SF1678 Groups and Rings - Course Summary

Leo Trolin

23/06-2025

About

This summary contains the contents of the course Groups and Rings which I believe to be important for the exam and would be suitable on a cheat sheet. Some content, mainly technical lemmas, have been omitted.

Groups

Groups & subgroups

Definition:

> Let $G \neq \varnothing$ be a set with a map $\circ : G \times G \to G$. We define the following properties (with the implicit operation $\circ$):
> - Associative: $\forall a, b, c \in G : (ab)c = a(bc)$
> - Unit element/Identity: $\exists e \in G : ea = a = ae$
> - Inverse elements: $\forall a \in G\ \exists b \in G : ab = e = ba$
> - Commutative: $\forall a, b \in G : ab = ba$
>
> Then, $(G, \circ)$ is called a
> - Semigroup if associativity holds.
> - Monoid if associativity and existence of a unit hold.
> - Group if associativity, existence of a unit, and existence of inverses hold.
> - Abelian group if associativity, existence of a unit, existence of inverses, and commutativity hold.

Proposition:

> Let G be a group.
> (a) The unit element is unique.
> (b) The inverse of any $a \in G$ is unique.

Proposition:

> Let $G \neq \varnothing$ be a set with a map $\circ : G \times G \to G$ such that
> - $\circ$ is associative
> - There exists a left unit: $\exists e \in G\ \forall a \in G : ea = a$.
> - All elements have a left inverse: $\forall a \in G\ \exists b \in G : ba = e$
>
> Then $(G, \circ)$ is a group.

Definition: (**Submonoid**)

> Let G be a monoid and $H \subseteq G$ a subset. H is a submonoid of G if
> (i) $e \in H$
> (ii) $\forall a, b \in H : ab \in H$

Definition: (**Subgroup**)

> Let G be a group and $H \subseteq G$ a subset. H is a subgroup of G, written $H \leq G$, if
> (i) $e \in H$
> (ii) $\forall a, b \in H : ab \in H$
> (iii) $\forall a \in H : a^{-1} \in H$

Group homomorphisms

Definition: (**Monoid homomorphism**)

> Let G_1, G_2 be monoids and $\varphi : G_1 \to G_2$ a map. φ is a monoid homomorphism if
> (i) $\forall a, b \in G_1 : \varphi(ab) = \varphi(a)\varphi(b)$
> (ii) $\varphi(e_{G_1}) = e_{G_2}$

Definition: (**Group homomorphism**)

> Let G_1, G_2 be groups and $\varphi : G_1 \to G_2$ a map. φ is a group homomorphism if
> (i) $\forall a, b \in G_2 : \varphi(ab) = \varphi(a)\varphi(b)$

Proposition:

> Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then:
> (a) $\varphi(e_{G_1}) = e_{G_2}$
> (b) $\forall a \in G_1 : \varphi(a)^{-1} = \varphi(a^{-1})$

Definition: (**Types of group homomorphisms**)

> (a) For two groups G_1, G_2: $\mathrm{Hom}(G_1, G_2) := \{\varphi : G_1 \to G_2 \mid \varphi \text{ is a group homomorphism}\}$.
> (b) An injective homomorphism is a monomorphism. A surjective homomorphism is an epimorphism. A bijective homomorphism is an isomorphism.
> (c) For a group G: $\mathrm{End}(G) := \mathrm{Hom}(G, G)$ and its elements are endomorphisms of G. Also, $\mathrm{Aut}(G) := \{\varphi \in \mathrm{End}(G) \mid \varphi \text{ is bijective}\}$ and its elements are automorphisms of G.

Proposition:

> Compositions of group homomorphisms are group homomorphisms.

Proposition:

> If G is a group, then $(\mathrm{Aut}(G), \circ)$ is a group.

Proposition:

> Let G_1 and G_2 be groups and $\varphi \in \mathrm{Hom}(G_1, G_2)$.
> (a) $\ker \varphi \leq G_1$
> (b) $\mathrm{im}\, \varphi \leq G_2$
> (c) φ injective $\iff \ker \varphi = \{e\}$
> (d) $H_1 \leq G_1 \implies \varphi(H_1) \leq G_2$
> (e) $H_2 \leq G_2 \implies \varphi^{-1}(H_2) \leq G_1$

Definition: (**Conjugation**)

> Let G be a group and $a \in G$ an element. We define conjugation by a as $\gamma_a : G \to G, g \mapsto aga^{-1}$; also called an inner automorphism of G.
>
> $\mathrm{Inn}(G) := \{\gamma_a \mid a \in G\} \leq \mathrm{Aut}(G)$.

↳ Comment:
It holds that $\gamma_a \in \mathrm{Aut}(G)$, and $G \to \mathrm{Aut}(G)$, $a \mapsto \gamma_a$ is a group homomorphism.

Cosets

Definition: (**Coset**)

> Let G be a group and $H \leq G$ a subgroup. For $a \in G$, a left coset is $aH := \{ah \mid h \in H\}$. The set of all left cosets of H in G are denoted $G/H := \{aH \mid a \in G\}$.
>
> Analogously, right cosets are Ha while the set of all right cosets are $H \backslash G$.

Lemma:

> Let $a, b \in G$. The following are equivalent:
> (a) $aH = bH$
> (b) $aH \cap bH \neq \varnothing$
> (c) $a \in bH$
> (d) $b^{-1}a \in H$

Corollary:

> Let $H \leq G$. Then G is the disjoint union of all left cosets of H in G:
>
> $$G = \dot{\bigcup_{C \in G/H}} C$$

Definition: (**Index**)

> Let $H \leq G$. The index of H in G is $[G : H] = |G/H| = |H \backslash G|$.

Theorem: (**Theorem of Lagrange**)

> Let $H \leq G$ where G is a finite group. Then
>
> $$\operatorname{ord}(G) = [G : H] \operatorname{ord}(H).$$

Normal subgroups

Definition/Lemma: (**Normal subgroup**)

> Let $H \leq G$. H is a normal subgroup of G, denoted $H \trianglelefteq G$, if one of the following equivalent statements are true:
> (i) $\forall \gamma \in \operatorname{Inn}(G)$, $\gamma(H) = H$ (meaning $\forall a \in G$, $aHa^{-1} = H$)
> (ii) $\forall \gamma \in \operatorname{Inn}(G)$, $\gamma(H) \subseteq H$
> (iii) $\forall \gamma \in \operatorname{Inn}(G)$, $\gamma(H) \supseteq H$
> (iv) $\forall a \in G$, $aH = Ha$

Example: (**Examples of normal subgroups**)

> - Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then $\ker(\varphi) \trianglelefteq G_1$ is a normal subgroup.
> - $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.
> - If G is an abelian group, then all its subgroups are normal subgroups.

Theorem/Definition:

Let G be a group and $N \trianglelefteq G$ be a normal subgroup.
(a) $\forall a, b \in G$, $(aN)(bN) = abN$
(b) G/N is a group called the quotient group or factor group of G modulo N.
- Its elements are on the form aN with multiplication as in (a).
- Its unit is $eN = N$.
- Inverses are $(aN)^{-1} = a^{-1}N$.

(c) The canonical projection $\pi : G \to G/N, a \mapsto aN$ is a surjective group homomorphism with $\ker(\pi) = N$.

Proposition: (**Universal property of π**)

Let $\varphi : G_1 \to G_2$ be a group homomorphism, and let $N \trianglelefteq G_1$ be a normal subgroup such that $N \subseteq \ker(\varphi)$. Then there is a unique group homomorphism $\bar{\varphi} : G_1/N \to G_2$ such that $\varphi = \bar{\varphi} \circ \pi$.

$$\begin{tikzcd} G_1 \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & G_2 \\ & G_1/N \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

Moreover,
(a) $\operatorname{im}(\bar{\varphi}) = \operatorname{im}(\varphi)$
(b) $\ker(\bar{\varphi}) = \pi(\ker(\varphi))$
(c) $\ker(\varphi) = \pi^{-1}(\ker(\bar{\varphi}))$
(d) $\bar{\varphi}$ injective $\iff N = \ker(\varphi)$

Corollary:

Let $\varphi : G_1 \to G_2$ be a surjective group homomorphism. Then G_2 is canonically isomorphic to $G_1/\ker(\varphi)$.

