma

Let $\mathfrak{a}, \mathfrak{b} \subseteq R$ be ideals in a commutative ring. Then

(a) $I = R \iff 1 \in I \iff I \cap R^{\times} \neq \emptyset$

(b) $(a) \subseteq (b) \iff b | a$

Proposition

Let $\varphi : R \to S$ be a ring homomorphism and $\mathfrak{a} \subseteq \operatorname{Ker} \varphi$ an ideal.
This induces a ring homomorphism $\overline{\varphi} : R/\mathfrak{a} \to S$ such that the following diagram commutes.

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\rho"'] & & S \\ & R/\mathfrak{a} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

and if $\mathfrak{a} = \operatorname{Ker} \varphi$, $\overline{\varphi}$ is an isomorphism.

For example, the map

$$\varphi : \mathbb{R}[X] \to \mathbb{C}, X \mapsto i$$

has kernel $(X^2 + 1)$ and gives us the isomorphism $\mathbb{R}/(X^2+1) \cong \mathbb{C}$.

Definition

An ideal $\mathfrak{p} \subseteq R$ is called a **prime ideal**, if $\mathfrak{p} \neq R$ and for all $a, b \in R$ we have

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

. An ideal $\mathfrak{m} \subseteq R$ is a **maximal ideal**, if $\mathfrak{m} \neq R$ and any other ideal containing $\mathfrak{m}$ is either $\mathfrak{m}$ or R. Equivalently, we have

(a) $\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.

(b) $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.

(a) $\mathbb{Z}/(0)$ is a prime ideal, but not a maximal ideal.

(b) For $R = \mathbb{Z}[X]/(X^2)$ we have

$$R/(X) \cong \mathbb{Z}[X]/(X^2, X) \cong \mathbb{Z}$$

so $(X) \subseteq R$ is a prime ideal.

Proposition

Let $\mathfrak{a}_0 \subseteq R$ be an ideal. There exists a correspondence between ideals that contain $\mathfrak{a}_0$ and ideals in $R/\mathfrak{a}_0$ given by

$$\mathfrak{a}_0 \subseteq \mathfrak{a} \subseteq R \leftrightsquigarrow \mathfrak{a} + \mathfrak{a}_0 \subseteq R/\mathfrak{a}_0$$

Theorem Krull's theorem

Assuming Zorn's lemma, for every ideal $\mathfrak{a} \subsetneq R$, there exists a maximal ideal $\mathfrak{a} \subseteq \mathfrak{m}$. In particular, every non-trivial ring has a maximal ideal.

Proposition Meta-Proposition

Every rule about matrices over a field k we know from LinAlg that only uses $+, -, \cdot, 0, 1$ also apply for matrices over a commutative ring R.

The proof of this is non-trivial, we will make use of the following lemma.

Lemma

If a polynomial $f \in \mathbb{R}[X_1, \dots, X_n]$ vanishes on $\mathbb{R}^n$, then $f = 0$.

Proof. Let $f = \sum_{k_1,\dots,k_n} a_{k_1,\dots,k_n} X_1^{k_1} \dots X_n^{k_n}$. If the polynomial vanishes everywhere, then so do its derivatives.
If the polynomial vanishes everywhere, then so do its derivatives. So to eliminate the coefficient $a_{k_1,\dots,k_n}$, all we have to do is to take the derivative with the same multi-index and evaluate at $X = 0$:

$$\partial_{k_1} \dots \partial_{k_n} f(0) = k_1! \dots k_n! a_{k_1,\dots,k_n}$$

□

The meta-proposition follows in that every "calculation rule" (for example $\det(AB) = \det(A)\det(B)$ etc.) can be written as a collection of polynomial equations with integer coefficients!

Definition

A ring R is a **noetherian ring**, if for every sequence of ideals $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots$ there exists a n_0 such that $n \geq n_0 \implies \mathfrak{a}_n = \mathfrak{a}_{n_0}$.

Theorem

Let R be a PID.

(a) R is noetherian

(b) For $a \in R \setminus (R^\times \{0\})$, there exists a prime p with $p|a$.

2.1 Factorisation

For this section, let R be an integral domain.

Definition

An element $p \in R \setminus \{0\}$ is **irreducible**, if $p \notin R^\times$ and for all $a, b \in R$

$$p = ab \implies a \in R^\times \text{ or } b \in R^\times$$

We say $p \in R \setminus \{0\}$ is **prime**, if (p) is a prime ideal. Equivalently, if $p \notin R^\times$ and for all $a, b \in R$

$$p|ab \implies p|a \text{ or } p|b$$

- Every prime $p \in R$ is also irreducible.
- $2 \in Z[i]$ is not irreducible because $2 = (1+i)(1-i)$.
- $2 \in Z[i\sqrt{5}]$ is irreducible, but not prime because $2|6$ but $6 = (1+i\sqrt{5})(1-i\sqrt{5})$.

Definition

An integral domain R is called a **unique factorisation domain** (UFD) (Faktorieller Ring), if every element $a \in R \setminus \{0\}$ can be written as a product of a unit and finitely many prime elements of R.

$$a = up_1 \dots p_n \quad \text{for} \quad u \in R^\times, p_1, \dots, p_n \text{ prime}$$

- Every PID is a UFD
- The factorisation is unique up association and permutation of prime elements.
- In a UFD, p prime $\iff$ p irreducible.
- $\mathbb{Z}[i\sqrt{5}]$ is an integral domain, but not a UFD.

Definition

In a UFD R, a collection $P \subseteq R$ of prime elements is called a **representation set**, if for every prime $q \in R$ there exists a unique $p \in P$ with $q \sim p$.

- Using the axiom of choice, every UFD has a representation set.
- In $R = K[X]$, the following is a representation set

$$P = \{f \in K[X] \big| f \text{ irreducible with leading coefficient } 1\}$$

Theorem

Let R be a UFD and $P \subseteq R$ a representation set. Then every element $a \in R \setminus \{0\}$ has a unique prime factorisation of the form

$$a = u \prod_{p \in P}{}' p^{\mu_p}, \quad u \in R^\times$$

where μ_p is non-zero for only finitely many $p \in P$.
If $a = u \prod_{p \in P} p^{\mu_p}$ and $b = v \prod_{p \in P} p^{\nu_p}$, then

$$a|b \iff \mu_p \leq \nu_p \quad \forall p \in P$$

Definition

Let R be a UFD and $a_1, \dots, a_n \in R$.

