1 Commutative Rings

1.1 Rings

Definition

A **Ring** ist a set R endowmed with elements $0 \in R, 1 \in R$ and three maps

$$+ : R \times R \to R, \quad - : R \to R, \quad \cdot : R \to R$$

such that the following axioms hold:

- (R,+) is an **abelian Group** with neutral element $0 \in R$ and inverse operation $-$, i.e such that for all $a, b, c \in R$:
  - $(a + b) + c) = a + (b + c)$,
  - $0 + a = a$
  - $(-a) + a = 0$
  - $a + b = b + a$
- Distributivity $(a + b) \cdot c = a \cdot c + b \cdot c$, and $a \cdot (b + c) = a \cdot b + a \cdot c$
- Associativity : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Additionally, if the multiplication is commutative, we call $(R, +, \cdot, 0, 1)$ a **commutative Ring**.

Note the following:

- Note that 0 is uniquely determined by the axioms ad that the additive inverse operation $-$ is well defined.
- $0 \neq 1$ is *not* part of the definition.
- $0 \cdot a = 0, \forall a \in R$. Proof: $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 = 0 \cdot a$

We will use the convention, where we omit parenthesis for addition and multiplication in series and we will do ("Punkt vor Strich").

Notation: For any Ring we will write for $n \in \mathbb{N}$ and $a \in R$ recursively:

$$0_{\mathbb{Z}} \cdot a := 0, \quad 1_{\mathbb{Z}} \cdot a := a, (n + 1) \cdot a := n \cdot a + a, (-n) \cdot a = -(n \cdot a)$$

In essence, we just contructed a mapping

$$\mathbb{Z} \times R \to R, \quad (n, a) \mapsto n \cdot a$$

This mapping is also distributive.
Further, we will also define the natural powers for elements a in the ring as:

$$a^0 := 1, a^1 := a, a^{n+1} := a^n \cdot a$$

For commutative rings we then have the properties

$$a^{m+n} = a^m \cdot a^n, (a^m)^n = a^{m \cdot n}$$

Definition

Let R, S be Rings and let $f : R \to S$ a map.
We say that f is a **Ring homomorphism**, if

- $f(1_R) = 1_S$
- $f(a+b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$

Further, if f is invertible, we call f a **Ring isomorphism**

- Note that $f(0_R) = 0_S$, since $f(0) = f(0) + f(0) \implies 0 = f(0)$
- $f(-a) = -f(a)$ for all $a \in R$

Definition

Let R be a Ring and $S \subseteq R$ a Ring aswell. We say that S is a **Subring** of R if the inclusion mapping $\iota : S \to R$ is a Ring homomorphism.

Examples:

- Since we didn't use the axiom that $0 \neq 1$, we can construct the trivial Ring $R = \{0\}$, where $0 = 1$.
- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{Q}$ are subrings each.
- Let V be a vector space. Then the **Endomorphism ring**
$$\operatorname{End}(V) := \{f : V \to V \text{linear}\}$$
is a Ring, where addition and is defined element wise and multiplication is composition.
- $\operatorname{Mat}_{m,n}(\mathbb{Q})$, or $\mathbb{R}, \mathbb{C}, \mathbb{Z}$ is a Ring with matrix addition and matrix multiplication.
- Let $m \geq 1$. Then $\mathbb{Z}_m = \mathbb{Z}_{/\mathbb{Z}m}$ is a Ring. We wil usually denote the equivalence clases $[a]$ with underlines $\underline{a}$. The addition and multiplication is indeed well defined:
$$\underline{a} + \underline{b} := \underline{a+b}, \underline{a} \cdot \underline{b} := \underline{a \cdot b}$$
- The adjoint Rings $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ or $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ are rings.
- Let X be a set and define $\mathbb{Z}^X := \{f : X \to \mathbb{Z}\}$ with element wise operations. This is a commutative Ring.
- The function space $C([0,1]) = \{f : [0,1] \to \mathbb{C} \text{continuous}\}$ is a commutative Ring.

Some examples of Ring homomorphisms:

- The following is *not* a Ring homomorphism $f : \{0\} \to \mathbb{Z}, f(0) = 0$, since $0_R = 1_R$, but $f(1_R) \neq 1$
- On the other hand, $R \to \{0\}, a \mapsto 0$ is a Ring homomorphism and is uniquely determined.

- The mapping $\mathbb{Z} \to R, n \mapsto n \cdot 1_R$ is also a Ring homomorphism and is uniquely determined.
- $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ as described earlier are Ring homomorphisms, as the are Subrings of eachother.
- $\mathbb{R} \to \mathrm{Mat}_{n,n}(\mathbb{R})t \mapsto t \cdot E_n$ is a Ring homomorphism.
- The mapping $C([0,1]) \to \mathbb{C}, f \mapsto f(x)$, some $x_0 \in \mathbb{C}$, is a ring homomorphism.
- $\mathbb{Z} \to \mathbb{Z}_m, a \mapsto \underline{a}$ is again a ring homomorphism.
- $\mathrm{mat}_{m,n}(\mathbb{C}) \to \mathrm{End}(\mathbb{C}^n), A \mapsto (x \in \mathbb{C}^n \mapsto Ax)$ is a Ring isomorphism.

Lemma

Let R be a ring and $a, b \in R$ such that $a \cdot b = b \cdot a$.. Then for any $n \in \mathbb{N}$ we have the well known Binomial formula

$$(a+b)^n = \sum k = 0^n \binom{n}{k} a^k b^{n-k}$$

Further, for $n = 2$. If the binomial formula holds, this also implies that $ab = ba$

1.2 Unit, Divisibility, Quotientfield

This corresponds to pages 34ff.

In $\mathbb{Z}_{15}$ we have $\underline{3} \cdot \underline{5} = \underline{15} = \underline{0}$ but $\underline{3} \neq 0 \neq \underline{5}$

Definition

Let R be a Ring, An element $a \in R \setminus \{0\}$ is called a **zero divisor** if there exists a $b \in R\{0\}$ such that $ab = 0$.

Definition

A commutative Ring is called an **integral domain**, if $0 \neq 1$ and the following holds

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

The Ring $C([0,1])$ is not an integral domain.
When is $\mathbb{Z}_m$ an integral domain? It is one if and only if m is prime.

Lemma

Let R be a commutative Ring with $0 \neq 1$. Then R is an integral domain if and only if R has no zero divisors.

Proof: If R is an integral domain and $a \in \mathbb{R} \setminus \{0\}$ and there exists a $b \in R$ such that $ab = 0$. Then $ab = a \cdot 0 \implies b = 0$. So a is not a zero divisor.
If on the converse R has no zero divisor, and $a, b, c \in R, a \neq 0$ such that $ab = ac \neq 0$. which implies $a(b-c) = 0 \implies b - c = 0 \implies b = c$.

Definition

Let R be a commutative Ring and $a, b \in R$, we say a **divides** b and we write $a|b$ (in R), if there exists a $c \in R$ such that $b = ac$.

Definition

We call $a \in R$ a unit if $a|1$ and we write

$$\mathbb{R}^\times := \{a \in R : a|1\}$$

Note that $\mathbb{R}^\times$ is a group under multiplication.
Examples:

- $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$
- $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$
- $\mathbb{Z}[\sqrt{2}]^\times = ?$

Definition Field

A **Field** is a commuative Ring K with $0 \neq 1$ and such that any element $a \neq 0 \in K$ has a multiplicative inverse

Lemma

A field is an integral domain

Let $a \neq 0$ and $b, c \in K$. Then $ab = ac \implies a^{-1}ab = a^{-1}ac \implies b = c$

Proposition

Let $m \geq 1 \in \mathbb{N}$. Then $\mathbb{Z}_m$ is a field if and only if m is prime.

Proof: If $m = 1$, then $\mathbb{Z}_1 = \{\underline{0}\}$ is not a field.
If $m = ab$, then $\underline{0} = \underline{a} \cdot \underline{b}$. So $\mathbb{Z}_m$ is not a field.

Not if m is prime and $\underline{a} \neq \underline{0}$. Set $d = \text{lcd}(m, a)$. Per definition, d divides m, but since m is prime, either $d = 1$ or $d = m$. If $d = m$, we would have $m|a$ which would imply $\underline{a} = \underline{0}\lightning$. So since $d = 1$, we can use the previous lemma to show that there exist $k, l \in \mathbb{Z}$ such that

$$1 = km + la \implies \underline{1} = \underline{l} \cdot \underline{a}$$

Which means that $\underline{a} \neq \underline{0}$ has a multiplicative inverse $\underline{l}$.

Theorem Quotient Field

Let R be an integral domain. Then there exists a field k which contains R and such that $K = \{\frac{p}{q} | p, q \in R, q \neq 0\}$. For $R = \mathbb{Z}$, we have $K = \mathbb{Q}$

Proof: We define the relation $\sim$ on the set $X = R \times R \setminus \{0\}$ as follows:

$$(a, b) \sim (p, q) \Leftrightarrow aq = pb$$

We can think of the tuple (a, b) as the fraction $\frac{a}{b}$, without having to define fractions.
This relation is an equivalence relation. Indeed since we have the equal sign in the definition, reflexivity and symmetry follow immediately.
Moreover, if $(a, b) \sim (p, q)$ and $(p, q) \sim (m, n)$ we have

$$aq = pb \wedge pn = mq \implies aqn = pbn \wedge pnb = mqb$$

Because R is an integral domain and $q \neq 0$, we get $an = mb$, which shows transitivity.
Now consider $K = X/_\sim$ and the Elements

$$0_k := [(0, 1)]_\sim \quad \text{and} \quad 1_K := [(1, 1)]_\sim$$

together with the operations $+$ and $\cdot$ defined as follows:

$$[(a, b)]_\sim + [(p, q)]_\sim := [(aq + pb, bq)]_\sim$$
$$[(a, b)]_\sim \cdot [(p, q)]_\sim := [(ap, bq)]_\sim$$

There operations are welldefined (i.e. independent on the choice of representation), refer to the Book!

Lastly, we need to show that K fulfills the field axioms. We will skip many of them here, so refer to the book.
We have that $[(a, b)]_\sim + [(p, q)]_\sim = [(aq + bp)]_\sim = [(pb + aq, qb]_\sim$.

It is also clear that $0_k = [(0, 1)]_\sim \neq [(1, 1)]_\sim = 1_k$, as $0 \cdot 1 \neq 1 \cdot 1$ in R.
Also if $[(a, b)]_\sim \neq [(0, 1)]_\sim = 0_k$, then $a \neq 0$ so we can write

$$[(a, b)]_\sim \cdot [(b, a)]_\sim = [(ab, ab)]_\sim = 1_k$$

From now on, we will write $\frac{a}{b} := [(a, b)]_\sim$.

To show that R is contained in K, we identify $a \in R$ with $\frac{a}{1} \in K$. Note that the corresponding mapping $\iota(a) = \frac{a}{1}$ is an *injective* Ringhomomorphism because for $a \neq 0$ we have $\frac{a}{1} \neq \frac{0}{1}$, so $\operatorname{Ker} \iota = \{0\}$

Definition

Let K be a field and $L \subseteq K$ a subring that is also a field. We then call L a subfield of K.

Exercise: Use SageMath to find out, for which $p = 2, 3, \ldots 100$ there exists a $g \in (\mathbb{Z}/_{p\mathbb{Z}})^\times$ such that

$$(\mathbb{Z}/_{p\mathbb{Z}})^x = \{g^k : k = 0, 1, \ldots\}$$

1.3 Polynomial Ring

In the following, R is always a commutative ring. We want to define the Polynomialring $R[X]$ of Polynomials in the variable X and coefficients in R.

For the field $\mathbb{F}_2 = \{0,1\}$ we do *not* want the Polynomiasl $X^2 + X$ to equal the zero polynomial, despite the fact that for any $x \in \mathbb{F}$ we have $x^2 + x = 0$. Therefore, we have to define the polynomials through its coefficients.

Definition Polynomial Ring

Let R be a commutative Ring. We define the Ring of formal power-series (in one variable over the Ring R) as

- The set of all sequences $(a_n)_{n\geq 0} \subseteq R^{\mathbb{N}}$
- $\mathbf{0} := ((0_n)_{n\geq 0}$ and $\mathbf{1} = (1,0,0,\dots)$
- $+ : (a_n)_{n\geq 0} + (b_n)_{n\geq 0} := (a_n + b_n)_{n\geq 0}$
- $\cdot : (a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} := (c_n)_{n\geq 0}$ where

$$c_n = \sum_{i=0}^{n} a_i b_{n-1} = \sum_{i+j=n} a_i b_j$$

  If $a_n = 0$ for all $n \geq N$ large enough, we call this the Polynomial Ring (in one Variable) over the Ring R

As usual, we have to show all the ring axioms but we will omit some of them.