Skipped: First and second isomorphism theorems

Cyclic groups

Definition: (**Generated subgroup, cyclic group**)

Let G be a group and $M \subseteq G$ be a subset.
(a) Then

$$\langle M \rangle := \{e\} \cup \left\{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} \mid n \in \mathbb{N}, a_i \in M, \varepsilon_i = \pm 1\right\} = \bigcap_{\substack{H \leq G, \\ M \subseteq H}} H$$

is the subgroup generated by M. It is the smallest subgroup of G containing M.
(b) If $M = \{a\}$, we write $\langle a \rangle$ and call it the cyclic group generated by a. Then $\langle a \rangle = \{e, a, a^2, \dots\}$.

↳ Comment:
Cyclic groups are abelian.

Theorem:

Let G be a cyclic group.
(a) If $|G| = \infty$, then $G \cong \mathbb{Z}$.
(b) If $|G| = m < \infty$, then $G \cong \mathbb{Z}/m\mathbb{Z}$.

Proposition:

Let $H \leq \mathbb{Z}$. Then $H = m\mathbb{Z}$ for some $m \in \mathbb{Z}$.

Proposition:

> Let G be a cyclic group and let $H \leq G$ be a subgroup. Then H is cyclic.

Definition: (**Order**)

> Let G be a group and $a \in G$ be an element. The order of a is $\text{ord}(a) := \text{ord}(\langle a \rangle)$.

↳ Comment:
If $\text{ord}(a) < \infty$, then the order of a is the smallest positive integer m such that $a^m = e$.

Theorem: (**Fermat's little theorem**)

> Let G be a finite group and $a \in G$ be an element. Then
>
> $$\text{ord}(a) \mid \text{ord}(G) \quad \text{and} \quad a^{\text{ord}(G)} = e.$$
>
> In a number theoretic setting, if p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.

Corollary:

> Let G be a group of prime order p. Then,
> (a) $G \cong \mathbb{Z}/p\mathbb{Z}$
> (b) $\forall a \in G$ except e, $\text{ord}(a) = p$ and $G = \langle a \rangle$.

Group actions

Definition: (**Group action**)

> Let G be a group and X a set. An action of G on X is a map $G \times X \to X$, $(g, x) \mapsto g \cdot x$ such that
> (i) $e \cdot x = x, \ \forall x \in X$
> (ii) $g \cdot (h \cdot x) = (gh) \cdot x, \ \forall x \in X, \forall g, h \in G$

Definition: (**Stabilizer**)

> Consider a group action of G on X and let $x \in X$. Then the stabilizer of x in G is $G_x := \{g \in G \mid g \cdot x = x\}$.

↳ Comment:
$G_x \leq G$.

Definition: (**G-orbit**)

> Consider a group action $G \times X \to X$ and let $x \in X$. Then the G-orbit of x is $G \cdot x := \{g \cdot x \mid g \in G\} \subseteq X$.
>
> The set of G-orbits in X is written $G \backslash X := \{G \cdot x \mid x \in X\}$.

Definition: (**Transitive**)

> A group action $G \times X \to X$ is transitive if $\left| G \backslash X \right| = 1$.

Proposition:

> Consider a group action $G \times X \to X$.
> (a) G-orbits constitute equivalence classes on X by $x \sim y \iff y \in G \cdot x$ for $x, y \in X$.
> (b) Let $x, y \in G$. Then, $G \cdot x = G \cdot y \iff G \cdot x \cap G \cdot y \neq \varnothing$.
> (c) X is the disjoint union of its G-orbits.

Corollary: (**Orbit equation**)

> Let $G \times X \to X$ be a group action on a finite set X. Then,
> $$|X| = \sum_{B \in G\backslash X} |B|.$$

Theorem: (**Orbit-Stabilizer theorem**)

> Let $G \times X \to X$ be a group action and $x \in X$ be an element.
> (a) The map $G \to X, g \mapsto g \cdot x$ induces a bijection of cosets $G/G_x \xrightarrow{\sim} G \cdot x$.
> (b) $|G \cdot x| = [G : G_x]$

Proposition: (**Burnside's lemma**)

> Let $G \times X \to G$ be a group action of a finite group G. For $g \in G$, define the set of fixed points $\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\}$. Then,
> $$\left|G\backslash X\right| = \frac{1}{\mathrm{ord}(G)} \sum_{g \in G} \left|\mathrm{Fix}(g)\right|.$$

Definition: (**Centralizer, center**)

> Let G be a group and $S \subseteq G$ a subset.
> (a) The centralizer of S is $Z_S(G) := \{g \in G \mid \forall s \in S : gs = sg\}$.
> (b) The center of G is $Z(G) := Z_G(G)$.

Proposition:

> Let G be a group and $S \subseteq G$ a subset.
> (a) $Z_S(G) \leq G$
> (b) $Z(G)$ is the kernel of $G \to \mathrm{Aut}(G), g \mapsto (\gamma_g : G \to G, a \mapsto gag^{-1})$
> (c) $Z(G) \trianglelefteq G$ and $G/Z(G) \cong \mathrm{Inn}(G)$.
> (d) $G/Z(G)$ is cyclic $\iff$ G is abelian.

Definition: (**System of representatives**)

> Let $G \times X \to X$ be a group action.
> (a) For $B \in G\backslash X$, $x \in B$ is called a representative of B.
> (b) For a family $(B_i)_{i \in I}$ of disjoint G-orbits, a system of representatives is a family $(x_i)_{i \in I}$ of elements of X such that $x_i \in B_i$ $\forall i \in I$.

Theorem: (**Class equation**)

> Let G be a finite group and consider the conjugation action $G \times G \to G, (g, x) \mapsto gxg^{-1}$. Let $x_1, \ldots, x_k$ be a system of representatives of the orbits contained in $G - Z(G)$. Then,
> $$\begin{aligned}\mathrm{ord}(G) &= \mathrm{ord}(Z(G)) + \sum_{i=1}^{k} [G : Z_{\{x_i\}}(G)] \\ &= \mathrm{ord}(Z(G)) + \sum_{i=1}^{k} |G \cdot x_i|.\end{aligned}$$

↳ Comment:
Orbits not contained in $G - Z(G)$ are singletons $\{z\}$ for some $z \in Z(G)$.

Corollary:

> Let G be a group of order p^2 for a prime p. Then G is abelian.

Sylow groups

Definition: (**Conjugate**)

> Let G be a group.
> (a) $h_1 \in G$ is conjugate to $h_2 \in G$ if there exists $g \in G$ such that $h_2 = gh_1g^{-1}$.
> (b) $H_1 \leq G$ is conjugate to $H_2 \leq G$ if there exists $g \in G$ such that $H_2 = gH_1g^{-1}$.

Defintion: (**p-group, p-Sylow subgroup**)

> Let G be a finite group and p be a prime.
> (a) G is a p-group if $\mathrm{ord}(G) = p^k$ for some $k \in \mathbb{N}$.
> (b) $H \leq G$ is a p-Sylow subgroup if H is a p-group and $p \nmid [G : H]$. (If $\mathrm{ord}(H) = p^k$, then no greater power of p is in the prime factorization of $\mathrm{ord}(G)$)

Theorem: (**Sylow theorems**)

> Let G be a finite group and p be a prime.
> (a) G has at least one p-Sylow subgroup. More precisely: For any p-subgroup $H \leq G$, there is a p-Sylow subgroup $S \leq G$ such that $H \leq S$.
> (b) Let $S \leq G$ be a p-Sylow subgroup and $H \leq G$ be a subgroup. Then, H is a p-Sylow subgroup if and only if H is conjugate to S.
> (c) Let $s_p(G)$ be the number of p-Sylow subgroups in G. Then, $s_p(G) \mid \mathrm{ord}(G)$ and $s_p(G) \equiv 1 \mod p$.