- $b \in R$ is called a **common divisor** of $a_1, \dots, a_n$, if $b|a_i$.
- b is called a **greatest common divisor** (gcd,ggT) of $a_1, \dots, a_n$, if for all other common divisors b' we have $b'|b$.
- We say that $a_1, \dots, a_n$ are **coprime**, if the gcd is associated to 1.
- Two ideals $\mathfrak{a}, \mathfrak{b}$ are **coprime**, if $I + J = R$, i.e. $\exists a \in \mathfrak{a}, b \in \mathfrak{b}$ with $a + b = 1$.

Proposition

Let R be a UFD with prepresentation set P. If $a = u \prod_{p \in P} p^{\mu_p}$ and $b = v \prod_{p \in P} p^{\nu_p}$, then a gcd exists and one of them has the form

$$\gcd(a, b) = \prod_{p \in P} p^{\min(\mu_p, \nu_p)}$$

The gcd is unique up to a unit.

Proposition

Let R be a UFD and $K = \mathrm{Quot}(R)$ its quotient field.
Then every $x \in K$ has a representation $x = \frac{a}{b}$ with a, b coprime. of the form

$$x = u \prod_{p \in P}{}' p^{\mu_p}$$

Proposition

In a PID R with elements $a_1, \dots, a_n$ we have

$$(a_1, \dots, a_n) = (\gcd(a_1, \dots, a_n))$$

in particular, there exists a linear combination

$$\sum_{i=1}^{n} x_i a_i \sim \gcd(a_1, \dots, a_n)$$

Theorem Chinese Remainder Theorem

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pairwise coprime ideals. Then the ringhomomorphism

$$\begin{aligned} \varphi : R &\to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n \\ x &\mapsto (x + \mathfrak{a}_1, \dots, x + \mathfrak{a}_n) \end{aligned}$$

is surjective and $\operatorname{Ker}\varphi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

Proposition Simplified Chinese Remainder Theorem

Let R be a PID, $a_1, \ldots, a_n \in R$ pairwise coprime.
Then the map

$$\begin{aligned} R/(a_1 \ldots a_n) &\to R/(a_1) \times \ldots \times R/(a_n) \\ x + (a_1 \ldots a_n) &\mapsto (x + (a_1), \ldots, x + (a_n)) \end{aligned}$$

is an isomorphism.

Definition

An integral domain R is called a **euclidean ring**, if there exists a function $N : \mathbb{R} \setminus \{0\} \to \mathbb{N}$ such that

(a) **Degree inequality:** $N(f) \leq N(fg)$ for all $f, g \in \mathbb{R} \setminus \{0\}$.

(b) **Division with rest:** For $f, g \in R$ with $g \neq 0$ there exist $q, r \in R$ such that $f = qg + r$ with either $r = 0$ or $N(r) < N(f)$. We call q the **quotient** and r the **rest** of the division.

- Any field is a euclidean ring.
- For a field K, $K[X]$ with $N = \deg$ is a euclidean ring.
- $\mathbb{Z}[i]$ with $N(a + ib) = a^2 + b^2$ is a euclidean ring.
- $\mathbb{Z}[\sqrt{2}]$ with $N(a + \sqrt{2}b) = |a^2 - 2b^2|$ (same with $\mathbb{Z}[\sqrt{3}]$)
- $Z[\frac{i+i\sqrt{19}}{2}]$ is a PID but not a euclidean ring.

Theorem Euclidean Algorithm

Let $a_0, a_1 \in R$.

- If $a_n = 0$, we are finished.
- After division with rest, obtain the next lement with $a_n = q_n a_n + a_{n+1}$.
- Repeat. If $a_m = 0$ for the first time, then $\gcd(a_0, a_1) = a_{m-1}$.

2.2 Polynomial Rings II

Let R be a factorial ring and $K = \operatorname{Quot}(R)$ it's quotient field. Then

$$f, g \in K, f \sim_R g \iff \frac{f}{g} \in R^\times$$

Definition

Let R be a UFD and $f = \sum_{i=0}^n a_i X^i \in R[X] \setminus \{0\}$.
The **content** (Inhalt) of f is defined as

$$I(f) := \gcd(a_1, \dots, a_n)$$

we say f is **primitive**, if $I(f) \in R^\times$.

Lemma

For $f \in K[X] \setminus \{0\}$, there exists a $d \in K \setminus \{0\}$ such that $f = df^*$ for $f^* \in R[X]$ primitive. We call d the **content** of f.
Furthermore

(a) $I(af) \sim aI(f)$

(b) $I(fg) \sim I(f)I(g)$

(c) $I(f) \in R \iff f \in R[X]$.

Theorem Gauss

Let R be a UFD. Then $R[X]$ is a UFD and $R[X]$ has exactly two types of prime elmements.

- $f = p \in R$ prime
- $f \in R[X]$ primitive such that f is irreducible as an element of $K[X]$.
- Let $f \in R[X]$ primitive. Then f is irreducible in $R[X]$ if and only if it is irreducible in $K[X]$.

Let R be a UFD and p prime. The inclusion $\iota : R \to R/(p), a \mapsto \overline{a} = a + (p)$ induces a ringhomomorphism

$$R[X] \to R/(p)[X], \quad f = \sum_{k=0}^n a_k X^k \mapsto \overline{f} = \sum_{k=0}^n \overline{a}_n X^k$$

Proposition

If $f \in R[X] \setminus \{0\}$ satisfies $\deg(f) = \deg(\overline{f})$ and $\overline{f} \in R/(p)[X]$ is irreducible, then f is irreducible.

Theorem Eisenstein Criterion

Let R be a UFD and $p \in R$ prime, $f = \sum_{i=1}^n a_i X^i$ primitive such that

$$p \not| a_n, p | a_i, 0 \leq i < n, p^2 \not| a_0$$

then f is irreducible.

Proof. Let $f = gh$ be a non-trivial decomposition. Since f is primitive and $I(gh) \sim I(g)I(h)$ both g and h must be primitive.
Take the equation $f = gh$ modulo p. Because all non-leading coefficients of f vanish, we are left with

$$\overline{f} = \overline{g}\overline{h} = a_n X^n$$

so $\overline{g}, \overline{h}$ must be of the form

$$\overline{g} = b_k X^k, \quad \overline{h} = c_l X^l$$

with $k, l > 0$. Because the constant terms of g, h vanished, it means that p must divide both b_0, c_0. But $a_0 = b_0 c_0$, which contradicts $p^2 \not| a_0$. □

A common trick is to take a polynomial $f(X)$ and use the substitution $Y = X + 1$ and look at $f(Y)$. This trick is commonly used with the Eisenstein criterion to show irreducibility.