- $(\mathbf{1} \cdot a)_n = \sum_{i+j=n} \underbrace{\mathbf{1}_i}_{\delta_{i0}} a_j = a_n$
- $(ab)c = a(bc)$ since

$$((ab)c)_n = \sum_{i+j=n} (ab)_i cJ = \sum_{i+j+k=n} a_i b_j c_k$$

- $((a+b)\cdot c)_n = \sum_{i+j=n}(a+b)_i c_j = \sum_{i+j=n} a_i c_j + \sum_{i+j=n} b_i c_j = (ac+bc)_n$
- We further check that the product of two polynomials is again a polynomial. So if a, b are polynomials, there exists $I, J \in \mathbb{N}$ such that $a_n = 0, \forall n \geq I$ and $b_n = 0, \forall n \geq J$. So $(a+b)_n = 0$ for $n \geq \max I, J$ and $(a \cdot b)_n = 0, \forall n \geq I + J$

Notation: We introduce a new Symbol X and identify the Symbol with the polynomial $X = (0,1,0,\dots)$, aswell as its powers $X^2 = (0,0,1,\dots)$ etc.
More generally, let $a = (a_0, a_1, a_2, \dots)$ be a polynomial, then we have

$$X \cdot a = (0, a_0, a_1, a_2, \dots), \quad (X \cdot a)_n = \sum_{i+j=n} X_i a_j = a_{n-1} \quad \text{for } n \geq 1$$

We will write $R[X] = \{\sum_{i=0}^{n} a_i X^i | n \in \mathbb{N}, a_i \in R\}$ ("R-adjoint-X") for the Polynomialring in the variable X.
And $R[[X] = \{\sum_{i=0}^{\infty} | a_i \in R\}$ for the Ring of formal power series in the variable X.

Definition Degree

Let $p \in R[X] \setminus \{0\}$. The **degree** of p, write $\deg(p)$ equals n, if $p_n \neq 0$ and $p_k = 0$ for $k > n$. We call p_n the leading coefficient of p. We define $\deg(0) := -\infty$

Proposition

Let R be an integral domain. Then $R[X]$ is also an integral domain. Further we have for $p, q \in R[X] \setminus \{0\}$:

- $\deg(pq) = \deg(p) + \deg(q)$ and the leading coefficient of the product is the product of the leading coefficients.
- $\deg(p+q) \leq \max \deg(p), \deg(q)$
- If $p|q$, then $\deg(p) \leq \deg(q)$

Proof: Let $f = p \cdot q \neq 0$. Then $f_n = \sum_{i+j=n} p_i q_j$.
If we assume $n > \deg(p) + \deg(q)$, then $p_i q_j = 0$ for all $i + j = n \implies f_n = 0$. For $n = \deg(p) + \deg(q)$, the only summand that doesn't vanish is for $i = \deg(p)$ and $j = \deg(q)$.
Assume, $p|q$, then there exists a Polynomial $g \neq 0$ such that $q = p \cdot g$. Since $\deg(q) = \deg(p) + \underbrace{\deg(g)}_{\geq 0} \geq \deg(p)$

Angenommen $p = \sum_{n=0}^{\deg p} p_n X^n, q = \sum_{n=0}^{\deg q} q_n X^n$. Dann ist $p + q = \sum_{n=0}^{\max\{\deg p, \deg q\}} (p_n + q_n) X^n$. Also folgt die Aussage. Die Ungleichheit gilt nur dann, falls $p_{\deg n} = -q_{\deg n}$ für $n = \deg q = \deg q$

Proposition

Sei K ein Körper. Dann wird der Quotientenkörper von $K[X]$ als der Körper der rationalen Funktionen $K(X) = \{\frac{f}{g} : f, g \in K[X], g \neq 0\}$ bezeichnet.
Die Elemente sind nicht unbedingt Funktionen, da die Polynome selber nicht Funktionen sind. (Siehe $X^2 + X$ in $\mathbb{F}_2$).

Wenn wir die obige Konstruktion iterieren, erhalten wir den Ring der Polynome in mehreren Variablen

$$R[X_1, X_2, \ldots, X_d] := R[X_1][X_2] \ldots [X_d]$$

Falls $R = K$ ein Körper ist, definieren wir auch

$$K(X_1, X_2, \ldots, X_d) = \{\frac{f}{g} | f, g \in K[X_1, \ldots, x_d]\}$$

Bemerkung: Auf $R[X_1, \ldots, X_d]$ gibt es mehrere Grad-Funktionen

$$\deg_{X_1}, \deg_{X_2}, \ldots, \deg_{X_d}, \quad \deg_{\text{tot}}(f) = \max\{m_1 + \ldots + m_d | f_{m_1, \ldots, m_d} \neq 0\}$$

Wobei hier $f \in R[X_1, \ldots, X_d]$ folgende Form hat

$$f = \sum_{m_1, \ldots, m_d} f_{m_1, \ldots, m_d} X_1^{m_1} \ldots X_d^{m_d}$$

Satz

Seien R, S zwei kommutative Ringe. Ein Ringhomomorphismus $\Phi : R[X]$ nach S ist eindeutig durch seine Einschränkung $\varphi = \Phi|_R$ und durch das Element $x = \Phi(X) \in S$ bestimmt. Des weiteren definiert

$$\Phi\left(\sum_n a_n X^n\right) = \sum_n \varphi(a_n) x^n$$

einen Ringhomomorphismus falls $\varphi : R \to S$ ein Ringhomomorphismus ist und $x \in S$ beliebig ist.

Beweis: Sei $\Phi : R[X] \to S$ ein Ringhomomorphismus, $\varphi = \Phi_R$ und $x = \Phi(X) \in S$. Dann gilt

$$\Phi\left(\sum_n a_n X^n\right) = \sum_n \Phi(a_n X^n) = \sum_n \varphi(a_n) \cdot \Phi(x)^n *) \qquad (()$$

Sei nun $\varphi : R \to S$ ein Ringhomomorphismus und $x \in S$ beliebig. Wir verwenden $(*)$ um Φ zu definieren. Es ist klar dass

- $\Phi(\mathbf{1}) = \varphi(1_R) x^0 = 1_S$
- $\Phi(a+b) = \Phi\left(\sum_n (a_n + b_n) X^N)\right) = \sum_n \varphi(a_n + b_n) x^n = \ldots = \Phi(a) + \Phi(b)$
- $\Phi(a \cdot b) = \sum_n \varphi\left(\sum_{i+j=n} a_i b_j) x^n\right) = \left(\sum_i \varphi(a_i) x^i\right)\left(\sum_j \varphi(b_j) x^j\right) = \Phi(a) \cdot \Phi(b)$

Notation, wir schreiben für zwei kommutative Ringe R, S

$$\mathrm{Hom}_{\mathrm{Ring}}(R, S) = \mathrm{Hom}(R, S) := \{\varphi : R \to S | \varphi \text{ ist ein Ringhomomorphismus}\}$$

In dieser Notation können wir den obigen Satz in der Form

$$\mathrm{Hom}(R[X], S) \cong \mathrm{Hom}(R, S) \times S$$

beziehungweise für den Fall in mehreren Variablen:

$$\mathrm{Hom}(R[X_1, \ldots, X_n], S) \cong \mathrm{Hom}(R, S) \times S^n$$

Falls wir $R = S$ und $\varphi = \mathrm{id}$ setzen, so erhalten wir für jedes $a \in R$ die entsprechende Auswertungsabbildung

$$\mathrm{ev}_a : f \mapsto f(a) = \sum_n f_n a^n$$

Wenn wir $a \in R$ variieren, ergibt sich auch eine Abbildung

$$\Psi : f \in R[X] \to (f(\cdot) : R \to R, a \mapsto f(a)) \in R^R$$

Wir statten R^R mit den punktweisen Operationen aus, womit $\Phi : R[X] \to \mathbb{R}^R$ ein Ringhomomorphismus ist.
Falls $|R| < \infty$ und $\mathbb{R} \neq \{0\}$, so kann Ψ nicht injektiv sein.
Beispiel: Sei $R = \mathbb{Z}$ und $S = \mathbb{Z}/\mathbb{Z}_m[X]$ für ein $m \geq 1$. Dann gibt es einen Ringhomomorphismus

$$f \in \mathbb{Z}[X] \mapsto \overline{f} = \sum_n (f_n \mod m) X^n \in \mathbb{Z}/\mathbb{Z}_m[X]$$

Beispiel: $R = \mathbb{C}, S = \mathbb{C}[X]$, $\varphi(a) = \overline{a}$. Dann ist

$$f \in \mathbb{C}[X] \mapsto \sum_n \overline{f_n} X^n \in \mathbb{C}[X]$$

2 Ideale und Faktorringe

Definition Ideal

Sei R ein kommutativer Ring. Ein Ideal in R ist eine Teilmenge $I \subseteq R$, so dass

(a) $0 \in I$

(b) $a, b \in I \implies a + b \in I$

(c) $a \in I, x \in R \implies xa \in I$

Beispiel: Seien R, S zwei kommutative Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist

$$\operatorname{Ker} \varphi = \{a \in \mathbb{R} | \varphi(a) = 0\}$$

ein Ideal.

Satz Faktorring

Sei R ein kommutativer Ring und $I \subseteq R$ ein Ideal.

(a) Die Relation $a\tilde{b} \Leftrightarrow a - b \in I$ ist eine Äquivalenzrelation auf R. Wir schreiben auch $a \equiv b \mod I$ und wir schreiben R/I (“R modulo I”) für den **Faktorring** der Äquivalenzklassen

(b) DIe Addition, Multiplikation und das Negative induzieren wohldefinierete Abbildungen $R/I \times R/I \to R/I$ bzw. $R/I \to R/I$.

(c) Mit diesen Abbildungen, $0_{R/I} = [0]_\sim, 1_{R/I} = [1]_\sim$ ist R/I ein Ring und die kanonische projektion

$$\rho : R \to R_i, \quad a \in R \mapsto [a]_\sim = a + I$$

ist ein surjektiver Ringhomomorphismus.

Beweis:

- $a \sim a$, denn $a - a = 0 \in I$. Weiter ist da falls $a - b \in I$ ist auch $b - a = (-1)(a - b) \in I$. Transitivität folgt, da $a - c = a - b + (b - c) \in I$. Also ist $\sim$ eine Äquivalenzrelation.
- Angenommen $a \sim a', b \sim b'$. Dann gilt

$$ab - a'b' = ab - a'b + a'b - a'b' = b(a - a') + a'(b - b') \in I$$

  Der Beweis für die Addition ist trivial und für das additive Inverse folgt aus Multiplikation mit -1.
- Da die Rinaxiome nur Gleichungen enthalten (i.e. $0 \neq 1$ ist kein Axiom) sind die Ringaxiome in R/I direkte Konsequenzen der Ringaxiome in R. Des weiteren ist die Projektion $p : R \to R/I, a \mapsto [a]_\sim$ ein Ringhomomorphismus.

Beispiele:

- $I = \mathbb{Z}_m \subseteq \mathbb{Z}$ ist ein Ideal.
- $I = R$ und $I = \{0\}$ sind Ideale in jedem beliebigen kommutativen Ring.

Lemma

Sei $I \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gilt

$$I = R \Leftrightarrow 1 \in I \Leftrightarrow I \cap R^{\times} \neq \emptyset$$

Beweis: Angenommen $u = v^{-1} \in I$ und $v \in R, a \in R$. Dann gilt $a = avu \in I$. Da $a \in R$ beliebig war, folgt $I = R$.

The Lemma answers the following question. What Ideals are there in a field K? Just $\{0\}$ and K itself.

Definition

Let R be a commutative Ring and let $a_0, \dots, a_n \in R$. Then

$$I = (a_1, \dots, a_n) = \{x_1 a_1 + x_2 a_1 +, \dots, x_n a_n | x_1, \dots, x_n \in R\}$$

is called the Ideal **generated** by $a_1, \dots, a - N$. For $a \in R$ we call $I(a) = Ra$ the **principal ideal** of a.

Lemma

Let R be a commutative Ring.

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

(b) If R is an integral domain, then $(a) = (b) \Leftrightarrow \exists u \in \mathbb{R}^{\times}$ such that $b = ua$

Proof: If $(a) \subseteq (b)$, then since $a = 1 \cdot a$, we have $a \in Rb$ which means $b|a$.

Lemma

Let R be a commutative Ring. Then

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

(b) If R is an integral domain, then

$$(a) = (b) \Leftrightarrow \exists c \in \mathbb{R}^{\times} : b = ac$$

Proof: Let $(a) \subseteq (b)$. Since $a = 1 \cdot a \in (a)$ it follows that $a \in (b) = Rb$, which means that there exists some $x \in R$ such that $a = xb$, i.e $b|a$. If on the other hand, if $b|a$, then $a \in (b)$, so $(a) = Ra \subseteq (b)$.
For the second item, the implication to the left follows from the first item. So if $(a) = (b)$, then there exist $x, y \in R$ such that $a = xb$ and $b = ya$. We then get $a = xb = xya$. If $a = 0$, then also $b = 1$ and we can just use $c := 1 \in R^{\times}$. If $a \neq 0$, then we have $xy = 1$ so $x, y \in R^{\times}$.