Lemma: (**"Key lemma"**)

> Let G be a group and $H, K \trianglelefteq G$ be normal subgroups such that $H \cap K = \{e\}$. Then,
> (a) $\forall h \in H, \forall k \in K : hk = kh$
> (b) $\varphi : H \times K \to G, (h, k) \mapsto hk$ is an injective group homomorphism.

Corollary:

> Let G be a finite group and p be a prime.
> (a) $p \mid \mathrm{ord}(G) \implies \exists g \in G : \mathrm{ord}(g) = p$
> (b) G is a p-group $\iff \forall g \in G\ \exists t \in \mathbb{N} : g^{p^t} = e$
> (c) Let $H \leq G$. H is a p-Sylow group $\iff H$ is a maximal p-group in G.
> (d) Let $S \leq G$ be a p-Sylow subgroup. Then $S \trianglelefteq G \iff s_p(G) = 1$.

Corollary:

> Let G be a finite abelian group and p be a prime. Then, G has exactly one p-Sylow subgroup, namely $S_p := \{g \in G \mid \exists t \in \mathbb{N} : g^{p^t} = e\}$.

Proposition:

> Let G be a finite abelian group. Then, G is the direct product of its p-Sylow subgroups.
>
> In other words, if we prime factorize $\mathrm{ord}(G) = \prod_{i=1}^k p_i^{n_i}$, then $G \cong \prod_{i=1}^k S_{p_i}$ with S_{p_i} defined above.

Theorem: (**Fundamental theorem of finite abelian groups**)

> Every finite abelian group is the direct product of cyclic groups of prime-power order.

Theorem: (**Fundamental theorem of finitely generated abelian groups**)

> Let G be an abelian group generated by $M \subseteq G$ with $|M| < \infty$. Then, $G \cong \mathbb{Z}^d \times G'$ where G' is a finite abelian group.

Permutation groups

Here, we are working with the permutation group S_n (see next subsection).

Definition: (**r-cycle, etc.**)

> (a) Let $\pi \in S_n$ and $r \geq 2$. π is an r-cycle if $\pi = (x_1, \dots, x_r)$ for distinct $x_1, \dots, x_r$, that is:
> - $\pi(x_i) = x_{i+1}$ for $i = 1, \dots, r-1$
> - $\pi(x_r) = x_1$
> - $\pi(x) = x$ if $x \neq x_1, \dots, x_r$.
>
> (b) Two cycles $(x_1, \dots, x_r)$ and $(y_1, \dots, y_s)$ are disjoint if $\{x_1, \dots, x_r\} \cap \{y_1, \dots, y_s\} = \varnothing$.
> (c) A 2-cycle is a transposition.

Proposition:

> Let $n \geq 2$.
> (a) If $\pi_1, \pi_2 \in S_n$ are disjoint cycles, then $\pi_1 \circ \pi_2 = \pi_2 \circ \pi_1$.
> (b) Every $\pi \in S_n$ is a product of disjoint cycles, unique up to ordering.
> (c) Every $\pi \in S_n$ is a product of transpositions.

Proposition/definition: (**sgn**)

> Let $\pi \in S_n$ be written as a product of transpositions $\pi = \tau_1 \dots \tau_l$. Then, the map $\operatorname{sgn} : S_n \to \{\pm 1\}, \pi \mapsto \operatorname{sgn}(\pi) := (-1)^l$ is a well-defined group homomorphism.

Definition: (**Even/odd**)

> A permutation $\pi \in S_n$ is even if $\operatorname{sgn}(\pi) = 1$ and odd if $\operatorname{sgn}(\pi) = -1$.

Definition: (**Alternating group A_n**)

> The alternating group on $\{1, \dots, n\}$ is $A_n := \ker(\operatorname{sgn}) = \{\pi \in S_n \mid \pi \text{ is even}\}$.

Proposition:

> (a) If $n \geq 2$, then $A_n \trianglelefteq S_n$ and $[S_n : A_n] = 2$.
> (b) If $n \geq 3$, then $A_n = \{\prod_{j=1}^{l} \sigma_j \mid l \in \mathbb{N}, \sigma_j \in S_n \text{ is a 3-cycle}\}$.

Some notation for important groups

Example: (**Permutation group**)

> Let $X \neq \varnothing$ be a set. Then $S(X) = \{\pi : X \to X \mid \pi \text{ is bijective}\}$ is a permutation group under composition. If $X = \{1, \dots, n\}$, then $S(X) = S_n$.

Example: (**Dihedral group**)

> For $n \in \mathbb{Z}_{>0}$, let $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ be rotation by $\frac{2\pi}{n}$ and $\tau : \mathbb{R}^2 \to \mathbb{R}^2$ be reflection across the x-axis. Then, $D_n := \{\sigma^k \mid k = 0, \dots, n-1\} \cup \{\tau\sigma^k \mid k = 0, \dots, n-1\}$ is the nth dihedral group under composition.
>
> It holds that $\tau\sigma\tau = \sigma^{-1}$.
>
> An alternate definition is $D_n := \langle \sigma, \tau \mid \mathrm{ord}(\sigma) = n, \mathrm{ord}(\tau) = 2, \tau\sigma\tau = \sigma^{-1} \rangle$.

Example: (**Matrix groups**)

> For a field $\mathbb{K}$, we define the following groups:
> - $\mathrm{GL}(n, \mathbb{K}) = \{M \in \mathbb{K}^{n\times n} \mid \det M \neq 0\}$ is the general linear group.
> - $\mathrm{SL}(n, \mathbb{K}) = \{M \in \mathbb{K}^{n\times n} \mid \det M = 1\}$ is the special linear group.
> - $\mathrm{O}(n, \mathbb{K}) = \{M \in \mathbb{K}^{n\times n} \mid M^{\mathrm{T}} = M^{-1}\}$ is the orthogonal group.
> - $\mathrm{U}(n) = \{M \in \mathbb{C}^{n\times n} \mid M^{\dagger} = M^{-1}\}$ is the unitary group.
> - $\mathrm{SO}(n, \mathbb{K}) = \mathrm{SL}(n, \mathbb{K}) \cap \mathrm{O}(n, \mathbb{K})$ is the special orthogonal group.
> - $\mathrm{SU}(n) = \mathrm{SL}(n, \mathbb{C}) \cap \mathrm{U}(n)$ is the special unitary group.

Rings

Rings, subrings & ideals

Definition: (**Ring**)

> A ring $(R, +, \cdot)$ is a set $R \neq \varnothing$ with maps $+ : R \times R \to R$, $\cdot : R \times R \to R$ where
> - $(R, +)$ is an abelian group
> - $(R, \cdot)$ is a monoid
> - $\forall a, b, c \in R : a(b + c) = ab + bc, (b + c)a = ba + ca$ (distributivity)
>
> A ring is commutative if $(R, \cdot)$ is a commutative monoid.
>
> We denote the additive identity as 0 and the multiplicative identity as 1. We denote the additive inverse of $a \in R$ as $-a$.

Proposition:

> Let $(R, +, \cdot)$ be a ring. Then,
> (a) $0 \cdot a = 0 = a \cdot 0 \ \forall a \in R$
> (b) $(-a)b = a(-b) = -(ab) \ \forall a, b \in R$

Definition: (**Subring, Ring Extension**)

> Let $(R, +, \cdot)$ be a ring. Then, $S \subseteq R$ is a subring if $(S, +, \cdot)$ is a ring and $1 \in S$. (thus, 1 will be the multiplicative identity of S)
>
> The pair $S \subseteq R$ is called a ring extension.