3 Modules

Modules are to ring what vector spaces are to fields.

Definition

For a ring R, an R**-module** M is an abelian group with scalar multiplication

$$R \times M \to M, \quad (a, m) \mapsto a \cdot m$$

For an index set I, we define the **free** R**-module**

$$R^{(I)} := \{x : I \to R | x_i = 0 \text{ for almost all } i\}$$

Any free module is isomorphic to $R^{(I)}$ for some set I.
For R-modules M, N, **module homomorphism** over R is a group homomorphism $\Phi : M \to N$ that satisfies

$$\Phi(am) = a\Phi(m) \quad \forall a \in R, m \in M$$

Definition

Let M be an R-module. An element $m \in M$ is called a **torsion element** of M, if there exists an $a \in R \setminus \{0\}$ with $a \cdot m = 0$.
Write M_{tor} for the set of torsion elements of M.
We say that M is a **torsion-module**, if $M_{\text{tor}} = M$ and we say that M is **torsion-free**, if $M_{\text{tor}} = \{0\}$.

- Every ideal $\mathfrak{a} \subseteq R$ is an R-module.
- If R is a PID, then $\mathfrak{a}$ is a free R-module.
- An abelian group is a $\mathbb{Z}$-module with $n \cdot g = g^n$. Taking $a = \text{ord}(g)$, we see that G is a torsion-module.
- $M = \mathbb{Q}/\mathbb{Z}$ is a torsion module over $\mathbb{Z}$.
- If R is an integral domain and M is a free R-module, then M is torsion-free.

Theorem Classification theorem

Let R be a PID and M a finitely generated R-module.
Then there exist $d_1|d_2|\ldots|d_n \in R \setminus \{0\}$ such that

$$M \cong R^r \times R/(d_1) \times \ldots \times R/(d_n)$$

alternatively, we can write

$$M \cong R^r \times \prod_{j=1}^{n} M_{\text{tors}}^{(p_i)}$$

where $p_1, \ldots, p_n$ are non-conjugate primes in R and

$$\begin{aligned} M_{\text{tors}}^{(p_i)} &:= \{m \in M_{\text{tors}} | \exists k \in \mathbb{N} \text{ with } p_i^k m = 0\} \\ &\cong R/(p_j^{n_{j,1}} \times \ldots \times R/(p_j^{n_{j,k}}) \end{aligned}$$

4 Groups

Notation

- $G \cong H$: G is isomorphic to H
- $H < G$: H is a subgroup of G.

Examples of groups

- $\mathrm{GL}(n, K), \mathrm{SL}(n, K), \mathrm{O}(n), \mathrm{SO}(n), \mathrm{U}(n), \mathrm{SU}(n), \mathrm{SP}(2n), O(p, q)$
- S_n, Dihedral group D_{2n} of order $2n$
- $\mathrm{Aut}(k), \mathrm{Aut}(G), \mathrm{Bij}(X)$.
- Vector spaces, $R^\times$, $\pi_1(X, x_0)$.

Example Dihedral group

For $n \in \mathbb{N}$, the dihedral group D_{2n} (in physics D_n) is the symmetry group of a regular n-gon embedded in $\mathbb{R}^2$ and has order $2n$.
If R is rotation with angle $\frac{2\pi}{n}$ and T is mirroring around the x-axis, the dihedral group can be written as

$$\begin{aligned} D_{2n} &= \{1, R, R^2, \ldots, R^{n-1}, T, RT, R^2T, \ldots, R^{n-1}T\} \\ &= \langle R, T | T^2 = 1, R^n = 1, RT = R^{-1} \rangle \end{aligned}$$

Definition

Let G be a group and $A \subseteq G$ a subset. The **subgroup generated by** A is the smallest subgroup that contains A:

$$\langle A \rangle := \bigcap_{X \subseteq H < G} H$$

It can alternatively be written as the set

$$\langle A \rangle = \{a_1^{k_1} \dots a_n k^n | n \in \mathbb{N}, a_1, \dots, a_n \in A, k_i = \pm 1\}$$

Definition

The **commutator** of two elements $g, h \in G$ is $[g, h] := ghg^{-1}h^{-1}$. The **commutator group** of G is the subgroup

$$[G, G] := \langle \{[g, h] | g, h \in G\} \rangle$$

Definition

For every $g \in G$, the mapping

$$\gamma_g : G \to G, \quad x \mapsto gxg^{-1}$$

is an automorphism, called a **inner automorphism**.
This induces a mapping

$$\Phi : G \to \mathrm{Aut}(G), \quad g \mapsto \gamma_g$$

The kernel of Φ is called the **center**

$$Z(G) = \{g \in G | \forall x \in G : [x, g] = 1\}$$

We say that two elements $x, y \in G$ are **conjugate**, if there exists a $g \in G$ such that $\gamma_g(x) = gxg^{-1} = y$.

- The center is obviously commutative, and the commutator group is not.
- Two matrices are conjugate, if and only if they have the same normal form.
- If the group is abelian, then every inner automorphism is trivially the identity id_G.

Definition

Let $X, Y \subseteq G$ be subsets and $g \in G$. We define

$$\begin{aligned} XY &= \{xy | x \in X, y \in Y\} \\ gX &= \{gx | x \in X\} \\ Xg &= \{xg | x \in X\} \\ X_g &= \{\gamma_g(x) | x \in X\} \\ g_X &= \{\gamma_x(g) | x \in X\} \\ X^{-1} &= \{x^{-1} | x \in X\} \end{aligned}$$

For a subgroup $H < G$, we define the set of **left-subclasses** (Linksnebenklassen)

$$G/H := \{gH | g \in G\}$$

and analogously the right-subclasses $H \backslash G$.
The **index** of the subgroup is

$$[G : H] := |G/H| = |H \backslash G|$$

Proposition

Let $g, g' \in G$, $H < G$. Then

$$gH = g'H \iff gH \cap g'H \neq \emptyset \iff g \in g'H$$

Theorem Lagrange

If $|G| < \infty$, then $|G| = |G/H| \cdot |H|$.