Beispiel Sei $R = C_{\mathbb{R}}([0,3])$. Betrachte die Funktionen

$$a(x) = \begin{cases} -x+1, & \text{für} \quad x \in [0,1], \\ x-2, & \text{für} \quad x \in [2,3], \\ 0 & \text{sonst} \end{cases}$$

$$b(x) = \begin{cases} x-1, & \text{für} \quad x \in [0,1], \\ x-2, & \text{für} \quad x \in [2,3], \\ 0 & \text{sonst} \end{cases}$$

Behauptung: Die Ideale $(a) = (b)$ sind gleich, aber $b \notin R^{\times} a$.
Die Ideale sind gleich, denn $a = b \cdot f$ für

$$f(x) = \begin{cases} -1, & \text{für} \quad x \in [0,1], \\ 1, & \text{für} \quad x \in [2,3], \\ 2x-3 & \text{sonst}, \end{cases}$$

Aber aus dem Zwischenwertsetz folgt, dass $f(x) = 0$ für ein $x \in [0,3]$. Also ist f nicht invertierbar (i.e. $f \notin R^{\times}$)

Falls $I \subseteq R$ ein Ideal ist und $a \in R$, dann ist die Restklasse für Äquivalenz modulo I gleich

$$[a]_{\sim} = \{x \in R . x \sim a\} = a + I$$

Erster Isomorphiesatz

Angenommen R, S sind kommutative Ringe und $\varphi : R \to S$ ist ein Ringhomomorphismus.

(a) Dann induziert φ einen Ringisomorphismus

$$\overline{\varphi} : R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi = \varphi(R) \subseteq R$$

so dass $\varphi = \overline{\varphi} \circ \rho$, wobei $\rho : R \to R/\operatorname{Ker}\varphi$ die kanonische Projektion ist. Das heisst es gilt folgendes **kommmutatives Diagramm**.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\rho"] & S \\ R/\operatorname{Ker}\varphi \arrow[ur, "\overline{\varphi}"] & \end{tikzcd}$$

Sei $I \subseteq \operatorname{Ker}\varphi$ ein Ideal in R. Dann induziert φ einen Ringhomomorphismus $\overline{\varphi} : R/I \to S$ mit $\varphi = \overline{\varphi} \circ \rho_I$.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\rho_I"] & S \\ R/I \arrow[ur, "\overline{\varphi}"] & \end{tikzcd}$$

Beweis: Wir beginnen mit 2) und definieren

$$\overline{\varphi}(x + I) = \varphi(x)$$

Dies ist wohldefiniert. Falls $x + I = y + I$, so ist $x - y \in I \subseteq \operatorname{Ker}\varphi$. Also ist $\varphi(x) - \varphi(y) = \varphi(x - y) = 0$.

Da φ ein Ringhomomorphismus ist, gilt

$$\begin{aligned} \varphi(1_R) = 1_S &\implies \overline{\varphi(1 + I) = 1_S} \\ \overline{\varphi}(x + i + y + I) &= \varphi(x + I) + \varphi(y + I) \\ \overline{\varphi}((x + I)(y + I)) = \overline{\varphi}(xy + I) = \varphi(xy) = \varphi(x) + \varphi(y) &= \overline{\varphi}(x + I)\overline{\varphi}(y + I) \end{aligned}$$

Und es gilt auch $\varphi = \overline{\varphi} \circ \rho_I$, denn für $x \in R$ gilt $\varphi_I(x) = x + I$, also $\overline{\varphi} \circ \rho_I(x) = \overline{\varphi}(x + I) = \varphi(x)$ per Definition von $\overline{\varphi}$. Also kommutiert das Diagramm.
Weiterhin haben wir

$$\begin{aligned} \operatorname{Ker}\overline{\varphi} &= \{x + I \big| \varphi(x) = 0\} = \operatorname{Ker}\varphi / I \\ \operatorname{Im}(\overline{\varphi}) &= \{\overline{\varphi}(x) \big| x \in R/I\} = \operatorname{Im}\varphi \end{aligned}$$

Da $\operatorname{Ker}\varphi$ ein Ideal Ist, folgt aus dem zweiten Teil, dass $\overline{\varphi}$ ein Ringhomomorphismus ist.
Weiterhin ist

$$\operatorname{Ker}\overline{\varphi} = \operatorname{Ker}\varphi / \operatorname{Ker}\varphi = \{0 + \operatorname{Ker}\varphi\}$$

Also ist $\overline{\varphi}$ injektiv.
Bemerkung: Sei $I_0 \subseteq R$ ein Ideal in einem kommutativen Ring. Dann gibt es eine kanonische Korrespondenz zwischen Idealen in R/I_0 und Idealen in R, die I_0 enthalten. Betrachte die Abbildung

$$(I \subseteq R, I_0 \subseteq I) \mapsto I/I_0 = \{x + I_0 \big| x \in I\} \subseteq R/I_0$$

$$J \subseteq R/_i \mapsto \rho_{I_0}^{-1}(J) \subseteq R$$

Definition

Wir sagen zwei Ideale I, J in einem kommutativen Ring sind **coprim**, falls $I + J = R$ ist. Also $\exists a \in I, b \in J$ mit $a + b = 1$.

Beispiel $I =\subseteq (p)$ und $J = (q) \subseteq \mathbb{Z} = R$. Dann sind die Ideal coprim, falls q und p verschiedene Primzahlen sind.

Chinese remainder Theorem

Let R be a commutative Ring and let $I_1, \ldots, I_n$ be pairwise coprime Ideals. Then the Ringhomomorphism

$$\begin{aligned} \varphi : R &\to R/I_1 \times \ldots \times R/I_n \\ x &\mapsto (x + I_1, \ldots, x + I_n) \end{aligned}$$

is surjective and $\operatorname{Ker}\varphi = I_1 \cap \ldots \cap I_n$

Proof: It follows directly from the definition, that $\operatorname{Ker}\varphi = I_1 \cap \ldots \cap I_n$
We show that φ is surjective, by finding an $x_i \in R$ for each i such that

$$\varphi(x_i) = (0 + I_n, \ldots, 1 + I_i, \ldots 0 + I_n) \in \operatorname{Im}(\varphi)$$

Without loss of generality, we can assume that $i = 1$. Then we want to show, that there exist $a \in I_1$ and $b \in I_2 \cap \ldots \cap I_n$ such that $a + b = 1$. We then can show that $x_1 = b$ satisfies

$$\varphi(x_1) = (b + I_1, b + I_2, \ldots, b + I_n) = (1 + I_1, 0 + I_2, \ldots, I_n)$$

We show this using induction on n. For $n = 2$, I_1 and I_2 we obtain the case in the previous lemma.
Now assume that I_1 and $I_2 \cap \ldots I_n$ are coprime, i.e. there exist $a \in I_1$ and $b \in I_2 \cap \ldots \cap I_n$ such that $a + b = 1$. Furthermore, since I_1 is coprime to I_{n+1}, (there exist $c \in I_1, d \in I_{n+1}$ such that $c + d = 1$.
We can then write

$$a + b(c + d) = 1 \implies a + bc + bd = 1$$

Since a and c are in I_n, the term $a + bc$ is also in I_1. And because the Intersectin of Ideals is again an ideal, we get $bd \in I_2 \cap \ldots \cap I_n$ and $bd \in I_{n+1}$. This shows that $bd \in I_2 \cap \ldots \cap I_{n+1}$
We can use this to show that φ is indeed surjective. Let

$$(a_1 + I_2, \ldots, a_n + I_n) \in R/I_1 \times \ldots \times R/I_n$$

Then we can write

$$\varphi(a_1x_1 + \ldots + a_nx_n) = (a_1x_1 + \ldots + a_nx_n + I_1, \ldots, a_1x_1 + \ldots + a_nx_n + I_n) = (a_1 + I_1, \ldots, a_n + I_n)$$

2.1 Characteristic of a Field

Let K be a field, Then there exists a Ringhomomorphism

$$\varphi : \mathbb{Z} \to K, \quad n \in N \mapsto 1 + \ldots + 1, \quad -n \in \mathbb{N} \mapsto -(1 + \ldots + 1)$$

Let $I = \operatorname{Ker}\varphi$ such that

$$\mathbb{Z}/I \simeq \operatorname{Im}\varphi \subseteq K$$

Since K is a field, we know that $\operatorname{Im}\varphi$ is an integral domain.

Lemma

Let $I \subseteq \mathbb{Z}$ be an ideal. Then it is also a principal Ideal $I = (m)$ for an $m \in \mathbb{N}$. The quotient is an integral domain if and only if $m = 0$ or if m is a prime number.

The proof will follow a similar idea as when showing that o If $I \cap \mathbb{N}_{>0}$ is the empty set, it's clear that $I = \{0\}$. Else we can look for the smallest non-zero element $m \in I \cap \mathbb{N}_{>0}$. If $n \in I$ we can use division with remainder to obtain $n = k \cdot m + r$ for $k \in \mathbb{Z}$ and $r \in \{0, \ldots, m - 1\}$. But since I is an ideal, r is also in I and because m is the smallest element, $r = 0$. So $I = (m)$.
If $m = ab$ trivial. If $m > 0$ is prime, then $\mathbb{Z}/(m)$ is a field and thus an integral domain.

Definition Characteristic

Let K be a field. We say that K has **characteristic** zero, if $\varphi : \mathbb{Z} \to K$ is injective. We say that K has characteristic $p \in \mathbb{N}_{>0}$, if $\operatorname{Ker} \varphi = (p)$.

Example: The fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero. Note that since $\mathbb{Z}$ is the initial ring, we can always divide out $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z})/\sim$. So such a field always contains an isomorphic copy of $\mathbb{Q}$.
The Field $\mathbb{F}_p = \mathbb{Z}/(p)$, for p prime (or else it's not a field) has characteristic p

Proposition

Let K be a field with characteristic $p > 0$. Then the *Frobeniusmap*

$$F : x \in K \to x^p$$

a Ring homomorphism. If $|K| < \infty$, F is a Ring automorphism.

Proof: $F(0) = 0, F(1) = 1$ $F(xy) = F(x)F(y)$. For addition, we use the binomial expansion.

$$F(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$$

Where we used $p | \binom{p}{k}$ for $k \notin \{0, p\}$. Since

$$\binom{p}{k} := \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!}$$

If $|K| < \infty$, F is also surjective since it is injective by $\operatorname{Ker} \varphi = \{0\}$ because K is finite.

2.2 Primeideals and Maximal ideals

Definition Primeideal & Maximal ideal

Let R be a commutative Ring and $I \subseteq R$ be an ideal.
We say I a **prime ideal**, if R/I is an integral domain.
We say I is a **maximal ideal**, if R/I is a field.

There are also other ways to define these properties:

Proposition

Let $I \subseteq R$ be an ideal of a commutative ring.

(a) I is a prime ideal if and only if $I \neq I$ and for all $a, b \in R$ we have

$$ab \in I \implies a \in I \text{ or } b \in I$$

(b) I is a maximal ideal if and only if $I \neq R$ and any other ideal J containing I is either I or R, so

$$J \supsetneq I \implies J = R$$

Proof: For prime ideals, we have the equivalency

$$\begin{aligned} R/I \neq \{0+I\} \text{ and } [a][b] = 0 &\implies [a] = 0 \text{ or } [b] = [0] \\ \iff I \neq R \text{ and } ab \in I &\implies a \in I \text{ or } b \in I \end{aligned}$$

For the maximal ideals assume that R/I is a field, then $0 \neq 1$, so $I \neq R$. If $J \supsetneq I$ is an ideal bigger than I, then $x \in J, x \neq I$ means $[x] \neq [0]$ and because R/I is a field, we can find its inverse $[y]$ such that $[xy] = [1]$which means $xy - 1 \in I \subseteq J$. But because J is an ideal, we have $xy - (xy - 1) = 1 \in J$ so $J = R$.

For the other way around, let $[x] \neq [0] \in R/I$. Define the ideal $J := (x) + I \subsetneq R$ which is bigger than I. Because I is maximal, it must mean that $J = (x) + I = R$, so x generates all the remaining numbers in R. In particular there exists a $y \in R$ such that $x \cdot y - 1 \in I$. Which means that in R/I we have $[x] \cdot [y] = [1]$, so R/I is a field.

Prime ideals in the well known ring $R = \mathbb{Z}$ are the principal ideals of prime numbers inlucding zero, so

$$I = (M) \text{ is prime ideal } \iff m = 0 \text{ or } m = \pm p \text{ for } p\text{prime}$$

and for maximal ideals we have

$$I = (m) \text{ is maximal ideal } \iff m = \pm p \text{ for } p \text{ prime}$$

In the next example we will look at maximal ideals in the polynomialrings and how we can describe it in other ways:
Example: Let K be a field and $a_1, \dots, a_n \in K$. We define the Ideal

$$I = (X_1 - a_1, \dots, X_n - a_n) \subseteq K[X_1, \dots, X_n]$$

Then I is a maximal Ideal and it is also the kernel of the evaluation mapping

$$\mathrm{ev}_{a_1,\dots,a_n} : K[X_1, \dots, X_n] \to K, \quad f \mapsto f(a_1, \dots, a_n)$$

Proof: I is included in $\mathrm{Ker}(\mathrm{ev}_{a_1,\dots,a_n}$ since $\mathrm{ev}(X_i - a_i) = a_i - a_i = 0$ for all $i = 1, \dots, n$. Now if $f \in \mathrm{Ker}\,\mathrm{ev}_{a_1,\dots,a_n}$ then we can write

$$f = \sum a_{k_1,\dots,k_n} X_1^{k_1} \dots X_n^{d_n}$$

$$X_i^{k_i} = (a_i + X_i - a_i)^{k_i} = a_i^{k_1} + \underbrace{k_i a_i^{k_i - 1}(X_i - a_i) + \dots}_{\in I}$$

So $[X_i^{k_i}][a_i^{k_i}]$. So since $f(a_1, \dots, a_n) = 0$ we have that

$$[f] = \left[\sum a_{k_1,\dots,k_n} a_1^{k_1} \dots a_n^{k_n}\right] = [0]$$

Therefore $I = \mathrm{Ker}\,\mathrm{ev}_{a_1,\dots,a_n}$. Using the first isomophism theorem we have that

$$K[X_1, \dots, X_n]/I = K[X_1, \dots, X_n]/\mathrm{Ker}(\mathrm{ev}_{a_1,\dots,a_n}) \simeq \mathrm{Im}(\mathrm{ev}_{a_1,\dots,a_n} = K$$

So since R/I is a field like K is, I is maximal.