Definition: (R^*)

> For a ring R, we define $R^* := \{a \in R \mid \exists b \in R : ab = 1 = ba\}$. The elements of R^* are called units.

Definition: (**Division Ring/Skew Field**)

> A ring R is a division ring/skew field if $R^* = R \setminus \{0\}$ and $R \neq \{0\}$.

Definition: (**Field**)

> A ring R is a field if it is a commutative skew field.

Definition: (**Ideal**)

> Let R be a ring and $I \subseteq R$ a subset. I is an ideal in R, written $I \trianglelefteq R$, if
> (i) I is an additive subgroup
> (ii) $\forall r \in R, \forall a \in I : ra, ar \in I$.

Proposition:

> Let R be a ring and $I \trianglelefteq R$ an ideal.
> (a) $1 \in I \iff I = R$.
> (b) If R is a field, then I is a trivial ideal $\{0\}$ or R.

Definition: (**Principal ideal**)

> Let R be a commutative ring and $a \in R$ an element. Then, $\langle a \rangle := aR \trianglelefteq R$ is the principal ideal generated by a.

Definition/Proposition: ($\langle A \rangle$)

> Let R be a commutative ring and $A \subseteq R$ a subset. The ideal generated by A is $\langle A \rangle := \{\sum_{i=1}^n a_i r_i \mid n \in \mathbb{N}, a_i \in A, r_i \in R\} \trianglelefteq R$. It is the smallest ideal in R containing A.
>
> If $|A| < \infty$, we say that $\langle A \rangle$ is finitely generated.

Definition/Proposition:

> Let R be a ring and $I, J \trianglelefteq R$ be ideals. Then the following are ideals:
> (a) $I + J := \{a + b \mid a \in I, b \in J\} \trianglelefteq R$
> (b) $I \cdot J := \{\sum_{i=1}^n a_i \cdot b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J\} \trianglelefteq R$
> (c) $I \cap J \trianglelefteq R$

Ring homomorphisms

Definition: (**Ring homomorphism**)

> Let R and S be rings and $\varphi : R \to S$ be a map. φ is a ring homomorphism if
> (i) $\forall a, b \in R : \varphi(a + b) = \varphi(a) + \varphi(b)$ (group homomorphism wrt. $+$)
> (ii) $\forall a, b \in R : \varphi(ab) = \varphi(a)\varphi(b)$
> (iii) $\varphi(1_R) = 1_S$ (monoid homomorphism wrt. $\cdot$)
> If φ is bijective, then φ is called a ring isomorphism.

Proposition:

> Let $\varphi : R \to S$ be a ring homomorphism.
> (a) $\ker(\varphi) \trianglelefteq R$
> (b) $\mathrm{im}(\varphi)$ is a subring of S.
> (c) $\varphi|_{R^*} : R^* \to S^*$ is a group homomorphism, where the group operation is $\cdot$. Note: φ maps units to units!
> (d) $\ker(\varphi)$ is a subring of $R \iff \ker(\varphi) = R \iff S = \{0\}$

Corollary:

> Let $\varphi : \mathbb{K} \to R$ be a ring homomorphism where $\mathbb{K}$ is a field and $R \neq \{0\}$. Then, φ is injective.

Theorem/Definition: (**Quotient ring**)

> Let R be a ring and $I \trianglelefteq R$ be an ideal.
> (a) $x \sim y \iff x - y \in I$ defines an equivalence relation on R with equivalence classes $[x] := x + I$ for $x \in R$.
> (b) Denote the set of all equivalence classes as R/I, called a factor/quotient/residue class ring. This is a ring with
> - $(x + I) + (y + I) := (x + y) + I, \forall x, y \in R$
> - $(x + I) \cdot (y + I) := (xy) + I, \forall x, y \in R$
>
> (c) The canonical projection $\pi : R \to R/I, x \to x + I$ is a surjective ring homomorphism with $\ker(\pi) = I$.

Proposition: (**Universal property of π**)

> Let $\varphi : R \to S$ be a ring homomorphism. Let $I \trianglelefteq R$ be an ideal with $I \subseteq \ker(\varphi)$. Then, there is a unique ring homomorphism $\bar{\varphi} : R/I \to S$ such that $\varphi = \bar{\varphi} \cdot \pi$.
>
> $$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\ & R/I \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$
>
> Moreover,
> (a) $\mathrm{im}(\bar{\varphi}) = \mathrm{im}(\varphi)$
> (b) $\ker(\bar{\varphi}) = \pi(\ker(\varphi))$
> (c) $\ker(\varphi) = \pi^{-1}(\ker(\bar{\varphi}))$
> (d) $\bar{\varphi}$ is injective $\iff$ $I = \ker(\varphi)$

Corollary:

> Let $\varphi : R \to S$ be a surjective ring homomorphism. Then, S is canonically isomorphic to $R/\ker(\varphi)$.

Skipped: First and second isomorphism theorems

Polynomials

Definition: (**Polynomial, etc.**)

> Let R be a ring and let $X_1, \ldots, X_k$ be variables. For an $i = (i_1, \ldots, i_k) \in \mathbb{N}^k$ we write $X^i := X_1^{i_1} \cdots X_k^{i_k}$ in multi-index notation. For $i, j \in \mathbb{N}^k$ we define $i + j := (i_1 + j_1, \ldots, i_k + j_k)$.
>
> A formal power series in $X_1, \ldots, X_k$ with coefficients in R is a formal sum $\sum_{i\in\mathbb{N}^k} a_i X_i$ where $a_i \in R\ \forall i \in \mathbb{N}^k$.
>
> We denote the set of all formal power series as
>
> $$R[[X_1, \ldots, X_k]] := \left\{ \sum_{i\in\mathbb{N}^k} a_i X_i \middle| a_i \in R \right\}.$$
>
> On these we define addition and multiplication via
>
> $$\sum_{i\in\mathbb{N}^k} a_i X^i + \sum_{i\in\mathbb{N}^k} b_i X^i := \sum_{i\in\mathbb{N}^k} (a_i + b_i) X^i,$$
> $$\sum_{i\in\mathbb{N}^k} a_i X^i \cdot \sum_{i\in\mathbb{N}^k} b_i X^i := \sum_{i\in\mathbb{N}^k} \left(\sum_{m+n=i} a_m b_n \right) X^i \qquad \text{(Cauchy product)}$$
>
> A formal power series is a polynomial if only finitely many a_i are nonzero. We denote the set of all polynomials as
> $$R[X_1, \ldots, X_k] := \left\{ f \in R[[X_1, \ldots, X_k]] \middle| f \text{ is a polynomial} \right\}.$$
> The degree of a polynomial is $\deg f := \max\{i_1 + \cdots + i_k \mid a_i \neq 0\}$ if $f \neq 0$, and $\deg 0 := -\infty$.
>
> A polynomial f is homogeneous of degree d if $a_i \neq 0$ holds only for $i_1 + \cdots + i_k = d$. We denote the set of all polynomials homogeneous of degree d as
>
> $$R[X_1, \ldots, X_k]_d := \left\{ f \in R[[X_1, \ldots, X_k]] \middle| f \text{ is homogeneous of degree } d \right\}.$$
>
> If $k = 1$, we say that the leading coefficient of a polynomial f of degree n is a_n.
>
> If $k = 1$, we say that a polynomial of degree n is monic if $a_n = 1$.