Proof sketch. Show that the map

$$\Phi : G/H \times H \to G, \quad (xH, h) \mapsto xh$$

is bijective. □

As a corollary, the index of every subgroup is a divisor of the order of the group.

4.1 Normal divisors

The set of left-subclasses is not always a group. For example in $G = D_{2 \cdot 3}$, we have $R\langle T \rangle R \langle T \rangle \neq R^2 \langle T \rangle$.

Definition

A subgroup $H < G$ is called a **normal divisor** (write $H \lhd G$) if

$$\pi : G \to G/H, \quad g \mapsto gH$$

is a group homomorphism.
We call G simple, if only $\{e\}$ and G itself are the only normal divisors of G.

- Every subgroup of an abelian group is normal.
- Every subgroup of index 2 is normal.

Theorem

Let $N < G$ be a subgroup. Then the following are equivalent

(a) $N \lhd G$

(b) $xN = Nx$ for all $x \in G$

(c) There exists a group homomorphism $\varphi : G \to S$ with $\operatorname{Ker}\varphi = N$

(d) $(xH)(yH) = (xy)H$ for all $x, y \in G$

Proposition Universal property of Normal divisors

Let $\varphi : G \to H$ and $N \lhd G$ with $N \subseteq \operatorname{Ker}\varphi$. Then there exists a unique group homomorphism $\overline{\varphi} : G/N \to H$ such that the following diagram commutes

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & H \\ & G/N \arrow[ur, "\exists!\overline{\varphi}"'] & \end{tikzcd}$$

Theorem First isomorphism Theorem

Let $\varphi : G \to H$ be a group homomorphism.
Then φ induces an isomorphism $\overline{\varphi} : G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ such that the following diagram commutes

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & H \\ G/\operatorname{Ker}\varphi \arrow[r, "\overline{\varphi}"] & \operatorname{Im}\varphi < H \arrow[u, "\iota"] \end{tikzcd}$$

where π is the canonical projection and ι is the inclusion mapping.

Proposition Second Isomorphism Theorem

Let $N \lhd G$ and $H < N$. Then

$$N \cap H \lhd H, \quad N \lhd HN$$
$$H/(N \cap H) \cong HN/N = NH/N < G$$

And in particular, $N \lhd G$, $N < H < G \implies N \lhd H$.

Proposition Third Isomorphism Theorem

Let $N \lhd G$. Then there exists a correspondence between subgroups that contain N and subgroups of H/N.
For such subgroups $N < H < G$

$$H/N \lhd G/N \iff H \lhd G$$

and we have an isomorphism

$$G/N \big/ H/N \cong G/H$$
$$(gN)(H/N) \leftrightsquigarrow gH$$

This corollary mirrors the one for ideals in a ring.

Proposition

Let $N \triangleleft G$. For any other group H, there exists a natural isomorphism

$$\mathrm{Hom}(G/N, H) \cong \{\varphi \in \mathrm{Hom}(G, H) | \varphi|_N = e_H\}$$

4.2 Group actions

Definition

Let G be a group and X a set. A **group action** (or left action) of G on X s a map

$$\cdot : G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

that is compatible with the group structure on G, i.e. such that for all $x \in X, g, g' \in G$

$$e \cdot x = x, \quad g \cdot (g' \cdot x) = (gg') \cdot x$$

We call X a G-set.

Equivalently, a group action corresponds to a group homomorphism

$$\rho : G \to \mathrm{Bij}(X), \quad g \mapsto (\rho(g) : x \mapsto g \cdot_\rho x)$$

, where $\mathrm{Bij}(X)$ is the group of bijective maps $X \to X$ called the **permutation group** of X. Analogously, we can define a right action $\tilde{\cdot} : X \times G \to X$ which corresponds to a left action

$$x \tilde{\cdot} g = g^{-1} \cdot x$$

Definition

Let X, Y be G-sets.

- A G-**morphism** is a map $f : X \to Y$ such that

$$f(g \cdot x) = g \cdot f(x) \quad \forall g \in G, x \in X$$

- A subset $A \subseteq X$ is called an **invariant** of the action, if $g \cdot A = A$ for all $g \in G$. Likewise, an element $x \in X$ is called a **fixpoint**, if $g \cdot x = x \forall g \in G$.
- For $x \in X$, denote its **orbit** by

$$Gx = \mathcal{O}_G(x) := \{g \cdot x | g \in G\} \subseteq X$$

and its **stabilizer** by

$$\mathrm{Stab}_G(x) := \{g \in G | gx = x\} \subseteq G$$

Write $G \backslash X$ for the set of orbits.

- If the group action $\rho : G \to \mathrm{Bij}(X)$ is injective, the group action is called **faithful**.

- The action is called **transitive**, if for every pair $x, y \in X$ there exists a $g \in G$ such that $g \cdot x = y$ and it's called **sharply transitive**, if such a g is uniquely determined.

Theorem Orbit Stabilizer Theorem

Let X be a G-set, $x_0 \in X$. Then $\mathrm{Stab}_G(x_0) \lhd G$ and $\mathcal{O}_G(x_0)$ are invariant under the action and the map

$$G/\mathrm{Stab}_G(x_0) \to \mathcal{O}_G(x_0), \quad g\mathrm{Stab}_G(x_0) \mapsto g\mathcal{O}_G(x_0)$$

is an isomorphism of G-sets.

- If $|G| < \infty$, then

$$|G| = |\mathcal{O}_G(x_0)| \cdot |\mathrm{Stab}_G(x_0)|$$

Proposition

Let X be a finite G-set. Then

$$|X| = |\mathrm{Fix}_G(X)| + \sum_{|\mathcal{O}_G(x)|>1} [G : \mathrm{Stab}_G(x)]$$

4.3 Symmetric groups

For $n \in \mathbb{N}$, let S_n denote the symmetric group of permutations of n-elements.

$$S_0 = S_1 = \{\mathrm{id}\}, S_2 \cong C_2, S_3 \cong D_{2\cdot 3}, |S_n| = n!$$

Definition

For $\sigma \in S_n$, the number of pairs (i, j) with $i < j$ and $\sigma(i) > \sigma(j)$ is called the number of inversions (**Fehlstände**) of σ.
This defines a homomorphism

$$\mathrm{sgn} : S_n \to \{\pm 1\}, \quad \sigma \mapsto (-1)^{\#\text{ of inversions}}$$

In particular, $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ and its kernel is the **alternating group** A_n.

$$A_1 \cong A_2 \cong \{e\}, A_3 \cong \mathbb{Z}/3\mathbb{Z}$$

Theorem Cayley

Every finite group is isomorphic to a subgroup of S_n for some n.