Note: Hilbert's Nullstellensatz says that every maximal ideal in $\mathbb{C}[X_1, \dots, X_n]$ is of this form which is one of the foundations of algebraic geometry.

2.3 Axiom of choice and Zorn's Lemma

The axiom of choice

Let I be a set and let X_i for $i \in I$ non-empty sets. Then the set $\prod_{i \in I} X_i$ is non-empty and there exists a function

$$f : I \to \bigcup_{i \in I} X_i \quad \text{with} \quad f(i) \in X_i \forall i \in I$$

Definition Poset

A set X is **partially ordered** (is a **poset**) if there is a relation $x \leq y$ defined on X which is

(a) reflexive: $x \leq x$ for all $x \in X$

(b) anti-symmetric: $x \leq y \wedge y \leq x \implies x = y$

(c) transitive $x \leq y \wedge y \leq z \implies x \leq z$

An element $x \in X$ is called **maximal**, if $x \leq y \implies y = x$ for all $y \in X$.
An element $x \in X$ is called a **maximum** of X, if $y \leq x$ for all $y \in X$.
If $A \subseteq X$ is a subset, then an element $x \in X$ is called an **upper bound** of A, if $a \leq x$ for every $a \in A$.

Definition chain

A Poset X is a **chain** (or totally ordered), if forall $x, y \in X$, either $x \leq y$ or $y \leq x$.
We call a poset **inductive**, if every chain has an upper bound.

Zorn's Lemma

Let $(X, \leq)$ be an inductive poset. Then X has a maximal element.

Theorem

Let R be a commutative Ring and $I \subsetneq R$ an ideal. Then there exists a Maximal ideal $\boldsymbol{m} \supseteq I$. In particular, every non-trivial Ring $R \neq \{0\}$ has a maximal ideal.

We will prove this using Zorn's lemma. For this we define

$$X = \{J \subsetneq R | J \text{ is an Ideal and} I \subseteq J\}$$

and we use inclusion of subsets as our ordering on X.
We have to show that every chain K in X has an ###. If $K = \emptyset$.###

Let K be a non-empty chain in X. We show that $\tilde{J} = \bigcup_{J \in K} J$ is an upper bound of K. For every $J \in K$ we have $J \subsetneq R$, which means $1 \neq J$. Therefore we also must have $1 \notin \tilde{J} \subsetneq R$. Therefore $\tilde{J}$ is an upper bound of K. This means that X is an inductive chain and we can use Zorn's lemma to find that there is a maximal element. In our case this is is an Ideal $\boldsymbol{m}$ that contains I and isn't equal to R.

Of course we would have to show that $\tilde{J}$ is in fact an ideal, but that is trivial.

We will now prove Zorn's Lemma using the axiom of choice.
The idea is that we start with the empty set $\emptyset$ representing a chain and we want to find elements of a continuosly growin chain by adding an upper bound to the chain.
The problem is that in general the union of chains doesn't have to be a chain.

Formal proof: For every subset $C \subseteq X$ we define

$$\hat{C} = \{x \in X \setminus C | x \text{ is an upper bound}\}$$

Using the axiom of choice, we can obtain a new element by looking at the choice-function f of the set

$$\left\{\hat{C} | C \subseteq X \wedge \hat{C} \neq \emptyset\right\}$$

Next we call a subchain $K \subseteq X$ an **f-chain** , if for every subset $C \subseteq K$ with $\hat{C} \cap K \neq \emptyset$ the element $f(\hat{C})$ is in K and is minmal uppper bound of C in K. (i.e. $f(\hat{C}) \leq y$ for all $y \in \hat{C} \cap K$.
We use this to remove unnecessary additions in the uninon of the chains. For example, the empty chain $K_{\text{min}} = \emptyset$ is an f-chain. Also, $K_1 = \{f(\hat{K_{\text{min}}})\} = K_{\text{min}} \cup \{f(\hat{K}_{\text{min}}\}$ is another f-chain.

We can generalize this to keep increasing the f-chains:

Lemma

If K is an f-chain and $\hat{K} \neq \emptyset$, then $K_{\text{new}} = K \cup \{f(\hat{K})\}$ is again an f-chain.

Proof: Let $C \subseteq K_{\text{new}}$. If $\hat{C} \cap K \neq es.$ then $f(\hat{C}) \in K$ is a minimal element of $\hat{C} \cap K$ since K is an f-chain. But then we also have that $f(\hat{C}) \in K_{\text{new}}$ is a minimal element of $\hat{C} \cap K_{\text{new}}$.
If $C \subseteq K$ and $\hat{C} \cap K = \emptyset$ then $\hat{C} = \hat{K}$. Therefore $f(\hat{C}) = f(\hat{K}) \in K_{\text{new}}$ is a minimal element of C.
If on the other hand $f(\hat{K}) \in C$, then $\hat{C} \cap K_{\text{new}} = \emptyset$ and we're done.

Now what happens if we compare two f-chains and take their union. Is it thrue that the union is just the bigger of the two?

Lemma

Let K, K' be two f-chains and $K' \setminus K \neq 0$. Then $K \subseteq K'$ and $x \leq x'$ for all $x \in K, x' \in K' \setminus K$.

Proof: Let $x' \in K', x \in K$. Define $C = \{x \in K \cap K' | x \leq x'\} \subseteq K'$ and use the fact that K' is an f-chain. Since $x' \in \hat{C} \cap K'$ we have $f(\hat{C}) \in K'$ and $f(\hat{C}) \leq x'$.
If $\hat{C} \cap K \neq 0$, then $f(\hat{C}) \in K$ because it is an f-chain. But then $f(\hat{C}) \in C \cap \hat{C}$, which can't be true.
###

Now assumptions on K and K' were that $x' \in K' \setminus K$, therefore $K \subseteq K'$ or else we could just switch the roles of K and K'.

Lemma

Now define the union of all such f-chains.

$$K_{\max} = \bigcup_{K \text{ is f-chain}} K$$

Then $K_{\max}$ is another f-chain.

Proof: Since for pairs of chains K, K' either $K \subseteq K'$ or $K' \subseteq K$, it is trivial that $K_{\max}$ is a chain. Now we have to show that it is also an f-chain.
Let $x' \in \hat{C} \cap K_{\max}$ and let K' be an f-chain such that $x' \in K'$. We now show that $C \subseteq K'$.
Let $x \in C$. Then there exists an f-chain K such that $x \in K$. From the previous lemma we have $K \subseteq K'$ or $K' \subseteq K$. In the first case, $x \in K'$ follows trivially. But if $K' \leq K$, since K' contains all elements of K which are boundend by x'. And since $x' \in \hat{C}$ and $x \in C$ we must have $x \leq x'$, which shows $x \in K'$.

So since $C \subsetneq K', x' \in \hat{C} \cap K'$ and because K' is an f-chain we must have $f(\hat{C}) \in K' \subseteq K_{\max}$ and $f(\hat{C}) \leq x'$. Since $x' \in \hat{C} \cap K_{\max}$ ###
Proof of Zorn's lemma: By Definition, $K_{\max}$ is a maximal f-chain in X. The first lemma however says that if $\hat{K}_{\max}$ were non-empy, we can find a "bigger" chai. Therefore $\hat{K}_{\max} = \emptyset$.
Further $K_{\max}$ is a partial chain, which has an upper bound $x_{\max}$ because X is an ordered set. Thefore $x_{\max} \in K_{\max}$ is a maximum of $K_{\max}$. Therefore, $x_{\max}$ is a maximal Element of X.
Further, $K_{\max}$ is a subchain which ## missing last 2 minutes

Notation: Let $S \subseteq R$ be a subring Let $a_1, \dots, a_n \in R$. We define

$$\begin{aligned} S[a_1, \dots, a_n] &= \bigcap_{\substack{T \subseteq R \\ T \supseteq S}} T \\ &= \mathrm{ev}_{a_1,\dots,a_n}\left(S[X_1, \dots, X_n]\right) \\ &:= \left\{ \sum_{k_1,\dots,k_n \in M} c_{k_1,\dots,k_n} a_1^{k_1} \dots a_n^{k_n} \middle| |M| < \infty, M \subseteq \mathbb{N}^n, c_{k_1,\dots,k_n} \in S \right\} \end{aligned}$$

Proof: We know from the exercises that $S[a_1, \dots, a_n]$ is a subring containing, by definition, S and $a_1, \dots, a_n$. Further, we know that $\mathrm{ev}_{a_1,\dots,a_n}[X_1, \dots, X_n]$ is also a subring, since ev is a Ringhomormorphism. Which shows

$$S[a_1, \dots, a_n] \subseteq \mathrm{ev}_{a_1,\dots,a_n}\left(S[X_1, \dots, X_n]\right)$$

The other inclusion folllows becuase $S[a_1, \dots, a_n]$ is a subring. And again, we know that S and $a_1, \dots, a_n$ are included which implies

$$\sum_{(k_1,\dots,k_n) \in M} \underbrace{c_{k_1,\dots,k_n}}_{\in S} a_1^{k_1} \dots a_n^{k_n} \subseteq S[a_1, \dots, a_n]$$

This underlines the idea that we can define the span in a vector space as the set containing all linear combinations, or as the vector space equivalent of an ideal generated by the vectors For example we have

$$\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{Z}\} \subseteq \mathbb{Q}$$
$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$
$$\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$
$$\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$$

The last one is indeed a field as we have

$$\frac{a+\sqrt{2}}{c+\sqrt{2}} = \frac{a+\sqrt{2}}{c+\sqrt{2}}\frac{c-\sqrt{2}d}{c-\sqrt{2}d} = \frac{1c-2bd+\sqrt{2}(ad-bc)}{c^2-2d^2}$$

2.4 Matrices

Let R be a commutative Ring, $m, n \in \mathbb{N}_{>0}$. We define the set $\mathrm{Mat}_{mn}(R)$ as the set of all $m \times n$ matrices

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

with coefficients $a_{11}, \dots, a_{mn} \in R$.
For $m = n$ we define Addition and Multiplication as usual, which defines a ringed structure on $\mathrm{Mat}_{nn}(R)$ with identity matrix

$$I_n = (\delta_{ij})_{i,j}$$

It should be noted that for $n > 1$ the ring is not comutative in general. We denote its unit by

$$\mathrm{GL}_n(R) := \mathrm{Mat}_{nn}(R)^\times$$

Meta-proposition

Every calculation-rule for matrices over R that only make use of $+, -, \cdot, 0, 1$ also apply for any commutative Ring R.
They are

- $\det(AB) = \det(A) \cdot \det(B)$
- $A\tilde{A} = \tilde{A}A = \det(A)I_m$, where $\tilde{A}$ is the complementary Matrix

$$\tilde{A} = \left((-1)^{i+j}\det(A_{ji})\right)_{i,j}$$

Lemma

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

Proof: Let $f = \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} X_1^{k_1} \dots X_n^{k_n}$ be a polynomial, for which the corresponding polyomial function

$$f : \mathbb{R}^n \to \mathbb{R}, \quad (a_1,\dots,a_n) \mapsto f(a_1,\dots,a_n)$$

vanishes. Then this must also be true for any partial derivative of f. Let $(l_1,\dots,l_n) \in \mathbb{N}^n$. Then we have

$$\begin{aligned} 0 &= \partial_{X_1}^{l_1} \dots \partial_{X_n}^{l_n} f(0) \\ &= \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} k_1 \cdot (k_1-1)\dots(k_1-l_1+1)X_1^{l_1} \dots k_n(k_n-1)\dots(k_n-l_n+1)X^{k_n-l_n} \\ &= c_{k_1,\dots,k_n} l_n! \dots l_n! \end{aligned}$$

So we can eliminate every $c_{k_1,\dots,k_n}$ which shows that $f = 0$.This lemma also holds for any field K with $|K| = \infty$.

To prove the proposition, we first note that

- Every entry in $A(BC)-(AB)C$ a polynomial with integer coefficients in the variables $a_{11},\dots,a_{nn}, b_{11}\dots b_{nn}, c_{11},\dots$
- $\det(AB) - \det(A)\det(B)$ is again a polynomial with integer coefficients in the variables a_{ij}, b_{kl}.
- Every entry in $A\tilde{A} - \det(A)I_n$ is a polynomial with integer coefficients in the variables a_{ij}.

For the case $R = \mathbb{R}$ we know that these polynomials evaluated at any point result in zero. Using the previous Lemma, the polynomials also must be zero, so using the Ringhomomorphism $\mathbb{Z} \to R$, on the coefficients, we know that all these equations hold for any matrices over R for any ring R.