Proposition:

> Let R be a ring.
> (a) $(R[[X_1, \dots, X_k]], +, \cdot)$ is a ring.
> (b) $R[[X_1, \dots, X_k]]$ is commutative $\iff$ R is commutative
> (c) $R[X_1, \dots, X_k]$ is a subring of $R[[X_1, \dots, X_k]]$.
> (d) $R[[X_1, \dots, X_k]] \cong R[[X_1, \dots, X_{k-1}]][[X_k]]$ as rings.
> (e) $R[X_1, \dots, X_k] \cong R[X_1, \dots, X_{k-1}][X_k]$ as rings.
> (f) $R[[X_1, \dots, X_k]]^* = \{\sum_{i \in \mathbb{N}^k} a_i X^i \mid a_{(0,\dots,0)} \in R^*\}$

Proposition:

> Let R be a ring and let $f, g \in R[X_1, \dots, X_k]$. Then,
> (a) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
> (b) $\deg(f \cdot g) \leq \deg(f) + \deg(g)$

Integral domains

Definition: (**Zero divisor**)

> Let R be a ring. $x \in R$ is a zero divisor if $\exists y \in R \setminus \{0\}$ such that $xy = 0$ or $yx = 0$.

Proposition:

> Units in a ring are not zero divisors.

Definition/Proposition: (**Integral domain**)

> Let $R \neq \{0\}$ be a commutative ring. It is an integral domain/ID if its only zero divisor is 0; or equivalently, if $\forall x, a, b \in R, x \neq 0$ it holds that $xa = xb \implies a = b$.

Proposition:

> Let R be an integral domain.
> (a) $f, g \in R[X_1, \dots, X_k] \implies \deg(fg) = \deg(f) + \deg(g)$
> (b) $R[X_1, \dots, X_k]^* = R^*$

Theorem/Definition: (**Field of fractions**)

> Let R be an integral domain.
> (a) Let $M := R \times R \setminus \{0\}$. Then, $(a, b) \sim (c, d) \iff ad = bc$ defines an equivalence relation on M. Denote the equivalence classes as $[a, b] := \frac{a}{b}$.
> (b) Let $Q(R) := \{\frac{a}{b} \mid (a, b) \in M\}$ called the field of fractions or quotient field of R. It is a field with
> - $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$
> - $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$
> - zero element $\frac{0}{1}$
> - one element $\frac{1}{1}$
> - $-\frac{a}{b} = \frac{-a}{b}$ and $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$
>
> (c) The map $R \to Q(R)$, $a \mapsto \frac{a}{1}$ is an injective ring homomorphism.
> (d) $Q(R)$ is the smallest field containing R. More specifically, for an injective ring homomorphism $\varphi : R \hookrightarrow \mathbb{K}$, there is a unique ring homomorphism $\bar{\varphi} : Q(R) \hookrightarrow \mathbb{K}$ with $\bar{\varphi}|_R = \varphi$, which is injective.
>
> $$\begin{tikzcd} R \arrow[rr, hook, "\varphi"] \arrow[dr] & & \mathbb{K} \\ & Q(R) \arrow[ur, hook, "\bar{\varphi}"'] & \end{tikzcd}$$

Definition: (**Associated**)

> Let R be a commutative ring, and $a, b \in R$. a and b are associated if $\exists c \in R^*$ such that $b = ca$. This is an equivalence relation.

Lemma:

> Let R be an ID, and $a, b \in R$. Then, a and b are associated $\iff \langle a \rangle = \langle b \rangle$.

Definition: (**Principal ideal domain**)

> Let R be an integral domain. R is a principal ideal domain/PID if every ideal is principal. (generated by a single element)

Primes

Definition: (**Prime, maximal ideal**)

> Let R be a commutative ring and $I \trianglelefteq R$ an ideal.
> (a) I is a prime ideal if $1 \notin I$ and $\forall a, b \in R : (ab \in I \implies a \in I \text{ or } b \in I)$.
> (b) I is a maximal ideal if $1 \notin I$ and $\forall J \trianglelefteq R$: $(I \subseteq J \implies J = I \text{ or } J = R)$.

Theorem:

> Let R be a commutative ring and $I \trianglelefteq R$ an ideal.
> (a) I is prime $\iff R/I$ is an integral domain.
> (b) I is maximal $\iff R/I$ is a field.
> (c) I is maximal $\implies I$ is prime.

Corollary:

> Let $m \in \mathbb{N}$.
> (a) $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ is prime $\iff m$ is a prime number or $m = 0$.
> (b) $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ is maximal $\iff m$ is a prime number

Definition: (**gcd, coprime**)

> Let R be a commutative ring.
> (a) $a \in R$ divides $b \in R$ if $b \in \langle a \rangle$, written $a \mid b$. (i.e., $b = ar$ for some $r \in R$)
> Note: Units divide everything
> (b) A greatest command divisor/gcd of $a_1, \dots, a_n \in R$ is a common divisor $g \in R$ of the a_i's such that every other common divisor divides g.
> Note: If g is a gcd of some numbers and $u \in R^*$ is a unit, then ug is also a gcd.
> (c) $a, b \in R$ are coprime if 1 is a gcd of a and b.

Proposition:

> In integral domains, gcd's are unique up to unit multiplication.

Definition: (**Prime, irreducible**)

> Let R be a commutative ring and let $p \in R$, $p \neq 0$, $p \notin R^*$.
> (a) p is prime if $\forall a, b \in R : p \mid ab \implies p \mid a$ or $p \mid b$.
> Note: p is prime $\iff \langle p \rangle$ is a prime ideal
> (b) p is irreducible if $\forall a, b \in R : p = ab \implies a \in R^*$ or $b \in R^*$. Otherwise, p is reducible.

Proposition:

> Let R be an integral domain and let $p \in R, p \neq 0, p \notin R^*$.
> (a) p is prime $\implies$ p is irreducible.
> (b) If R is a PID, then p is irreducible $\iff$ p is prime $\iff$ $\langle p \rangle$ is maximal.

Corollary:

> Let R be a PID and let $I \trianglelefteq R$ be an ideal with $I \neq \{0\}$. Then, I is prime $\iff$ I is maximal.

Definition: (**Coprime ideals**)

> Let R be a ring. Two ideals $I, J \trianglelefteq R$ are coprime if $I + J = R$.

↳ Comment:
Let $m, n \in \mathbb{N}$. $m\mathbb{Z}, n\mathbb{Z} \trianglelefteq \mathbb{Z}$ are coprime $\iff$ m and n are coprime integers.

Theorem: (**Chinese remainder theorem/CRT**)

> Let R be a ring and let $I_1, \ldots, I_n \trianglelefteq R$ be pairwise coprime ideals. Denote $\pi_i : R \to R/I_i$ as the canonical projections. Then, $\pi : R \to R/I_1 \times \cdots \times R/I_n$, $x \mapsto (\pi_1(x), \ldots, \pi_n(x))$ is a surjective ring homomorphism with $\ker(\pi) = I_1 \cap \ldots \cap I_n$. In particular, $R/\bigcap_{i=1}^n I_i \cong \prod_{i=1}^n R/I_i$.

Definition: (**Congruent**)

> Let R be a ring and $I \trianglelefteq R$ an ideal. Two elements $x, y \in R$ are congruent modulo I if $x - y \in I$, written $x \equiv y \mod I$, or if $I = \langle a \rangle$, $x \equiv y \mod a$.

Corollary: (**Classic CRT**)

> Let $a_1, \ldots a_n \in \mathbb{Z}$ be pairwise coprime. Then, the system of conguences $x \equiv x_i \mod a_i, i = 1, \ldots, n$ is solvable for arbitrary $x_i \in \mathbb{Z}$. The solution x is unique modulo $a_1 \cdots a_n$, i.e. all solutions are $x + a_1 \cdots a_n\mathbb{Z}$.

↳ Solution algorithm:

1. Let $a := a_1 \cdots a_n$.
2. $\forall 1 \leq i \leq n$: Find $d_i \in a_i\mathbb{Z}$ and $e_i \in \frac{a}{a_i}\mathbb{Z}$ such that $d_i + e_i = 1$, e.g. via the extended Euclidian algorithm.
3. $x := \sum_{i=1}^n x_i e_i$ is a solution.