Proof Sketch. Let $|G| = n$. Enumerate the elements of G, then left-multiplication with $g \in G$ corresponds to a permutation of the n-elements in G. This gives us a map

$$G \to S_n, \quad g \mapsto \text{ left multiplication with } g$$

which has kernel $\{1\}$ and so is injective. □

Proposition

Two permutations are conjugates in S_n if and only if they have the same cycle strucutre.

Theorem

For $n \geq 4$, A_n and S_n are resolvable and A_n is simple for $n \geq 5$.

Proposition

(a) Disjoint cycles commute.

(b) For every cylce, $(i_1 \dots i_k)^{-1} = (i_k \dots i_1)$.

(c) For $\sigma \in S_n$, conjugation of cycles is given by

$$\sigma(i_1 \dots i_k)\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$$

(d) $\operatorname{sgn}(i_1 \dots i_k) = (-1)^{k-1}$.

4.4 Nilpotent and resolvable groups

Definition

A group is called **nilpotent** of **order** 1, if G is abelian.
We say G is nilpotent of order $n+1$, if $G/Z(G)$ is nilpotent of order n.

Definition

Let G be a group and $p \in \mathbb{N}$ prime. We say G is a ***p*-group** if $|G| = p^k$ for some $k \geq 0 \in \mathbb{N}$.

Proposition

Every p-group is nilpotent.

Proof Sketch. Under conjgation, G admits a group action on itself. Then the center $Z(G)$ is exactly the fixpoints of the group action. With

$$|G| = |\mathrm{Fix}_G(G)| + \sum_{\text{non-trivial orbits}} [G : \mathrm{Stab}_G(x)]$$

since non-trivial orbits divide $|G| = p^k$ and have index > 1, when factoring out the center, the group $G/Z(G)$ becomes strictly smaller. $\square$

Definition

A sequence of chains of normal subgroups

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n = G$$

is called a **subnormal series** (Subnormalreihe).
A group G is called **resolvable** (auflösbar), if there exists a subnormal series such that the G_{k+1}/G_k are abelian groups.

- The dihedral group D_{2n} is resolvable with $\{e\} \lhd \langle R \rangle \lhd D_{2n}$.
- The affine group $A_k = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) | a \in R^\times, b \in R\}$ is resolvable and is not nipotent if $|R^\times| > 1$.
- S_4 is resolvable with $\{1\} \lhd \langle (12)(34), (13)(24) \rangle \lhd A_4 \lhd S_4$.

Proposition

Let G be a group. Then $[G, G] \lhd G$ and $G/[G, G]$ is abelian.
Moreover, it is the "largest" abelian factor group: If H is an abelian group and $\varphi : G \to H$ is a group homomorphism, then $[G, G] \subseteq \operatorname{Ker}\varphi$ and there exists a group homomorphism $\overline{\varphi} : G/[G, G] \to H$ such that the following diagram commutes

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & H \\ G/[G,G] \arrow[ur, "\overline{\varphi}"] & \end{tikzcd}$$

Proposition

A group G is resolvable if and only if the series

$$G^{(0)} := G, \quad G^{(n+1)} := [G^{(n)}, G^{(n)}]$$

reaches the trivial subgroup $\{e\}$.

Proposition Lego property

Let $N \lhd G$ be a normal subgroup. Then G is resolvable if and only if N and G/N are resolvable.

Proof sketch. By the third isomorphism theorem, there is a correspondence between subgroups of G/N and subgroups that contain N.
So we get subnormal series

$$\{e\} \lhd G_1 \lhd \ldots \lhd N$$
$$\{e\} \lhd H_1/N \lhd \ldots \lhd G/N$$

which we can combine to get a subnormal series for G. □

4.5 Sylow's Theorem

Definition

For a finite group, p prime and p, m coprime, write $|G| = p^k m$. A subgroup of order p^l is called a **p-subgroup**.

Theorem Sylow's Theorem

Let G be a finite group of order $|G| = p^k m$ as above.

(a) There exists a maximal p-subgroup H_p of order $|H_p| = p^k$. We call H_p a **Sylow p-subgroup**.

(b) Every p-subgroup is contained in a Sylow p-subgroup.

(c) Any two Sylow p-subgroups are conjugates.

Proof Sketch. Set $T = \{A \subseteq G | |A| = p^k\}$. Then T is a G-set with left multiplication and $|T| = \binom{n}{p^k} \neq 0 \mod p$. With

$$|T| = |\mathrm{Fix}_G(T)| + \sum_{\text{non-trivial orbits}} [G : \mathrm{Stab}_G(A)]$$

Unless $p^k < |G|$, then there are no fixpoints of the group action. □

Proposition

Let G be a group and p prime with $p||G|$. THen there exists an elment $g \in G$ of order $\mathrm{ord}(g) = p$.

Proof. Chose a Sylow p-subgroup H_p and an element $g \in H_p \setminus \{e\}$ □

Proposition

The group A_n is simple for $n \geq 5$. In particular, A_n, S_n are resolvable if and only if $n \leq 4$.

Proposition

Groups of order pq, p^2q, pqr for p, q, r prime are resolvable.

Lemma

A non-trivial simple group has no subgroup of index ≤ 4.
If it has a subgroup of index 5, it is isomorphic to A_5.

Theorem Classification theorem

Let G be a group of order $n = |G| \leq 100$. Then either G is resolvable or $G \cong A_5$ (and $|G| = 60$)

4.6 Free groups

Definition

For $n \geq 1$, let $\mathbb{Z}^n$ denote the **free abelian group** with n generators

$$b_1 = (1, 0, \ldots, 0), \ldots, b_n = (0, \ldots, 0, 1)$$

Lemma

For every free abelian group G with elements $a_1, \ldots, a_n$ there exists a unique group homomorphism

$$\varphi : \mathbb{Z}^n \to G, \quad \varphi(b_i) = a_i$$

Definition

Let $n \in \mathbb{N}$ and $b_1, \ldots, b_n$ pairwise disjoint.
A finite list of entries from $b_1^{\pm 1}, \ldots, b_n^{\pm 1}$ is called a **word**.
A word is said to be **reduced**, if a b_i is never followed by a b_i^{-1} or vice versa.
The **free group** F_n generated by $b_1, \ldots, b_n$ is the set

$$F_n = \{\text{reduced words in } b_1^{\pm 1}, \ldots, b_n^{\pm 1}\}$$

Composition of words given by concatenation and reduction of the lists defines a group structure on F_n.
The neutral element of F_n is the empty word.