3 Faktorisierungen in Ringen

We want to factorize Rings with unique prime-factorisation. In the following, let R denote an integral domain.
Recall the definition of divisibility: $a|b \iff \exists c$ such that $ac = b$ and of the unit: $a \in R^\times \iff a|1$.

Definition irreducible/prime

We say an element $p \in R \setminus \{0\}$ is **irreducible**, if $p \notin R^\times$ and for all $a, b \in R$ we have

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

We say $p \in R \setminus \{0\}$ is **prime**, if the ideal (p) is a prime ideal. In other words: if $p \notin R^\times$ and for all $a, b \in R$ we habe $p|ab \implies p|a$ or $p|b$.

In a general Ring, the two definitions are not equivalent but we have the following implication

Lemma

Let R be an integral domain. Then every $p \in R$ prime is also irreducible.

Proof: Let $p \in R \setminus \{0\}$ and let $p = ab$ for some $a, b \in R$. Since then also $p|ab$ and because p is prime we can assume without loss of generality, that $p|a$. Then $a = p \cdot c$ for some $c \in R$ and because R is an integral domain, we can show that

$$p = ab = pcb \implies 1 = cb, \implies b \in R^\times$$

3.1 Euclidean Rings

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 the following holds:

- **Degree inequality:** $N(f) \leq N(fg)$, for all $f, g \in \mathbb{R} \setminus \{0\}$..
- **Division with rest:** For $f, g \in R$ with $f \neq 0$ there exist $q, r \in R$ such that $g = qf + r$ where $r = 0$ or $N(r) < N(f)$. We call q the **quotient** and r the **rest** of the division.

Examples:

- Any field K with $N(f) = 0$ is a euclidean ring.
- $R = \mathbb{Z}$ with $N(n) = |n|$ is a euclidean ring.
- For a field K, the Ring $R = K[X]$ and $N(f) = \deg f$ is a euclidean ring.
- $R = \mathbb{Z}[i]$ with $N(a + ib) = |a + ib|^2 = a^2 + b^2$ is a euclidean ring.
- $R = \mathbb{Z}[\sqrt{2}]$ with $N(a + \sqrt{2}b) = |a^2 + 2b^2|$ is a euclidean ring.

Algebraic number theory works with these objects. Here we prove the division with rest for $R = K[X]$. Let $f \neq 0, g \in R$. If $\deg g < \deg f$ chose $q = 0$ and $r = g$ and we're done. We use induction on the degree of g. Let $m \in \mathbb{N}$ be the degree of g and $\deg f = n \leq m$. We define

$$\tilde{g} = g - \frac{g_m}{f_n} X^{m-n} f$$

Since $\tilde{g}$ has $\deg \tilde{g} \leq< \deg g$ there exist $\tilde{q}, \tilde{r}$ such that

$$\tilde{g} = f\tilde{q} + \tilde{r} \implies g = f(\frac{g_m}{f_n} X^{m-1} + \tilde{q}) + \tilde{r}$$

We will now prove that $\mathbb{Z}[i]$ is in fact a euclidean ring. Recall that $N(a + ib) = |a + ib|^2$. Which has the nice property of being multiplicative:

$$N(z \cdot w) = N(z)N(w), \quad \text{for } z, w \in \mathbb{Q}[i] \text{ or } \mathbb{Z}[i]$$

The degree inequality immediately follows from the multiplicativity, as for $z \neq 0$ we have $N(z) \geq 1$. Division with rest is as follows. Let $f, g \in \mathbb{Z}[i], f \neq 0$. We define $z := \frac{g}{f} \in \mathbb{Q}[i]$ for $z = a + ib, a, b \in \mathbb{Q}[i]$ and consider its best approximation in $\mathbb{Z}[i]$. Using the rounding operation $[\cdot] : \mathbb{Q} \to \mathbb{Z}$, we chose q and r to be

$$q := [a] + i[b] \in \mathbb{Z}[i], \quad r := g - fq$$

Which because $(x - [x]) \leq \frac{1}{2}$ satisfy

$$|z - q| \leq \sqrt{(a - [a])^2 + (b + [b])^2} \leq \frac{1}{\sqrt{2}} \implies N(z - q) < 1$$

From the definition of r, we have $g = fq + r$. Therefore

$$N(r) = |r|^2 = |g - fq|^2 = |f^2| \underbrace{|z - q|^2}_{<1} < N(f)$$

We can also show that $R = \mathbb{Z}[\sqrt{2}]$ is also a euclidean Ring and the proof is similar to the previous example. We define

$$\Phi : \mathbb{Q}[\sqrt{2}] \to \mathrm{Mat}_{22}(\mathbb{Q}), \quad a + \sqrt{2}b \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

which is a Ring homomorphism (and is also $\mathbb{Q}$-linear), since $\Phi(1) = I_2$ and $\Phi(\sqrt{2})^2 = \Phi(2)$.
We define the Norm function using this homomorphism:

$$N(a + \sqrt{2}b) = |\det \Phi(f)| = |a^2 - 2b^2|$$

The division with rest is similar as with $\mathbb{Z}[i]$. This works because $\mathbb{Q}[\sqrt{2}]$ is a field, which means that $z = \frac{g}{f} a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$ so we can round to the nearest integer again

$$q = [a] + \sqrt{2}[b] \in \mathbb{Z}[\sqrt{2}] \implies N(z - q) = |(a - [a])^2 - 2(b - [b])^2| < 1$$

Theorem

In a euclidean Ring, every Ideal is a principal ideal.

Proof: Let $I \subseteq R$ be an ideal. If $I = \{0\}$, then $I = (0)$. Now assume that $I \neq \{0\}$. Now define $f \in I$ as an element such that

$$N(f) = \min\{N(g) | g \in I \setminus \{0\}\} \subseteq \mathbb{N}$$

We then show that $I = (f)$. Since $f \in I$ we obviously have $(f) \subseteq I$. Now assume $g \in I$. After division with rest there exist $q, r \in R$ such that $g = q \cdot f + r$ with $r = 0$ or $N(r) < N(f)$. If $r = 0$, then $g = qf \in (f)$, but if $r \neq 0$, then we have

$$r = g - qf \in I \implies N(r) < N(f) = \min\{N(x) | x \in I \setminus \{0\}\} ↯$$

3.2 Principal Ideal Domain

Definition Principal Ideal Domain

Let R be an integral domain. We call R a **Principal Ideal Domain**, if every Ideal in R is a principal ideal.

Every euclidean Ring is Principal Ideal Domain.

Proposition

Let R be a Principal Ideal Domain. For every two elements $f, g \in \mathbb{R} \setminus \{0\}$ there exists a greatest common denominator d such that $(d) = (f) + (g)$

Proof: Since $I = (f) + (g)$ is an Ideal and R is a principal ideal domain, there exists a $d \in R$ such that $I = (d)$. Therefore, because $(f), (g) \subseteq (d)$ we have $d|f$ and $d|g$. If d' is another gcd, of f and g, then $(d) \subseteq (d') \implies d'|d$.

Definition gcd

Let $f, gd \in \mathbb{R} \setminus \{0\}$. We say d is a largest common denominator of f and g, if $d|f$ and $d|g$ and if every other common denominator also divides d.

Note that if d, d' are two gcd's have $d = ad'$ for $a \in R^\times$.

In a euclidean Ring we can obtain a gcd of $f, g \in R \setminus \{0\}$ using the *euclidean algorithm.*
Without loss of generality we can assume $N(f) \leq N(g)$. Divide with rest and obtain $g = qf + r$. If $r = 0$, then $\gcd(f, g) = f$. If $r \neq 0$ then $\gcd(f, g) = \gcd(r, f)$. Because $N(r) < N(f) \leq N(g)$, this algorithm will end. This algorithm works, since

$$r = g - qf \in I \implies f \in (r) + (f), g = qf + r \in (r) + (f) \implies (f) + (g) = (r) + (f)$$

Theorem Prime elements

Let R be a principal ideal domain. Then

(a) $p \in R \setminus \{0\}$ is prime if and only if p is irreducible.

(b) Every $f \in R \setminus \{0\}$ can be written as a product of a unit and finitely many prime elements.

Proof: We already know that prime $\implies$ irreducible. Let $p \in R \setminus \{0\}$ be irreducible and assume that $p|ab$. If $p|a$ there is nothing to show.
If $p \nmid a$, we use the fact that there exists a gcd d of p and a. Since $d|p$ we have $p = de$, but because p is irreducible, either $d \in R^\times$ or $e \in R^\times$. If the latter were true, we would have $d = pe^{-1}$, but then we would have $p|d, d|a \implies p|a \lightning$. Therefore $d \in R^\times$. Therefore

$$d = xp + ya \implies b = xbd^{-1}p + \underbrace{yd^{-1}ab}_{p|ab} \implies p|b$$

Which shows that p is prime. Before proving (b), we first prove the next proposition

Proposition

Let R be a principal ideal domain and $p \in R$ irreducible. Then (p) is a maximal ideal, and p is prime.

Proof: Let $J \subseteq R$ be an ideal such that $J \supsetneq (p)$. Since R is a PID, there exists a $d \in R$ such that $J = (d) \supsetneq (p)$, which means that $d|p$, i.e. $\exists c \in R : p = dc$. Because p is irreducible, we know that either d or c is a unit. If c were a unit, we had $d = pc^{-1}$, but that would be that $d \in (p)$ which contradicts our assumption that $(d) \supsetneq (p)$. Therefore d is a unit, which shows that $(d) = R$. In other words, (p) is indeed a maximal ideal, and therefore p is prime.

We also need one more proposition for the proof of the theorem

Proposition

Let R be a PID and let

$$J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$$

be an ascending chain of Ideals in R. Then there exists an $n \in \mathbb{N}$ such that $J_m = J_n$ for all $m \geq n$

Proof: Define $J = \bigcup_{n=\mathbb{N}} J_n$. Since it is the union of ideals containing the ideals lower in the chain, we know that J itself is an ideal. And since R is PID, $J = (d)$. But then there exists an $n \in N$ such that $J_n = (d) = J = J_m$ for $m \geq n$.

With this, we can easily prove (b) from the previous theorem:
Let $f \in R \setminus \{0\}$. If f is a unit or is irreducible, then f there is nothing to show.
Now assume that $f \in R \setminus \{0\}$ can not be written as a finite product of a unit and prime elements. Assume that $f = f_0 = f_1\tilde{f}_1$. If both f_1 or $\tilde{f}_1$ could be decomposed, then the same would be true for f. We may now assume that it is f_1 that can't be decomposed. Then we would ahve

$$f_0 = f_1\tilde{f}_1, f_1 = f_2\tilde{f}_2, f_2 = f_3\tilde{f}_3 \dots$$

In particular we would have a sequence of elements that divide each other: $f_{n+1}|f_n$ which means that we get an ascending chain of ideals

$$(f_n) \subseteq (f_{n+1}), \quad \forall n \in \mathbb{N}$$

Using the second proposition, we would have that there exists an $n \in \mathbb{N}$ such that $(f_n) = (f_{n+1})$. But since R is a PID, we know that after looking at the prime elemnts which generate these ideals, that $f_n = af_{n+1}$ for some unit $a \in R^\times$. And because the $\tilde{f}_n$ which contradicts the constructin of $f_n, \tilde{f}_n$.

For example, let's look at some prime numbers in $\mathbb{Z}[i]$. Some of them are $1 \pm i, 3, 2 \pm i$. Then we can describe the units of this Ring to be

$$\mathbb{Z}[i]^\times = \{z \in \mathbb{Z}[i] | N(z) = 1\} = \{\pm 1, \pm i\}$$

We also know that 2 is not prime in $\mathbb{Z}[i]$ since $2 = (1+i)(1-i)$ as well as $5 = (2+i)(2-i)$ is not prime either.

Lemma

Let $z \in \mathbb{Z}[i]$ such that $N(z) = p \in \mathbb{Z}$ for p prime in $\mathbb{N}$. Then z is irreducible (and prime since $\mathbb{Z}[i]$ is a PID).

Proof: Let $z = uv$ for $u, v \in \mathbb{Z}[i]$. Then

$$p = N(z) = N(uv) = N(u)N(v) \implies \text{wlog } N(u) = 1 \implies u \in \mathbb{Z}[i]^\times$$

Lemma

Let $p \in \mathbb{N}$ be prime in $\mathbb{N}$ that can not be written as a sum of two squares, then p is also prime in $\mathbb{Z}[i]$

Proof: Assume $p = z \cdot w$. Then $N(z) \cdot N(w) = N(p) = p^2$. So $N(z)|p^2$ (in $\mathbb{N}$). So we have $N(z), N(w) \in \{1, p, p^2\}$. But we can remove p from the list since

$$N(z) = N(a + ib) = a^2 + b^2 = p \lightning$$

contradicts the property of p, so wlog $N(z) = 1$ and $N(w) = p^2$. So one of them is a unit which shows that p is irreducible (and prime).

In another example, we look at $K[X]$ for some field K. Then no polynomials of degree 0 is irreducible, for they are the constants. If the degree is 1, then every polynomial is irreducible. If the degree is 2, then it is irreducible if and only if it has no zeros. If the degree is 3, then we can use the same criterion as before. If the degree is 4 however, we could have it as product of two polynomials of degree 2 without zeros so the criterium doesn't work here.

In general, the question of finding irreducible polynomials depends alot on the field we are working with.