Euclidian domains

Proposition: (**Polynomial division**)

> Let R be a commutative ring and let $g \in R[X]$, $g \neq 0$ whose leading coefficient is a unit in R. Then, for any $f \in R[X]$, there are unique $q, r \in R[X]$ such that $f = qg + r$ and $\deg(r) < \deg(g)$.

Definition: (**Euclidian domain**)

> Let R be an integral domain. It is an Euclidian domain if there is a map $\delta : R \setminus \{0\} \to \mathbb{N}$ such that, $\forall f, g \in R, g \neq 0 \ \exists q, r \in R : f = qg + r$ and $r = 0$ or $\delta(r) < \delta(g)$. Here, δ is called the Euclidian function or degree function.

Algorithm: (**Euclidian algorithm**)

> Let R be a Euclidian domain and $a, b \in R \setminus \{0\}$. We wish to compute a gcd of a and b.
> 1. Set $z_0 := a$, $z_1 := b$.
> 2. For $i = 1, 2, \dots$: If $z_i = 0$, then set $z_{i+1} := 0$. If $z_i \neq 0$, then compute $q_i, z_{i+1} \in R$ such that $z_{i-1} = q_i z_i + z_{i+1}$ and $z_{i+1} = 0$ or $\delta(z_{i+1}) < \delta(z_i)$.
> 3. Return z_n such that $z_n \neq 0$ and $z_{n+1} = 0$.

Corollary: (**Extended Euclidian algorithm**)

> Let R be a Euclidian domain and $a, b \in R \setminus \{0\}$. Then, the Euclidian algorithm yields $x, y \in R$ such that the returned gcd is $xa + yb$, via substitution in the equations $z_{i-1} = q_i z_i + z_{i+1}$.

Corollary:

> The extended Euclidian algorithm can compute a gcd of multiple elements in a Euclidian domain, since $\gcd(a, b, c)$ is associated to $\gcd(\gcd(a, b), c)$

Proposition:

> Let R be an integral domain and let $a_1, \dots, a_n \in R$. If $\langle a_1, \dots, a_n \rangle = \langle g \rangle$ for some $g \in R$, then g is a gcd of $a_1, \dots, a_n$. In particular, in PIDs, gcd's always exist.

Corollary:

> Let R be a PID and let $a_1, \dots, a_n \in R$. Then, $g \in R$ is a gcd of $a_1, \dots, a_n \iff \langle g \rangle = \langle a_1, \dots, a_n \rangle$.

Unique factorization domains

Definition/Proposition: (**Unique factorization domain**)

> Let R be an integral domain. It is a factorial ring/unique factorization domain/UFD if every $a \in R$, $a \neq 0$, $a \notin R^*$ is a finite product of prime elements. Then, such a factorization is unique up to ordering and unit multiplication of each element.

↳ Comment:
In a UFD, gcd's always exist.

Proposition:

> Let R be a UFD and let $p \in R$, $p \neq 0$, $p \notin R^*$. Then, p is irreducible $\iff$ p is prime.

Skipped: Noetherian rings. Sorry Emmy :(

Theorem: (**Gauss**)

> If R is a UFD, then $R[X]$ is a UFD.

Corollary:

> If R is a UFD, then $R[X_1, \dots, X_n]$ is a UFD.

Proposition/Definition: (**Valuation**)

Let R be a UFD and let $P \subseteq R$ be a system of representatives of the prime elements in R, that is, every prime in R is associated to exactly one element in P. Consider the field of fractions $Q(R)$. Then, every $x \in Q(R)^*$ admits a unique factorization of the form $x = \varepsilon \prod_{p \in P} p^{v_p(x)}$ where $\varepsilon \in R^*$ and $v_p(x) \in \mathbb{Z}$ is the p-adic valuation of x. All but finitely many $v_p(x)$ are zero, that is, the product is finite.

If $f = \sum_{i=0}^{n} a_i X^i \in Q(R)[X]$, then for a prime p we define $v_p(f) := \min\{v_p(a_i) \mid i = 0, \dots n\}$. We set $v_p(0) := \infty$.

Definition: (**Primitive**)

Let R be a UFD. $f \in R[X]$ is primitive if 1 is a gcd of its coefficients.

Lemma:

Let R be a UFD and let $f \in R[X]$. Then, f is primitive $\iff$ $v_p(f) = 0$ for all primes $p \in R$.

Skipped: Gauss lemma and tools for proving Gauss theorem.

Proposition:

Let R be a UFD and $f \in R[X]$.
 (a) If $\deg(f) = 0$, then f is prime in $R[X]$ $\iff$ f is prime in R.
 (b) If $\deg(f) > 0$, then f is prime in $R[X]$ $\iff$ f is primitive and prime in $Q(R)[X]$.
Note: primes and irreducibles are equivalent in R, $R[X]$ and $Q(R)[X]$.

Proposition: (**Eisenstein's criterion**)

Let R be a UFD and let $f = a_n X^n + \cdots + a_0 \in R[X]$ be a primitive polynomial with $\deg(f) > 0$. If there is a prime $p \in R$ such that $p \nmid a_n$, $p \mid a_i$ for $i = 0, \dots, n-1$ and $p^2 \nmid a_0$, then f is irreducible in $R[X]$ (and equivalently in $Q(R)[X]$).

Proposition:

Let R be a UFD and S be an ID, and let $\sigma : R \to S$ be a ring homomorphsim. Let $f = a_n X^n + \cdots + a_0 \in R[X]$, and define $f^\sigma := \sigma(a_n)X^n + \cdots + \sigma(a_0) \in S[X]$. If $\deg(f^\sigma) = \deg(f) > 0$, and $f^\sigma \in S[X]$ is irreducible, then $f \in R[X]$ is irreducible.

↳ Comment:
This is usually used by applying the canonical projection $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}[X]$.

Modules

Definition: (**Module**)

Let R be a ring. A left R-module M is an abelian group $(M, +)$ with a map $R \times M \to M, (r, m) \mapsto rm$ such that
 (i) $\forall r_1, r_2 \in R, \forall m \in M : (r_1 r_2)m = r_1(r_2 m)$
 (ii) $\forall r_1, r_2 \in R, \forall m \in M : (r_1 + r_2)m = r_1 m + r_2 m$
 (iii) $\forall r \in R, \forall m_1, m_2 \in M : r(m_1 + m_2) = rm_1 + rm_2$
 (iv) $\forall m \in M : 1m = m$
Right R-modules are defined analogously with $M \times R \to M, (m, r) \mapsto mr$. If R is commutative, these coincide and we just say R-module.

Definition: (**Module homomorphism**)

> Let R be a ring and let M, N be left R-modules. A map $\varphi : M \to N$ is an R-module homomorphism if $\forall r_1, r_2 \in R, \forall m_1, m_2 \in M : \varphi(r_1 m_1 + r_2 m_2) = r_1\varphi(m_1) + r_2\varphi(m_2)$. We denote the set of these as $\mathrm{Hom}_R(M, N)$.
>
> A bijective R-module homomorphism is an isomorphism.

Definition: (**Submodule**)

> Let R be a ring and M be a left R-module. A subset $M' \subseteq M$ is a submodule of M if $M' - M' \subseteq M'$ and $RM' \subseteq M'$.

Proposition:

> Let R be a ring, M, N be left R-modules, $\varphi \in \mathrm{Hom}_R(M, N)$ be an R-module homorphsim and $M' \subseteq M$ and $N' \subseteq N$ be submodules. Then, $\varphi^{-1}(N') \subseteq M$ and $\varphi(M') \subseteq N$ are submodules. Specifically, $\ker(\varphi) = \varphi^{-1}(0)$ and $\mathrm{im}(\varphi) = \varphi(M)$ are submodules.