Theorem

The free group has the universal property that for every group with elements $a_1, \dots, a_n \in G$, there exists a unique group homomorphism

$$\varphi : F_n \to G \quad \varphi(b_i) = a_i$$

in particular if $G = \langle \alpha_1, \dots, \alpha_n \rangle$, then $G \cong F_n / \operatorname{Ker} \varphi$.

Definition

Let F_n be the free group with n generators. For $W \subseteq F$ let

$$N = \langle gwg^{-1} | g \in F_n, w \in W \rangle$$

be the normal divisor of F_n generated by W.
F_n/N is called the group with generators $b_1, \dots, b_n$ and relations $w \in W$ and is written as

$$\langle b_1, \dots, b_n | w = e \text{ for } w \in W \rangle := {}^{F_n}\!\big/_{N}$$

- $\mathbb{Z}^2 \cong \langle a, b | ab = ba \rangle$ uses the relation $W = \{aba^{-1}b^{-1}\}$.
- $D_n \cong \langle R, T | R^n = e, T^2 = e, RT = TR^{-1} \rangle$ uses $W = \{R^n, T^2, RTRT\}$.

5 Fields

Instead of understanding fields intrinsically by studying their elements, it is often better to understand fields extrinsically through their relations with other fields.

5.1 Field Extensions

Definition

Let L be a field and k a subring that is also a field.
Then say that k is a **subfield** of L and we call L a **field extension** of k and write L/k to denote this fact.
Because L is also a k-vector space, write $[L : K] := \dim_k L$ for its **degree**.
If $[L : K] < \infty$, we say that L is a **finite** field extension of k.

Lemma Multiplicity of degree

Let $F/L/K$ be finite field extensions. Then

$$[F : K] = [F : L][L : K]$$

Proof sketch. If $x_1, \dots, x_m \in F$ are a basis of F over L and $y_1, \dots, y_n \in L$ are a basis of L over K, then the products $x_i y_j \in F$ are a basis of F over k. $\square$

Definition

Every field k contains a smallest subfield callled the **prime field** of k. It is either isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p.
The **characteristic** of a field k is define as

$$\operatorname{char} k := \begin{cases} p & \text{if its prime field is } F_p \\ 0 & \text{if its prime field is } \mathbb{Q} \end{cases}$$

Proposition

A ring homomorphism between two fields is always injective and only exists if the two fields have the same characteristic.

That is because the kernel is an ideal and the only ideals are K and $\{0\}$.

Definition

Let L/k and $A \subseteq L$. Write $k(A)$ for the smallest intermediate field between k and L that contains A. If $A = \{\alpha_1, \dots, \alpha_n\}$, write $K(a_1, \dots, a_n)$.

5.2 Polynomial rings over fields

Definition

Let L/k. For $\alpha \in L$ let

$$\mathrm{ev}_\alpha : K[X] \to L, \quad f \mapsto f(\alpha)$$

be the evaluation mapping. $\alpha \in L$ is called

- **transcendent** over k, if ev_α is injective.
- **algebraic** over k, otherwise. The kernel $\operatorname{Ker} \varphi_\alpha$ is an ideal. Since $K[T]$ is a PID, it has a unique normed (leading coefficient = 1) generator which we call the **minimal polynomial** of α

$$m_\alpha = \operatorname{irr}(\alpha, k) \in K[X] \quad \text{with} \quad \operatorname{Ker} \varphi_\alpha = (\operatorname{irr}(\alpha, k))$$

  in particular, if a polynomial $f(X)$ has $f(\alpha) = 0$, then the minimal polynomial divides f.

- $e, \pi \in \mathbb{R}$ are transcendent over $\mathbb{Q}$.
- $\sqrt{2} \in \mathbb{R}$ is algebraic with minimal polynomial $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$.

If α is algebraic, then $\operatorname{irr}(\alpha, k)$ is irreducible and the ideal $(\operatorname{irr}(\alpha, k)) = \operatorname{Ker} \mathrm{ev}_\alpha$ is maximal. Therefore, $k[X]/(\operatorname{irr}(\alpha, k)$ is a field and ev_α induces a field isomorphism

$$\overline{\mathrm{ev}_\alpha} : {}^{k[X]}\!/\!_{\mathrm{ev}_\alpha} \to k(\alpha)$$

- $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\} \cong Q[X]/(X^2 + 1) = \{aX + b | a, b \in \mathbb{Q}\}$.

- $\mathbb{Q}(e) = \{\frac{f(e)}{g(e)} | f, g \in Q[X], g(e) \neq 0\}$.

Proposition Wantzel

With ruler and compass, neither $\sqrt[3]{2}$ nor an angle $\frac{\pi}{9}$ can be constructed.
If $p \in \mathbb{N}$ is an odd prime number and the regular p-gon is constructable with ruler and compass, then p must be of the form $p = 2^{2^n} + 1$.

Proof Sketch. Start at $0 \in \mathbb{R}^2$. Then the set of constructable points is a field.
Let k_n be the field generated by the points obtained after n steps. Then $[k_{n+1} : k_n] \leq 2$. So $[k_n : 1]$ must be a power of 2. But $[Q(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
Moreover, $\cos(\frac{\pi}{9})$ has a minimal polynomi that is not 2^k. $\square$

Definition

A field extension L/k is called **algebraic**, if every $\alpha \in L$ is algebraic over k

If L/k is a finite field extension of degree n, then the $n+1$ elements $1, x, x^2, \ldots, x^n$ are linearlydependent. So every finite field extension is algebraic.

Proposition

If in a field extension L/k, $x, y \in L$ algebrac over k, then $x+y, x-y, xy, \frac{x}{y}$ are algebraic over k.

Proposition

Let $F/L/k$ be field extensions. Then

$$F/k \text{ algebraic} \iff F/L \text{ and } L/k \text{ are algebraic}$$

Theorem Kronecker

Let k be a field, $f \in K[X]$ with $n = \deg f > 0$. Then there exists a field extension L/k such that

$$f(X) = a \prod_{i=1}^{n} (X - \alpha_i)$$

where $a \in K^\times, \alpha_i \in L$.