3.3 Unique factorisation domain

Definition UFD

An integral domain R is called a **unique factorisation domain** (or factorial 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:

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

Note: Every PID (and thus every euclidean Ring) is a UFD.

Proposition

Let R be a UFD. Then $p \in \setminus\{0\}$ is prime if and only if p is irreducible.

Proof: As with any integral domain, prime implies irreducible. So let p be irreducible. Because R is a UFD, $p = up_1 \dots p_n$, but since p is irreducible, n must be 1, or else p wouldn't be irreducible so $p = up_1$. But becase u is a unit, we have $(p) = (up_1) = (p_1)$ which means that (p) is a prime ideal so p is prime.

Corollary

Let R be an integral domain. Then R is a UFD if and only if every element $a \in R \setminus \{0\}$ can be written as a product of a unit and finitely many irreducible elements and if the ring has the property that irreducible $\implies$ prime.

Definition

Let R be a commutative Ring and $a, b \in R$. We say a and b are **associated** and write $a \sim b$ if there exists a unit $u \in R^\times$ such that $a = ub$

This also induces an equivalence relation. Reflexivity follows by chosing $u = 1$, symmetriy by using $b = u^{-1}a$ and transitivity comes from the product of the units u_1 and u_2.

Lemma

Let R be an integral domain and let p, q be irreducible such that $p|q$. Then $p \sim q$

Proof: Becuase $p = ap$ and because p is irreducible, and q is not a unit, it follows that a is a unit.

Definition

For $n \in \mathbb{N}$ we define the **symmetric** group S_n to be the set of consisting of the bijections

$$S_n := \{\sigma : \{1, \dots, n\} \to \{1, \dots, n\} | \sigma \text{ bijective}\}$$

Theorem Unique factorisation

Let R be a unique factorisation domain. Then the factorisation of every nonzero element a is unique up to permutation of the prime elements. In other words

$$up_1 \dots p_n = a = vq_1 \dots q_m \implies n = m \text{ and } \exists \sigma \in S_n : q_i \sim p_{\sigma(j)} \text{ for all } 1 \leq i \leq n$$

Proof: Let $a = up_1 \dots p_m = vq_1 \dots q_n$ be two prime factoristions.
We use induction on n. If $n = 0$, then $a = v \in R^\times$ and thus also $m = 0$ because if $m > 0$ we would have $p_1 | a$ and $a | 1$ which means that $p_1 | 1$ but then p_1 would be a unit $\lightning$

Since we have $q_n | a$, and q_n is prime, it must divide one of the factors $a = up_1 \dots p_m$. Say $q_n | p_{\sigma(n)}$ which is again prime, so $q_n \sim p_{\sigma(n)}$. Using the induction hypothesis for

$$\frac{a}{q_n} = \underbrace{u \frac{p_{\sigma(n)}}{q_n}}_{\in R^\times} p_1 \dots p_{\sigma(n)-1} p_{\sigma(n)+1} \dots p_m = v = q_1 \dots q_{n-1}$$

It follows that $m - 1 = n - 1$ and there exists a bijection

$$\sigma : \{1, \dots, n-1\} \to \{1, \dots, \sigma(n) - 1, \sigma(n) + 1, \dots, m\}$$

such that $q_j \sim p_{\sigma(j)}$ for $j = 1, \dots, n-1, n$.

Definition

Let R be a UFD. We say $P \subseteq R$ is a **representation set** (of prime elements) if every $p \in P$ is prime and for every prime element $q \in R$ there exists a unique $p \in P$ such that $q \sim p$.

For example, the prime numbers in $\mathbb{Z}$ are $\pm$ the "prime numbers" of $\mathbb{N}$ (which isn't a ring). So for $R = \mathbb{Z}$ the set

$$P = \{p \in \mathbb{Z} | p \text{ prime and positive}\}$$

For $R = K[X]$ we test

$$P = \{f \in K[X] | f \text{ is irreducible and normed}\}$$

This is possible since the units in $K[X]$ are exactly the constant polynomials, so we can always divide out the leading coefficients.

For $R = \mathbb{Z}[i]$ we can set

$$P = \{a + ib \text{ prime in } R, a > 0 \text{ and } -a < b \leq a\}$$

which corresponds to the quarter plane on the right side.

Lemma

Let R be a UFD, then it has a representation set.

Proof: We use the axiom of choice on the set

$$\{[p]_\sim | p \in R \text{ prime}\}$$

If we want the unique factorisation domain, then we want the prime factorisation be unique including the unit u or v, so we have the following theorem

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

$$a = u \prod_{p \in P}' p^{n_p}$$

where n_p is zero for all but finitely many $p \in P$.

Proof: If $a \in R^\times$ we set $u = a$ and $n_p = 0$ for all $p \in P$. Otherwise we just use the property of UFD's that $a = up_1 \dots p_m$ and for every p_j there exists a unique $p_i \sim p \in P$ and we get

$$a = u \frac{p_1 \dots p_n}{\prod_{p \in P} p^{n_p}} \prod_{p \in P} p^{n_p}$$

where n_p is the number of indices i such that $p_i \sim p$.
To show that the factorisation is unique, we assume that

$$a = u \prod_{p \in P} p^{n_p} = v \prod_{p \in P} n^{n'_p}$$

If $n'_p = 0$, for all $p \in P$, then $a = v \in R^\times$ and $n_p = 0$ for all p. Else if $n'_{p_0} > 0$ then p_0 divides a but since there is only one $p \in P$ that is associated to p_0, it follows that $n'_{p_0} = n_{p_0}$.
Using induction on the sum $\sum_{p \in P} n'_p$ the theorem follows.

Lemma

Let R be a UFD and $P \subseteq R$ a representation set. IF $a = u\prod_{p\in P} p^{m_p}$ and $b = v\prod_{p\in P} p^{n_p}$ then a divides b if and only iff $m_p \leq n_p$ for all $p \in P$.

Proof: If $b = ac$ and $c = w\prod_{p\in P} p^{k_p}$. then

$$b = v\prod_{p\in P} p^{n_p} = uw\prod_{p\in P} p^{m_p+k_p}$$

Then $v = uw$ and $n_p = m_p + k_p \geq m_p$.
If $m_p \leq n_p$ we chose our c to be

$$c = vu^{-1}\prod_{p\in P} p^{n_p-m_p} \in R$$

which is well defined, since u is a unit and $n_p - m_p \geq 0$.

Proposition GCD

Let R be a UFD with representation set P. Then for every nonzero pair $(a, b) \neq (0, 0)$ there exists a **greatest common divisor**. If $a = u\prod_{p\in P} p^{m_p}, b = v\prod_{p\in P} p^{n_p}$ then the divisor is given by

$$d = \prod_{p\in P} p^{\min(m_p,n_p)} =: \gcd(a, b)$$

We can show that for any integral domain, the gcd is unique up to a unit.

Proof: We see from the definition that $\gcd(a, b)$ divides both a and b. If we have another divisor of a and b, then its exponents of p must also be smaller than those of a and b and thus smaller than their mimumum.

Analogously we can define the gcd of multiple elements $a_1, \ldots, a_n \in R$ and the above proposition holds aswell.

Definition

Let R be a UFD. We say that $a_1, \ldots a_l \in R$ are **coprime** if $\gcd(a_1, \ldots, a_l) = 1$ or equivalently if for every prime element $p \in R$ there is a a_j such that $p \nmid a_j$.

Corollary

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 $a, b \in R$ coprime.

Proof: Let $x = \frac{\tilde{a}}{\tilde{b}} \in K$ and let $d = \gcd(\tilde{a}, \tilde{b})$. Then set

$$a := \frac{\tilde{a}}{d} \text{ and } b := \frac{\tilde{b}}{d} \implies a, b \text{ coprime}$$

Corollary

Let R be a UFD with quotient field $K = \mathrm{Quot}(R)$. Then every $x \in K$ has a representation of the Form

$$x = u \prod_{p \in P} p^{n_p}, \quad \text{for} \quad n_p \in \mathbb{Z}, n_p \neq 0 \text{ for only finitely many } p \in P$$

Not all rings are UFDs. For example we can look at $R = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{Q}[i\sqrt{5}] \subseteq \mathbb{C}$. And try to see if we can find two different factorisations of the number 6.

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

First of all we can see that all of these factors are irreducible and they are not associated with eachother as the units of this ring are just ± 1.

Dedekind found that this counterexample could be resolved if we looked at at better, idealised prime factors in a better ring.

$$(6) = (2, 1 + i\sqrt{5})^2 (3, 1 + i\sqrt{5})(3, 1 - \sqrt{5})$$

3.4 Examples of euclidean rings

All examples we look at here live in a quadratic field $K = \mathbb{Q}[\sqrt{d}]$ where $d \in \mathbb{Z}$ is not a square number.

$$K = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : |a, b \in \mathbb{Q}\} \simeq \mathbb{Q}[X]/(X^2 - d)$$

We define the **conjugation**

$$\tau : K \to K, \quad a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

which defines a field automorphism on K.
First we prove that the fields $\mathbb{Q}[\sqrt{d}]$ and $\mathbb{Q}[X]/(X^2 - d)$ are indeed isomorphic. We define the evaluation mapping

$$\mathrm{ev}_{\sqrt{d}} : \mathbb{Q}[X] \to K, \quad f \mapsto f(\sqrt{d}), \quad \mathrm{ev}_{\sqrt{d}}(X^2 - d) = 0$$

Since $X^2 - d$ has no roots in $\mathbb{Q}$, it is irreducible/prime in the PID $\mathbb{Q}[X]$. Therefore its principal ideal $(X^2 - d)$ is a maximal ideal. So since $(X^2 = \mathrm{Ker}\,\mathrm{ev}_{\sqrt{d}}$. THe first isomorphism theorem say that

$$\mathbb{Q}[X]/(X^2 - d) = \mathbb{Q}[X]/\,\mathrm{Ker}\,\mathrm{ev}_{\sqrt{d}} \simeq \mathrm{Im}(\mathrm{ev}_{\sqrt{d}}) = \mathbb{Q}[\sqrt{d}]$$

Using this isomorphism we get that the mapping τ can be thought of as the quasi-composition $-\sqrt{d} \circ \sqrt{d}$ of isomorphisms

$$K \overset{\sqrt{d}}{\to} \mathbb{Q}[\sqrt{d}] \simeq \mathbb{Q}[X]/(X^2 - d) \overset{-\sqrt{d}}{\to} K$$
$$\sqrt{d} \mapsto [X]_{\sim_{(X^2-d)}} = X + (X^2 + d) \mapsto -\sqrt{d} + (-d + d) = -\sqrt{d} = \tau(\sqrt{d})$$

So τ is again an isomorphism.

Then we can define a norm on $K = \mathbb{Q}[\sqrt{d}]$.

$$N(z) = N(a + b\sqrt{d}) = z\tau(z) = a^2 - db^2$$

which is multiplicative, since τ is an isomorphism:

$$N(zw) = (zw)\tau(zw) = z\tau(z)w\tau(w) = N(z)N(w)$$

When we loook at the Ring $\mathbb{Z}[\sqrt{d}]$ and we can define the degree using the norm function and obtain the following theorem

Theorem

For $d = -1, -2, 2, 3$ the Ring $R = \mathbb{Z}[\sqrt{d}]$ is a euclidean Ring using the degree function $\varphi(z) := |N(z)|$

Proof: Let $f, g \in R$, with $f \neq 0$. We calculate division in $\mathbb{Q}[\sqrt{d}]$ such that $z = a + b\sqrt{d} = \frac{g}{f} \in \mathbb{Q}[\sqrt{d}]$ and chose the best approximation in $\mathbb{Z}[\sqrt{d}]$:

$$q := [a] + [b]\sqrt{d} \in R$$

Then we have

$$\varphi(z - q) = |N(z - q)| = |(a - [a]^2 - d(b - [b])^2| \leq \frac{1}{4} + \frac{1}{4}d < 1 \quad \text{for } d = -1, -2, 2$$

Even for $d = 3$, since we have a minus in the absolute value, the upper bound holds. If $d = -3$, the above argument would be incorrect.
We define $r = g - fq \in \mathbb{Z}[\sqrt{d}]$ and get that $g = fq + r$ and

$$\varphi(r) = |N(g - fq)| = |N(f)N(z - q)| < |N(f)| = \varphi(f)$$

From this we obtain the following

Lemma

Let $R = \mathbb{Z}[\sqrt{d}]$. Then we have

(a) $u \in R^\times$ if and only if $N(u) = \pm 1$

(b) If $z \in R$ such that its Norm is prime in $\mathbb{Z}$, then z is irreducible (in R).

(c) If $p \in \mathbb{Z}$ is prime, such that neither p nor $-p$ is a Norm of an element in R, then p is irreducible.

Proof:

(a) If $u \in R^\times$ is a unit, then there exists $v \in R^\times$ such that $uv = 1$. Therefore $N(u) \cdot N(v) = N(uv) = 1$. Since $N(u), N(v)$ is an element of $\mathbb{Z}$, it follows that they must be ± 1. If $N(u) = \pm 1$, then $u(\pm\tau(u)) = \pm N(u) = 1$, so it has an inverse $u^{-1} = \pm\tau(u)$.