Proposition/Definition: (**Quotient module**)

> Let R be a ring, M be a left R-module and $N \subseteq M$ be a submodule.
> (a) $M/N := \{m + N \mid m \in M\}$ is a left R-module via $r(m + N) := rm + N$ called the quotient module.
> (b) The canonical projection $\pi : M \to M/N, m \mapsto m + N$ is a surjective R-module homomorphism with $\ker(\pi) = N$.
> (c) Let $\varphi \in \mathrm{Hom}_R(M, L)$ with $\ker(\pi) = N$. Then, $\mathrm{im}(\varphi)$ is canonically isomorphic to M/N.

Definition/Proposition: (**Generated submodule**)

> Let R be a ring, M be a left R-module and $E \subseteq M$ be a subset. Then, the submodule generated by E is, equivalently,
>
> $$\langle E\rangle := \bigcap_{\substack{\text{submodules } N\subseteq M,\\ E\subseteq N}} N = \left\{\sum_{i=1}^{n} r_i e_i \mid n \in \mathbb{N}, r_i \in R, e_i \in E\right\}.$$

Definition: (**Basis, etc.**)

> Let R be a ring, M be a left R-module and $E \subseteq M$ be a subset.
> (a) E generates M if $\langle E\rangle = M$.
> (b) M is finitely generated if $\exists E' \subseteq M$ that generates M with $|E'| < \infty$.
> (c) E is R-independent if $\forall n \in \mathbb{N}, \forall r_i \in R, \forall e_i \in E$ with pairwise distinct e_i's: $\sum_{i=1}^{n} r_i e_i = 0 \implies r_i = 0, i = 1, \dots, n$.
> (d) E is an R-basis of M is E generates M and E is R-independent. Note: This is equivalent to that every element in M can be written uniquely up to ordering as an R-linear combination of elements in E.
> (e) M is free if it has a basis.

Theorem/Definition:

> Let $R \neq \{0\}$ be a commutative ring and M be a finitely generated free R-module. Then, every R-basis of M has the same finite cardinality, called the rank of M.

Field extensions

Proposition/Definition: (**Characteristic**)

> Let R be an integral domain. Then, there is a unique ring homomorphism $\varphi : \mathbb{Z} \to R$. There is a $p \in \mathbb{N}$ such that $\ker(\varphi) = \langle p \rangle$ where p is either 0 or a prime number, called the characteristic of R, written $p = \mathrm{char}(R)$.

Definition: ($\mathbb{F}_p$)

> Let p be a prime number. Then, $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ as a field.

Proposition:

> (a) $0 = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = \mathrm{char}(\mathbb{R}[X])$
> (b) $\mathrm{char}(\mathbb{F}_p) = p$

Definition: (**Subfield**)

> A subring T of a field $\mathbb{K}$ is a subfield if T is a field.

Proposition/Definition: (**Prime subfield**)

> Let $\mathbb{K}$ be a field.
> (a) For every subfield T of K, we have $\mathrm{char}(T) = \mathrm{char}(\mathbb{K})$.
> (b) $P := \bigcap_{\text{subfields } T \subseteq \mathbb{K}} T$ is a subfield of $\mathbb{K}$, called the prime subfield of $\mathbb{K}$. It is the unique smallest subfield of $\mathbb{K}$.

Proposition:

> Let $\mathbb{K}$ be a field and P be its prime subfield.
> (a) $\mathrm{char}(\mathbb{K}) = p > 0 \iff P \cong \mathbb{F}_p$
> (b) $\mathrm{char}(\mathbb{K}) = 0 \iff P \cong \mathbb{Q}$

Definition: (**Extension field, etc.**)

> Let $\mathbb{L}$ be a field with a subfield $\mathbb{K}$.
> (a) The pair $\mathbb{K} \subseteq \mathbb{L}$ is called a field extension; $\mathbb{L}$ is an extension field of $\mathbb{K}$. We denote this as $\mathbb{L}/\mathbb{K}$.
> (b) An intermediate field is a subfield T such that $\mathbb{K} \subseteq T \subseteq \mathbb{L}$.
> (c) $\mathbb{L}$ is a $\mathbb{K}$-vector space by restricting $\cdot : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ to $\mathbb{K} \times \mathbb{L} \to \mathbb{L}$. The dimension of this vector space is $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$, called the degree of $\mathbb{L}$ over $\mathbb{K}$.
> (d) The field extension $\mathbb{K} \subseteq \mathbb{L}$ is finite if $[\mathbb{L} : \mathbb{K}]$ is finite, otherwise it is infinite.

Proposition:

> Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ be field extensions. Then, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}]$.

Corollary:

> Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ be field extensions. If $[\mathbb{M} : \mathbb{K}]$ is prime, then $\mathbb{L} = \mathbb{K}$ or $\mathbb{L} = \mathbb{M}$.

Definition: (**Algebraic**)

> Let $\mathbb{K} \subseteq \mathbb{L}$ be a field extension.
> (a) An element $\alpha \in \mathbb{L}$ is algebraic over $\mathbb{K}$ if $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ for $n \geq 1$ and $c_1, \ldots, c_n \in \mathbb{K}$. Otherwise, α is transcendental over $\mathbb{K}$.
> (b) The extension field $\mathbb{L}$ is algebraic over $\mathbb{K}$ if every $\alpha \in \mathbb{L}$ is algebraic over $\mathbb{K}$. Then, $\mathbb{K} \subseteq \mathbb{L}$ is an algebraic field extension.

Proposition/Definition: (**Minimal polynomial**)

> Let $\mathbb{K} \subseteq \mathbb{L}$ be a field extension and let $\alpha \in \mathbb{L}$ be algebraic over $\mathbb{K}$.
> (a) There is a unique monic polynomial $f_\alpha \in \mathbb{K}[X]$ of smallest degree such that $f_\alpha(\alpha) = 0$, called the minimal polynomial of α over $\mathbb{K}$.
> (b) f_α is irreducible. Moreover, if $f \in \mathbb{K}[X]$ is a monic, irreducible polynomial with $f(\alpha) = 0$, then $f = f_\alpha$.
> (c) $K[\alpha] \cong K[X]/\langle f_\alpha \rangle$ is an extension field of $\mathbb{K}$.
> (d) $[K[\alpha] : \mathbb{K}] = \deg(f_\alpha)$

Proposition/Definition: (**Generated field, etc.**)

> Let $\mathbb{K} \subseteq \mathbb{L}$ be a field extension.
> (a) For $\mathcal{A} \subseteq \mathbb{L}$, the subfield of $\mathbb{L}$ generated by $\mathcal{A}$ over $\mathbb{K}$ is
> $$\mathbb{K}(\mathcal{A}) := \bigcap_{\substack{\text{subfields } T \subseteq \mathbb{L}, \\ \mathbb{K} \cup \mathcal{A} \subseteq T}} T.$$
> It is the smallest subfield of $\mathbb{L}$ that contains both $\mathbb{K}$ and $\mathcal{A}$.
> (b) If $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$, we write $\mathbb{K}(\alpha_1, \ldots, \alpha_n) := \mathbb{K}(\mathcal{A})$. It holds that $\mathbb{K}(\alpha_1, \ldots, \alpha_n) = Q(K[\alpha_1, \ldots, \alpha_n])$.
> (c) The field extension $\mathbb{K} \subseteq \mathbb{L}$ is finitely generated if $\exists \alpha_1, \ldots, \alpha_n \in \mathbb{L} : \mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$. It is called simple if $n = 1$. The degree of α over $\mathbb{K}$ is $[\mathbb{K}(\alpha) : \mathbb{K}]$.
> (d) For (possibly infinite!) $\mathcal{A} \subseteq \mathbb{L}$, $\mathbb{K}(\mathcal{A}) = \bigcup_{\mathcal{A}' \subseteq A, |\mathcal{A}'| < \infty} \mathbb{K}(\mathcal{A}')$.