Proof Sketch. Let p be an irreducible divisor of f. By induction over n, define

$$K_1 = \frac{K[X_1]}{p(X_1)}$$

then $f(X)$ has a root $\alpha_1 := X_1 + (p(X_1)) \in K_1$. Divide f by α_1 which has smaller degree and keep going until $f_n \in K^\times$. $\square$

- $f = X^2 + 1 \in \mathbb{R}[X]$ has the extension $\mathbb{C}$
- For $f = X^3 - 2 \in \mathbb{Q}[X]$ we have the extension $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$.

5.3 Algebraic Closure

Definition

Let k be a field, $f \in k[X]$ with $\deg f > 0$. A **splitting field** of f over k is a field extension L/k such that

(a) f splits into linear factors in $L[X]$

(b) In any intermediate proper subfield $k \subseteq E \subsetneq L$, f does not split over E.

- Such a splitting field always exists and is unique up to isomorphism.
- A splitting field is an algebraic field extension of k.
- For $f \in k[X]$ and L a splitting field of f over k

$$[L : k] \leq (\deg f)!$$

Definition

A field k is called **algebraically closed**, if every polynomial $f \in k[X]$ with $\deg f > 0$ has a root in k.

Every finite field is not algebraically closed, because we can take the polynomial

$$f(X) = 1 + \prod_{\lambda \in k} (X - \lambda)$$

Proposition

Let L/k be a field extension and L algebraically closed. Then

$$E = \{x \in L | x \text{ is algebraic over } k\} \subseteq L$$

is also an algebraically closed field extension of k.

Proof Sketch. Since x, y algebraic means that $x + y, xy, \frac{x}{y}$ are algebraic for $y \neq 0$, E is a field.
For $f \in E[X], \deg f > 0$, by Kronecker's theorem, there exists a field $F \supseteq E$ over which f splits. But L is algebraically closed, so any root $\alpha \in F$ of f is also present in L. Which means $\alpha \in L$ is algebraic over k, so by construction $\alpha \in E$. □

The construction of E is in fact not dependent on the choice of L.

Theorem

For any field k, there exists a field extension L/k with L algebraically closed.
Such extensions are unique up to isomorphism.

Proof sketch. For any $f \in k[X], \deg f > 0$, we take a free variable Y_f. □

6 Galois Theory

Definition

Let L/k be a field extension. The **Galois group** of the extension is the subgroup

$$\mathrm{Gal}(E/k) := \{\sigma \in \mathrm{Aut}(L) | \sigma|_k = \mathrm{id}_k\} < \mathrm{Aut}(L)$$

- $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \bar{\cdot}\}$
- $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}, (\sqrt{2} \mapsto -\sqrt{2})\}$
- $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \{\mathrm{id}\}$, because $X^3 - 2)$ only has one root in $\mathbb{Q}(\sqrt[3]{2})$.
- $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})/\mathbb{Q}) = \{\mathrm{id}, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\} \cong D_{2\cdot 3}$, where σ is complex conjugation and
$$\rho : \sqrt[3]{2} \mapsto e^{\frac{2\pi i}{3}} \sqrt[3]{2}$$

Definition

Let $f \in k[X]$ and L/k such that f splits in L. Write

$$R(f) := \{x \in L | f(x) = 0\}$$

for its collection of roots.

Lemma

Let E/k be a splitting field of a polynomial $f \in k[X]$. Then every element $\sigma \, \mathrm{Gal}(E/k)$ induces a permutation on the roots of f and the restriction mapping

$$\mathrm{Gal}(E/k) \to S_{R(f)}, \quad \sigma \mapsto \sigma|_{R(f)}$$

Proof. Let $R(f) = \{\alpha_1, \dots, \alpha_n\}$. Then write

$$E = k(\alpha_1, \dots, \alpha_n) = \left\{ \frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)} | p, q \in k[X_1, \dots, X_n], q(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

applying any $\sigma \in \mathrm{Gal}(E/k)$ on a rational function obviously keeps it invariant. □

6.1 Separablility

Let p be prime and consider

$$f(X) = X^p - t \in \mathbb{F}_p(t)[X]$$

If a is a root in some splitting field, we have

$$(X - a)^p = \mathrm{Fr}_p(X - a) = X^p - a^p = X^p - t$$

which means it only has one root $R(f) = \{a\}$.

Definition

A polynomial $f \in k[X]$ is said to have no **multiple roots** (mehrfachen Nullstellen), if in a splitting field $|R(f)| = \deg f$.

Lemma

For $f \in k[X]$ and $f' \in k[X]$ its formal derivative

$$f \text{ has no multiple roots} \iff \gcd(f, f') \in k[X]^\times$$

Proof. For $f(X) = a\prod_{i=1}^{n}(X - \lambda_i) \in \overline{k}[X]$ we have

$$f'(X) = a\sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{\infty}(X - \lambda_j)$$

□

Proposition

Let $f \in k[X]$ irreducible. Then f has no multiple roots if and only if $f' \neq 0$.

Definition

An irreducible polynomial is called **separable**, if it does not have multiple roots.
A reducible polynomial is called **separable**, if all its irreducible factors are separable.

- By the corollary, every polynomial in $\mathbb{Q}[X]$ is separable because $\operatorname{char}\mathbb{Q} = 0$.
-

Theorem

Let $\varphi : k \to k_*$ be a field isomorphism, $f \in k[X], f_* = \varphi_*(f) \in k_*[X]$, E/k a splitting field of f and E_* a splitting field of f_*.
If f is separable, then there are exactly $[E : k]$ isomorphisms $\Phi : E \to E_*$ that extend φ.
In particular, when taking $k_* = k, \varphi = \mathrm{id}_k$ we find

$$[E : k] = |\mathrm{Gal}(E/k)|$$

Proposition

Let E/k be a splitting field of a separable polynomial $f \in k[X]$. If f is irreducible, then

$$\deg f \,|\, |\mathrm{Gal}(E/k)| \,|\, (\deg f)!$$

Theorem

Let p be prime, $n \geq 1 \in \mathbb{N}$. Then

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

and a generating elment of the galois group is the **Frobenius homomorphism**

$$\mathrm{Fr} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^p$$

Definition

Let E/k be a field extenion, $\alpha \in L$.

- We say α is **separable** if $\mathrm{irr}(\alpha, k)$ is separable.
- We call the extension **separable**, if every $\alpha \in L$ is separable.