(b) If $N(z) = p \in \mathbb{Z}$ is prime. From the multiplicativity of the Norm we have that

$$z = ab \implies N(z) = p = N(a)N(b) \implies N(a) = \pm 1 \text{ or } N(b) = \pm$$

From the first part, this means that one of a or b is a unit.

(c) Let $p \in \mathbb{Z}$ be prime, such that p and $-p$ are not norms of numbers. If $p = ab$, then

$$N(p) = p^2 = N(a)N(w) \implies N(a), N(b) \in \{\pm 1, \pm p, \pm p^2\}$$

But since they cant be $\pm p$, of of them must have norm 1 and must be a unit.

Theorem Gaussian Integers

Let $R = \mathbb{Z}[i]$ be the Ring of Gaussian integers. Then R is a euclidean ring and we can look at the representation set

$$P = \{z = a + ib \in R | z \text{ prime and } -a < b \leq a\}$$

whose elements we can categorize as

- $z = 1 + i$ (which divides $2 = -i(1+i)^2$
- (inert)$p \in \mathbb{N}$ prime with $p = 3 \mod 4$ with examples $3, 7, 11, \ldots$
- (split) $z = a \pm bi$ prime in R, such that $a, b \in \mathbb{N}$, $b < a$ and

$$a^2 + b^2 = p = 1 \mod 4 \quad \text{for } p \in \mathbb{N} \text{ prime}$$

  which includes $5, 13, \ldots$

Note: There are infinitely many inert and split primes in R.

To prove this, we need the following lemma:

Lemma

Let $p \in \mathbb{N}$ be prime. Then $(p-1)! = -1 \mod p$

Proof: We have that

$$(p-1)! = \prod_{k=1}^{p-1} k = 1 \cdot (p-1) \prod_{\substack{1<a<b<p-1 \\ ab=1 \mod p}} = -1 \mod p$$

Which is true, since for any $x \in \mathbb{F}_p^\times$

$$x = x^{-1} \iff x^2 = 1 iff (x+1)(x-1) = 0 \iff x = \pm 1$$

Proposition

Let $p \in \mathbb{N}$ such that $p = 1 \mod 4$. Then there are two solutions of the equation $x^2 - 1$ in $\mathbb{F}_p$.

Proof: Define $x = (\frac{p-1}{2})!$ in $\mathbb{F}_p$. Then since $(\frac{p-1}{2})$ is divisble by four, we have

$$\begin{aligned} x^2 &= 1 \cdot 2 \ldots (\frac{p-1}{2}) \cdot (\frac{p-1}{2}) \ldots 2 \cdot 1 \cdot (-1)^{\frac{p-1}{2}} \\ &= 1 \cdot 2 \ldots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \ldots (p-2)(p-1) \\ &= (p-1)! = -1 \in \mathbb{F}_p \end{aligned}$$

Corollary

Let $p \in \mathbb{N}$ be congruent to $1 \mod 4$. Then p is not prime in $\mathbb{Z}[i]$.

Proof: Consider

$$\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1), \quad a+ib+(p) \mapsto a+bX \mod p$$

But since X^2+1 has two roots, it is not irreducible in $\mathbb{F}_p$. Therefore $\mathbb{Z}[i]/(p)$ is not an integral domain and p is not a prime element.
Now we have everything we need to prove the theorem.

Proof theorem: $1+i$ is irreducible, since $N(1+i) = 2$ is prime in $\mathbb{Z}$. Because the ring is euclidean, irreducible also means prime.
Now let $p \in \mathbb{Z}$ be congruent to $3 \mod 4$. Then since for any $a, b \in \mathbb{Z}$ we have $a^2+b^2 \neq 3$ (easy calculation), we have that $p \neq a^2+b^2 \mod 4$.

Therefore p (and $-p$) is not a norm of an element in $R = \mathbb{Z}[i]$ and the lemma shows that it is prime.

If $p \in \mathbb{N}$ is congruent to $1 \mod 4$, then the corollary says it it is not prime in R. Therefore there exists a $z \in R$ such that $N(z) = p$. So we have found a, b such that $p = a^2+b^2$. Since $2 \not| p$ we can assume $b < a$. Then

$$p = (a+ib)(a-ib) \text{ such that} a \pm ib \text{ not associated}$$

, since the angle between them is smaller than 90 degrees.

We now show that the three cases encompass all prime numbers. Let $z \in \mathbb{Z}[i]$ be prime. Thenn since $n = N(z)$ is a natural number. If $p = 2$, then we already know that $2 = (1+i)(1-i)$.
If $p = 3 \mod 4$, and $p | z\tilde{z}$ and p is prime in $\mathbb{Z}[i]$, then $p|z$ or $p|\tilde{z}$.
If $p = 1 \mod 4$. Then we already know that

$$(a+ib)|p|z\tilde{z} \implies (a+ib)|z$$

We sat that the rings $R = \mathbb{Z}[\sqrt{d}]$ for $d \in \{-2, -1, , 2, 3\}$ were euclidean by explicitely writing out the division algorithm. But in the case for $d = -3$, the division algorithm doesnt work anymore, but in the Ring $S = \mathbb{Z}[\frac{1+\sqrt{3}i}{2}]$ it does.
Next we want to compare the prime numbers of $\mathbb{Z}$ with the prime numbers of $\mathbb{Z}[i]$.

Some of the prime numbers of $\mathbb{Z}$ are still prime in $\mathbb{Z}[i]$, but some of them can be factored out. For example we have

$$5 = (2+i)(2-1) \quad \text{and} \quad 13 = (3+2i)(3-2i)$$

3.5 Polynomialrings

Theorem Gauss

If R is a UFD, then $R[X]$ is again a UFD. Further, $R[X]$ has exactly two types of prime elements.

Those with $f = p \in R$ prime and $f \in R[X]$ primitive, such that f is irreducible as Element of $K[X]$.

From iteration, we immediately get the corollary

Corollary

The ring $\mathbb{Z}[X_1, \dots, X_n]$ and for any field K, the ring $K[X_1, \dots, X_n]$ are UFDs.

To prove the theorem, we need the following definition

Definition

Let R are be a UFD and $f \in R[X] \setminus \{0\}$. We call the gcd of the coefficients of f the **content** $I(f)$ of f. We say f is **primitive**, if $I(f) \in R^\times$.

Examples: For $R = \mathbb{Z}$, we have $I(2X + 2) \sim 2$ and $3X + 2$ is primitive.
Note the following:

- Every normed or monic polynomial is primitive.
- If $a \in R \setminus \{0\}, f \in R[X] \setminus \{0\}$ then $I(af) \sim aI(f)$
- If $f \in R[X]$ is irreducible, then either $f \in R$ or f is primitive.
  This is true since if the degree is positive, then $f = af^*$, so either a or $f*$ is a unit. But since the degree of f^* is equal to the degree of f and thus positive, it is not possible that f^* that f is a unit.

Lemma

Let R be a UFD and $K = \mathrm{Quot}(R)$. Then every $f \in K[X]$ has a Representation $f = df^*$, where $d \neq 0 \in K$ and $f^* \in R[X]$ is primitive.
This representation is unique up to associates in R

$$f = d_1 f_1^* = d_2 f_2^* \implies d_1 \sim_R d_2 \wedge f_1^* \sim_R f_2^*$$

Proof: Let $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$. We can write out the a_i as fractions $a_i = \frac{b_i}{c_i}$ for $b_i, c_i \in R, c_i \neq 0$. After multiplying f by all c_i, we can obtain a polynomial with coefficients in R:

$$g := f \prod_{i=0}^n c_i \in R[X]$$

Let $d' \sim I(g)$ an gcd of the coefficients of g. Then $g = d' g^*$ for some $g^* \in R[X]$ primitive. By dividing g^* by the coefficients c_i again, we get that the existence of the representation:

$$f := \underbrace{\frac{d'}{\prod_{i=0}^n c_i}}_{:=d} \underbrace{g^*}_{:=f^*}$$

To show uniqueness assume that $d_1 f_1^* = d_2 f_2^* = f$. We can interpret d_1 and d_2 in R by writing $\frac{d_1}{d_2} = \frac{a_1}{a_2}$ with $a_1, a_2 \in R$ coprime, which gives us

$$f_2^* = \frac{d_1}{d_2} f_1^* = \frac{a_1}{a_2} f_1^* \implies a_1 f_1^* = a_2 f_2^* \implies a_1 \sim I(a_1 f_1^*) \sim I(a_2 f_2^*) \sim a_2$$

This shows that $\frac{d_1}{d_2} \in R^\times$, which means $d_1 \sim_R d_2$ and $f_1^* \sim_R f_2^*$.

This lemma allows us to broaden the definition of content

Definition

For $f \in K[X] \setminus \{0\}$, we call $d \in K \setminus \{0\}$ such that $f = df^*$ for $f^* \in R[X]$ primitve, the **content** of f.

Proposition

Let R be a UFD. For $f, g \in R[X]$ we have $I(fg) \sim I(f)I(g)$. In particular, the product of primitive elements of $R[X]$ is again primitive.

In the following, we will use reduction of the coefficients:

For an element $p \in R$ there exists a Ringhomomorphism

$$f \in R[X] \mapsto f \mod p \in R/(p)[X]$$
$$\sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} (a_i + (p))X^i$$

It follows from section 1.3 that ### missing 2 lines
Proof: Let $f, g \in R[X]$ be primitive polynomials and let $p \in R$ be prime. Since they are primitive, $f \mod p, g \mod p \neq 0$. Further, since $R/(p)$ is an integral Domain, we have that $R/(p)[X]$ is also an integral domain (because the degrees add up). Then since the projection $\mod p$ is a Ring homomorphism, we have

$$(fg) \mod p = f \mod p g \mod p \neq 0$$

In other words, not all coefficients of fg are divisible by p. So since p could be any prime element, we see that fg is primitive.
Now let $f, g \in K[X] \setminus \{0\}$. The previous lemma says that we can write $f = af^*, g = bg^*$ for $a \sim I(f), b \in I(g)$ and f^*, g^* primitive. Then their product $fg = abf^*g^*$ will be such that f^*g^* is also primitive. Since this representation is unique up to association we have $I(fg) \sim_R ab \sim I(f)I(g)$

And as a corollary of Gauss's Theorem we get the following co

Corollary

Let $f \in R[X]$ be primitive. Then f is irreducible in $R[X]$ if and only if it is irreducible in $K[X]$

Proof (Gauss's Theorem): We first show that the two types of prime elements are indeed prime elements of $R[X]$.
Let $p \in R$ be prime. Then using the fact that $\Phi : R[X] \to R/(p)_R[X]$ is a ring homomorphism and that $\operatorname{Ker} \Phi$ is just all polynomials $f \in R[X]$ that whose coefficients are divisible by p, so $\operatorname{Ker} \Phi = (p)_{R[X]}$ we have the Isomorphism

$$R[X]/(p)_{R[X]} \simeq R/(p)_R[X]$$

using the first isomorphism theorem.

Now let $f \in R[X]$ be primitive and be irreducible in $K[X]$. We show that f is prime in $R[X]$. Assume that $f | gh$ in $R[X]$. Observe that this relation also holds in $K[X]$, since f is irreducible in $K[X]$ and because

$K[X]$ is a PID, it is also prime in $K[X]$, so there either $f|g$ or $f|h$ in $K[X]$. So without loss of generalit, we can assume that $f|g$, i.e $g = q \cdot f$.
Because $I(f)$ is a unit, (because $f = af^*$) we have

$$I(q) \sim_R I(q)I(f) \sim_R I(qf) \sim_R \underbrace{I(g)}_{\in R[X]} \in R$$

so also $I(q) \in R$ and because $q \sim I(q)q^*$, and therefore $q \in R[X]$. Therefore $f|g$ in $R[X]$ aswell, so f is indeed prime in $R[X]$. Now we only need to show that all irredcble elements are of these two types.
Since $R[X]$ is a UFD, the prime elements are exactly the irreducible ones in $R[X]$.
So let $f \in R[X]$ be irreducible. If $N(f) = 0$, then $f \in R$ is irreducible and also Prime, because R is assumed to be a UFD.
If $N(f) > 0$, then since f is irreducible, f must also be primitive, or else we would have a factorisation $f = I(f)f^*$, for $I(f) \notin R^\times \lightning$. So f is of the second type.
Now assume that $f = gh$ for some $g, h \in K[X]$ and we show that f can be written as a product of elements in $R[X]$ aswell. From the Lemma we know that $g = cg^*$ and $h = dh^*$, with $c, d \in K$ and $g^*, h^* \in R[X]$ primitve. From the corollary, the product of primitives is again primitve, so $f = (cd)g^*h^*$ is the decomposition of f into primitives and $I(f)$, which means $cd \in R^\times$. Therefore, we can factor $f = (cdg^*)h^*$. And since f is irreducible in $R[X]$, either g^* or h^* must be a unit. So f is irreducible in $K[X]$ aswell.