Theorem:

> Let $\mathbb{K} \subseteq \mathbb{L}$ be a field extension. Then, the following are equivalent:
> (i) $\mathbb{L}/\mathbb{K}$ is finite.
> (ii) $\exists \alpha_1, \ldots, \alpha_n \in \mathbb{L}$ which are algebraic over $\mathbb{K}$ with $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ (which also implies $\mathbb{L} = \mathbb{K}[\alpha_1, \ldots, \alpha_n]$).
> (iii) $\mathbb{L}/\mathbb{K}$ is finitely generated and algebraic.

Corollary:

> Let $\mathbb{K} \subseteq \mathbb{L}$ be a field extension. Then, $\mathbb{L}/\mathbb{K}$ is algebraic $\iff$ $\exists \mathcal{A} \subseteq \mathbb{L}$ with $\mathbb{L} = \mathbb{K}(\mathcal{A})$ and all $\alpha \in \mathcal{A}$ are algebraic over $\mathbb{K}$.

Proposition:

> Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ be field extensions.
> (a) If $\alpha \in \mathbb{M}$ is algebraic over $\mathbb{L}$, and $\mathbb{L}/\mathbb{K}$ is algebraic, then α is algebraic over $\mathbb{K}$.
> (b) $\mathbb{M}/\mathbb{K}$ is algebraic $\iff$ $\mathbb{M}/\mathbb{L}$ and $\mathbb{L}/\mathbb{K}$ are algebraic.

Algebraic closures

Proposition: (**Kronecker's construction**)

> Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[X]$ with $\deg(f) \geq 1$. Then, there is a finite field extension $\mathbb{K} \subseteq \mathbb{L}$ such that $f(\alpha) = 0$ for some $\alpha \in \mathbb{L}$. If f is irreducible, then we can set $\mathbb{L} := \mathbb{K}[X]/\langle f \rangle$ and $\alpha = \pi(X)$.

Corollary:

> Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[X]$ with $\deg(f) \geq 1$. Then, there is a finite field extension $\mathbb{K} \subseteq \mathbb{L}$ such that f factorizes into linear factors in $\mathbb{L}[X]$.

Definition/Proposition: (**Algebraically closed**)

> Let $\mathbb{K}$ be a field. It is algebraically closed if one of the following equivalent statements hold:
> (i) $\forall f \in \mathbb{K}[X] \setminus \mathbb{K}\ \exists \alpha \in \mathbb{K} : f(\alpha) = 0$
> (ii) $\forall f \in \mathbb{K}[X] \setminus \mathbb{K}\ \exists c \in \mathbb{K}^*, \exists \alpha_1, \ldots, \alpha_n \in \mathbb{K} : f = c \prod_{i=1}^{n}(X - \alpha_i)$
> (iii) Every algebraic field extension $\mathbb{K} \subseteq \mathbb{L}$ is trivial, i.e. $\mathbb{K} = \mathbb{L}$

Definition: (**Algebraic closure**)

> Let $\mathbb{K}$ be a field. An algebraic closure $\overline{\mathbb{K}}$ is an extension field of $\mathbb{K}$ that is algebraically closed, and algebraic over $\mathbb{K}$.

Definition: (**$\mathbb{K}$-homomorphism**)

> Let $\mathbb{K} \subseteq \mathbb{L}$ and $\mathbb{K} \subseteq \mathbb{L}'$ be field extensions. A field homomorphsim $\varphi : \mathbb{L} \to \mathbb{L}'$ is a $\mathbb{K}$-homomorphism if $\varphi|_{\mathbb{K}} = \mathrm{id}_{\mathbb{K}}$. If φ is also a field isomorphism, then φ is a $\mathbb{K}$-isomorphism.

Theorem:

> Let $\mathbb{K}$ be a field.
> (a) $\mathbb{K}$ has an algebraic closure $\overline{\mathbb{K}}$.
> (b) For any two algebraic closures $\overline{\mathbb{K}}_1, \overline{\mathbb{K}}_2$ of $\mathbb{K}$, there is a $\mathbb{K}$-isomorphism $\varphi : \overline{\mathbb{K}}_1 \xrightarrow{\sim} \overline{\mathbb{K}}_2$.

Skipped: Tools for proving this theorem

Splitting fields

Definition: (**Splitting field**)

> Let $\mathbb{K}$ be a field and let $\mathcal{F} \subseteq \mathbb{K}[X] \setminus \mathbb{K}$. A splitting field of $\mathcal{F}$ over $\mathbb{K}$ is an extension field $\mathbb{L}$ of $\mathbb{K}$ such that
> (i) Every $f \in \mathcal{F}$ factorizes into linear factors in $\mathbb{L}[X]$
> (ii) $\mathbb{L} = \mathbb{K}(\mathcal{A})$ where $\mathcal{A} = \{\alpha \in \mathbb{L} \mid \exists f \in \mathcal{F} : f(\alpha) = 0\}$

↳ Comment:
$\mathbb{L}$ is a splitting field of $\{f_1, \ldots, f_n\} \iff \mathbb{L}$ is a splitting field of $f_1 \cdots f_n$.

Theorem:

> Let $\mathbb{K}$ be a field and let $\mathcal{F} \subseteq \mathbb{K}[X] \setminus \mathbb{K}$.
> (a) There is a splitting field of $\mathcal{F}$ over $\mathbb{K}$.
> (b) For any two splitting fields $\mathbb{L}_1, \mathbb{L}_2$ of $\mathcal{F}$ over $\mathbb{K}$, there is a $\mathbb{K}$-isomorphism $\mathbb{L}_1 \xrightarrow{\sim} \mathbb{L}_2$.

Finite fields

Theorem:

> Let $\mathbb{F}$ be a finite field. Denote $p := \mathrm{char}(\mathbb{F})$ and $q := |\mathbb{F}|$.
> (a) $p > 0$, and $\mathbb{F}$ contains $\mathbb{F}_p$ as its prime subfield.
> (b) $q = p^n$ where $n = [\mathbb{F} : \mathbb{F}_p]$.
> (c) $\mathbb{F}$ is a splitting field of $X^q - X$ over $\mathbb{F}_p$. Its elements are precisely the q different zeros of $X^q - X$.

Theorem:

> Let $n \in \mathbb{N}$ and let p be a prime number. Let $q := p^n$.
> (a) There exists a field $\mathbb{F}_q$ with $\left|\mathbb{F}_q\right| = q$.
> (b) $\mathbb{F}_q$ is unique up to $\mathbb{F}_p$-isomorphism.

Overview of types of rings

Rings $\subset$ Commutative rings $\subset$ IDs $\subset$ GCD domains $\subset$ UFDs $\subset$ PIDs $\subset$ Euclidian domains $\subset$ Fields

Implications of general ring types:

- If R is an ID, then $R[X_1, \ldots, X_k]$ is an ID.
- If $\mathbb{K}$ is a field and $R \subseteq \mathbb{K}$ is a nonzero subring, then R is an ID.
- If R is a UFD, then $R[X_1, \ldots, X_n]$ is a UFD (Gauss theorem).
- If $\mathbb{K}$ is a field, then $\mathbb{K}[X]$ is a Euclidian domain (with $\delta = \deg$).
- If $\mathbb{K}$ is a field and $f \in \mathbb{K}[X]$ with $\deg(f) \geq 1$, then $\mathbb{K}[X]/\langle f \rangle$ is a field $\iff$ f is irreducible.

Specific examples of rings:

- $\mathbb{Z}$ is a Euclidian domain (with $\delta = \mathrm{abs}$).
- $\mathbb{Z}[X]$ is a UFD, but not a PID.
- $\mathbb{Z}/p\mathbb{Z}$ is a field iff p is prime (otherwise just a commutative ring)
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, out of which only $\mathbb{C}$ is algebraically closed.