- If a is a root of $X^p - t$, then $(\mathbb{F}_p(t))(a)/\mathbb{F}_p(t)$ is not separable.

Proposition

The extension $k(A)/k$ is separable if and only if every $a \in A$ is separable.
In particular, every field extension with caracteristic 0 is separable. Every algebraic field extension of a finite field is separable.

6.2 Normal Field extensions

Definition

A field extension E/k is called **normal**, if E the splitting field of some polynomial $f \in k[X]$.

Proposition

Let $L = k(\alpha_1, \ldots, \alpha_n)$ and $\overline{L}$ an algebraic closure of L. Then the following are equivalent

(a) L is normal

(b) For ally $\alpha \in L$, the minimal polynomial $\mathrm{irr}(\alpha, k)$ splits over L.

(c) The minimal polynomial of all α_i splits over L

(d) For $\varphi \in \mathrm{Hom}(L, \overline{L})$ with $\varphi|_k = \mathrm{id}_k$ it holds $\varphi(L) \subseteq L$

(e) For $\varphi \in \mathrm{Hom}(L, \overline{L})$ with $\varphi|_k = \mathrm{id}_k$ it holds $\varphi(L) = L$

(f) Every irreducible polynomial in $k[X]$ with one root in L splits over L

- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. Because $X^3 - 2$, has a root, but doesn't split.

Proposition

Let $B/E/K$ be algebraic extensions. Then

$$B/k \text{ normal} \implies B/E \text{ normal}$$

Other implications are not true. Take for example

$$\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$$

shows that E/k is not normal.
The tower

$$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt[2]{2})/\mathbb{Q}$$

has B/E and E/k normal (with $X^2 - 2$ and $X^2 - \sqrt{2}$, but B/k is not normal.

Definition

Let k be a field and $H \subseteq \mathrm{Aut}(k)$ a subset. The **fixing field** (Fixkörper) of H is

$$k^H := \{x \in k \big| \sigma(x) = x \quad \forall \sigma \in H\} \subseteq E$$

The map $H \mapsto k^H$ is contravariant with respect to inclusion. For E/k, we always have $k \subseteq E^{\mathrm{Gal}(E/k)}$.

Definition

A finite field extension L/k is called **Galois** (galoissch), if L is the splitting field of a separable polynomial in $k[X]$.

Proposition

Let E/k be a finite field extension. Then the following are equivalent

(a) E/k is a Galois extension

(b) E/k is normal a separable extension.

(c) $E^{\mathrm{Gal}(E/k)} = k$

(d) $[E/k] = |\mathrm{Gal}(E/k)|$

Proposition

Given a tower $B/E/K$

$$B/k \text{ Galois} \implies B/E \text{ galois}$$

The counterexamples for the other implications are the same as for normal towers.

Definition

For a group G define the collection of subgroups of G

$$\mathrm{Sub}(G) := \{H \text{ group} \mid H < G\}$$

Fr a field extension E/k define the collection of intermediate fields

$$\mathrm{Int}(E/k) := \{B \text{ field} \mid E/B/k\}$$

Theorem Galois Correspondence

Let E/k be a finite Galois extension.

(a) There are bijective maps (that are contravariant with respect to inclusion)

$$\begin{aligned} \mathrm{Sub}(\mathrm{Gal}(E/k)) &\leftrightarrow \mathrm{Int}(E/k) \\ H &\mapsto E^H \\ B &\mapsfrom \mathrm{Gal}(E/B) \end{aligned}$$

(b) $B \in \mathrm{Int}(E/k)$ is Galois if and only if $\mathrm{Gal}(E/B)$ is a normal subgroup of $\mathrm{Gal}(E/k)$. If that is the case, then

$$\mathrm{Gal}(E/k) \big/ \mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/k)$$

Example

For the finite galois extension $E/k := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$. Find all intermediate fields.
To do so, set

$$a_1 := \sqrt[3]{2}, a_2 := \zeta_3 \sqrt[3]{2}, a_3 := \zeta_3^2 \sqrt[3]{2}$$

and let T be complex conjugation, R multiplication with ζ_3. We already know that $\mathrm{Gal}(E/k) = \langle T, R \rangle \cong D_3$

$$\begin{tikzcd}
 & & & \{e\} \arrow[hook, dlll, "2"'] \arrow[hook, dll, "2"] \arrow[hook, d, "2"] \arrow[hook, ddr, "3"] & \\
\langle T \rangle \arrow[hook, ddrrr, "3"] & \langle T, R \rangle \arrow[hook, ddrr, "3"] & & \langle T, R^2 \rangle \arrow[hook, dd, "3"] & \\
 & & & & \langle R \rangle \arrow[hook, dl, "2"'] \\
 & & & \mathrm{Gal}(E/k) &
\end{tikzcd}$$

and the corresponding diagram for the fixing fields is given by

$$\begin{tikzcd}
 & & \mathbb{Q}(\sqrt[3]{2},\zeta_3) & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[urr, hook, "2"] & \mathbb{Q}(\zeta_3,\sqrt[3]{2}) \arrow[ur, hook, "2"] & \mathbb{Q}(\zeta_3^2,\sqrt[3]{2}) \arrow[u, hook, "2"] & \\
 & & & \mathbb{Q}(\zeta_3) \arrow[uul, hook, "3"'] \\
 & & \mathbb{Q} \arrow[uull, hook, "3"] \arrow[uul, hook, "3"] \arrow[uu, hook, "3"] \arrow[ur, hook, "2"] &
\end{tikzcd}$$

where the coloured morphisms are the normal subgroup inclusions, or the Galois extensions, respectively.
Where the numbers are the index of the subgroups, or the degree of the field extension.

7 Appendix

Fields	Euclidean Ring	PID	UFD	Integral Domain	Commutative	Ring
$\mathbb{Q},\mathbb{R},\mathbb{C}$	$\mathbb{Z},K[X],\mathbb{Z}[i]$	$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$	$\mathbb{Z}[X,Y]$	$\mathbb{Z}[i\sqrt{5}]$	$C([0,1])$	$\mathrm{Mat}_{n\times n}(R)$
$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}[i\sqrt{2}],\mathbb{Z}[\sqrt{3}]$		$K[X_1,\dots,X_n]$		$\mathbb{Z}/n\mathbb{Z}$	
			prime $\iff$ irred.			

Table 1: Example of rings. The inclusion goes from left to right.