Now we only need to show that every $f \in R[X] \setminus \{0\}$ is a finite product of prime elements of $R[X]$. Because we can write $f = df^*$ for $d \in R \setminus \{0\}$ and $f^* \in R[X]$ primitive. Since R is a UFD, d is a finite product of prime elements in R.
To show that f^* can also be written as a finite product of prime elements in $R[X]$, we can use induction on the degree $\deg(f^*)$.
If the degree is zero, then $f^* \in R^\times$ and if $\deg(f^*) = 1$, then it is irreducible, since f^* is primitive.
For the induction step if $f^* = gh$ for $g, h \in R[X]$, and f^* is irreducible, then it automatically follows, since one of them is a unit. If f^* is not irreducible, then both g, h are automatically primitive, (or else f^* wouldn't be), and since $\deg(g), \deg(h) < \deg(f)$it follows by induction that they can be written as a finite product of prime elements.

Lemma

Let K be a field and $a \in K$, then for every $f \in K[X]$

$$f(a) = 0 \iff (X - a)|f(X)$$

Proof: By using polynomial division for $f(x)/(X - a)$, then

$$f(X) = (X - a)g(X) + r \quad \text{for} \quad g(X) \in K[X], r \in K$$

Proposition

Let K be a field. Then linear Polynomials of the Form $X - a$ for $a \in K$ are irredicible in $K[X]$. For quadratic and cubic polynomials $f \in K[X]$:

$$f \text{ irreducible} \iff \forall a \in K : f(a) \neq 0$$

Proof: For linear polynomials, it follows directly from the lemma. If $\deg(f) \in \{2,3\}$, and $f = gh$ for some $g, h \notin K[X]^\times$, then $\deg(f) = \deg(g) + \deg(h)$ so at least of g, h is of degree 1. If $\deg(g) = 1$, then g has a root, and $f = gh$ has one aswell.
If f hast a root, then again take the previous lemma.

Fundamental Theorem of Algebra

Every polynomial $f \in \mathbb{C}[X]$ with $\deg(f) > 0$ has a root and the irreducible elements of $\mathbb{C}[X]$ are the linear Polynomials. In particular, every polynomial $f \in \mathbb{C}[X]$ has a linear factorisation

$$f(X) = a \prod_{i=1}^{\deg(f)} (X - z_i)$$

For some $a \in \mathbb{C}^\times$ and $z_i \in \mathbb{C}$

As a corollary, we get the the Fundamental theorem for $K = \mathbb{R}$:
A polynomial in $\mathbb{R}[X]$ is irreducible if and only if $\deg(f) = 1$ or $\deg(f) = 2$ and f has no roots (in $\mathbb{R}$).
Proof: We look at the polynomial as an element in $\mathbb{C}[X]$. Since it has real coefficients, the complex roots come in conjugate pairs $z, \overline{z}$. Then we see that $(X - z)(X - \overline{z}) = (X^2 - (z + \overline{z})X + z\overline{z}) | f(X)$ in $\mathbb{C}[X]$. And since the coefficients $z + \overline{z}, z\overline{z}$ are real, the same also holds in $\mathbb{R}[X]$.

Proposition

Let R be a UFD and $f \in R[X]$ and $\frac{a}{b} \in K = \mathrm{Quot}(R)$ with $b \neq 0$ and a, b coprime. If $f(\frac{a}{b}) = 0$, then b divides the leading coefficient of f and a divides the constant coefficient of f.

Proof: Let $f(\frac{a}{b}) = 0$. Then $(X - \frac{a}{b}) | f(X)$ in $K[X]$, therefore $(bX - a) | f(X)$, but this time in $R[X]$, because if we then write $f(X) = (bX - A)h(x)$ for some $h \in K[X]$, then since the content is multiplicative, and since b and a are coprime we get

$$R \ni I(f) \simeq \underbrace{I(bX - a)}_{\sim 1} I(h) \simeq I(h)$$

Therefore $h(x) \in R[X]$. From this we get that the leading coefficient of f equals b times the leading coefficient of h. And the constant coefficient of f is $-a$ times the constant coefficient of h.

For example, we can ask for which $a \in \mathbb{Z}$ we have that the polynomial

$$f_a(X) := X^2 + aX + 1 \in \mathbb{Z}[X]$$

is irreducible. Using the proposition, we know that the roots must either be $+1$ or -1 or else they wouldn't divide the leading/constant coefficients of f. Then

$$f_a(1) = 0 \iff a = -2 \quad \text{and} \quad f_a(-1) = 0 \iff a = 2$$

so for $a \in \mathbb{Z} \setminus \{\pm 2\}$, $f_a \in \mathbb{Z}[X]$ is irreducible, since it is primitve and has no roots.

For the next example, let K be a field and look at $f(X, Y) = Y^3 - X^5 \in K[X, Y]$. In this case, we can look at the ring $R = K[X]$ and show that it is irreducible in $R[Y]$:

Since f is primitive in $R[Y]$, it is irreducible in $R[Y]$ if and only if f is irreducible in $\text{Quot}(R)[Y] = K(X)[Y]$. If we assume that f is not irreducible in $K(X)[Y]$, then it must have a root in $K(X)$. Now let $p, q \in K(X)$, such that $f(\frac{p}{q}) = 0$. Since $K(X)$ is a field, without loss of generality $q = 1$ and $f(q) = 0$. Then

$$f(y) = Y^3 - X^5 \implies p(X)^3 = X^5 \in K[X]$$

but then since $p(X)|X^5$, we must have

$$p(X) = aX^k \implies p(X)^3 = a^3X^{3k} = X^5 \lightning$$

therefore $f(Y)$ has no roots in $K[X]$, it is irreducible in $K(X)[Y]$ and primitive in $K[X][Y]$ and therefore also irreducible in $K[X][Y] = K[X, Y]$.

Proposition

Let R be a UFD and $p \in R$ prime. If $f \in R[X] \setminus \{0\}$ satisfies

$$f \text{ primitive}, \quad \deg(f) = \deg(f \mod p, \quad f \mod p \in R/(p)[X] \text{ is irreducible}$$

then $f \in R[X]$ is prime.

Proof: Let f satisfy the above conditions and let $g, h \in R[X]$ such that $f = gh$. Then also $f \mod p = g \mod p h \mod p$, and since $f \mod p$ is irreducible in $R/(p)[X]$, we know that either $g \mod p$ or $g \mod p$ is a unit in $R/(p)[X]$. Without loss of generality, we can assume that it is $g \mod p$, so in particular we can write

$$g \equiv a \mod p, \quad \text{for some} \quad a \in R$$

We then can show that $g \mod p$ is of degree zero. Since g modulo p is a constant, then the coefficient of any non-constant term must be divisible by p. But then the leading coefficient of f must also be divisible by p, but that isn't possible since $\deg(f) = \deg(f \mod p$, which wouldn't be true. Therefore $g|I(f)$, but since f is primitive, $I(f) \sim 1$ and therefore $g \in R^\times = R[X]^\times$. Which shows that f irreducible, and since R is a UFD, by Gauss's Theorem $R[X]$ is also a UFD so f is also prime.

Let's test this condition for $f(X) = X^4 + 3X^3 - X^2 + 1 \in \mathbb{Z}[X]$ by showing that for $p = 5$, f satisfies these three conditions. Because its leading coefficient is 1, it is clearly primitive and keeps its degree under mod 5. Here, $R/(p)[X]$ is exactly $\mathbb{F}_5[X]$ so to show that it is irreducible we wil show that $f \mod 5 \in \mathbb{F}_5$ has no linear or quadratic factors. We can rule out the linear factors because $f \mod p \in \mathbb{F}_5$ has no roots:

$$f(0) = 1 \neq 0, \quad f(1) = -1 \neq 0, \quad \dots$$

The quadratic factors can also be ruled out using SageMath[1].
Alternatively we can find out that

$$f \mod 2 = (X+1)(X^3+X+1) \quad \text{and} \quad f \mod 3 = (X^2+1)^2$$

So if $f = gh \in \mathbb{Z}[X]$ were a non-trivial factorisation, for some $g, h \notin \mathbb{Z}[X]^\times$, then the same must be true mod 2 and mod 3. But the calculation mod 2 gives us, that the degree of g is either 1 or 3, whereas the calculation mod 3 need its degree to be 2.

[1]SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more.

Eisenstein-Criterium

Let R be a UFD and $p \in R$ prime. And let $f(X) = \sum_{i=1}^{n} a_i X^i$ be primitive for $n \geq 1$ such that

$$p \not| a_n, \quad p | a_i, \text{ for } 0 \leq i \leq n-1, \quad p^2 \not| a_0$$

then f is prime in $R[X]$.

Proof: Let $f = gh$ be a non-trivial decomposition for $g, h \notin R[X]$. Since f is primitive, also g and h must be primitive. Set $\deg(g) =: k > 0$ and $\deg(h) =: l > 0$ and let's look at $f = gh$ modulo p:

$$f \mod p = a_n \mod p X^n = g \mod p h \mod p$$

Now let's look at this in $K[X] := \mathrm{Quot}(R/(p))[X]$, where $a_n \neq 0$ is a unit and X is a prime factor. We know that

$$g \mod p = bX^{k'}, \quad h \mod p = cX^{l'} \quad \text{for some} \quad k' \leq k, l' \leq l, b \neq 0, c \neq 0$$

But $k' + l' = n$, which is only possible if $k' = k, l' = l$. Therfore$p$ must divide the constant term of both g and h, since p is prime. So looking at $f = gh$ in $R[X]$ again, we see that a_0 is the product of two coefficients, both of which are divisible by p. But that would mean that $p^2 | a_0$, which contradicts the assumtion $\lightning$. Therefore, f is irreducible and since R is a UFD, f is also prime.

For an example we can use the Eisenstein criterium to show that $X^n - 2 \in \mathbb{Z}[X]$ is irreducible for every $n \geq 1$.

Corollary

For every prime number $p \in \mathbb{N}$, the p-th circle divison polynomial

$$\Phi_p(X) = 1 + X + X^2 + \dots X^{p-1} = \frac{X^p - 1}{X - 1}$$

is irreducible in $\mathbb{Z}[X]$

Proof: We use the Eisenstein Criterium for

$$f(Y) = \frac{(Y+1)^p - 1}{Y} = Y^{-1} \left(\sum_{k=0}^{n} \binom{p}{k} Y^k - 1 \right) = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1}$$

We can immediately see that the highest coefficient $k = p$ is normed, since $\binom{p}{p} = 1$, so f is primitive. Further, the other terms, excluding the non constant term are divisible by p, and the constant term is 1, which is not divisible by p^2. By the Eisenstein criterium, $f(Y)$ is irreducible in $\mathbb{Z}[Y]$.
To import this property onto $\mathbb{Z}[X]$ we show that $\mathbb{Z}[Y]$ and $\mathbb{Z}[X]$ ar isomorphic for $X = Y + 1$ using the evalution mapping to define the isomorphisms

$$\Psi(f(Y)) = f(X - 1), \quad \tilde{\Psi}(g(X)) = g(Y + 1)$$

So since $f \in \mathbb{Z}[Y]$ is irreducible and since $\Phi_p(X) = \Psi(f)$, the ciricle division polynomial is also irreducible.

Another application of the Eisenstein Criterium is that we can show that for every $n \geq 1$ the polynomial $X^n + Y^n - Z^n \in \mathbb{C}[X,Y,Z]$ is irreducible, by setting $R = \mathbb{C}[Y,Z]$, and $p = Y - Z \in R$ prime. Then $p | Y^n - Z^n$ since

$$(Y-Z)(Y^{n-1} + Y^{n-2}Z + \ldots + YZ^{n-2} + Z^{n-1}) = Y^n - Z^n$$

and $p^2 \not| Y^n - Z^n$ by showing that $(Y-Z)$ does not divide the right side $(Y^{n-1} + \ldots + Z^{n-1})$.

4 Group Theory

4.1 Definitions and Examples

Definition Group

A **Group** is a set G with an operation $\circ : G \times G \to G$ that satisfies the following axioms.

G1 Associativity: $\forall a,b,c \in G : \quad (a \circ b) \circ b) = a \circ (b \circ c)$

G2 Identity Element: $\exists e \in G : \forall a \in G : e \circ a = a \circ e = a$

G3 Inverse Element: $\forall a \in G \exists x \in G : a \circ x = x \circ a = e$

Note: The inverse element is uniquely determined for every $a \in G$, since for two inverses x, y of a we have by associativity

$$y = (x \circ a) \circ y = x \circ (a \circ y) = x$$

We write a^{-1} for the inverse element. The identity element is also uniquely determined through left identity $\forall a \in G : e \circ a = a$ or idempotency: $e \circ e = e$, since

$$\tilde{e} = \tilde{e} \circ e = e, \quad \text{and} \quad \tilde{e}^{-1} \circ \tilde{e} \circ \tilde{e} = \tilde{e}^{-1} \circ \tilde{e} = e$$

Definition abelian group

Let G be a group. We say that two elements $a, b \in G$ **commute**, if $ab = ba$. If every pair of elements in G commute, we say that G is **abelian**, or **commutative**.

Note: For abelian Groups, we often use additive Notation: $+ : G \to G$ and write 0 for the identity.

Definition powers

For a group G and $a \in G$ and for $k \in \mathbb{Z}$ we define the **powers** of a as

$$a^k := \begin{cases} \underbrace{a \circ \ldots \circ a}_{k-\text{times}} & \text{for } k > 0 \\ e & \text{for } k = 0 \\ \underbrace{a^{-1} \circ \ldots \circ a^{-1}}_{|k|-\text{times}} & \text{for } k < 0 \end{cases}$$

Note: We have the following properties for all $a \in G$:

- $\forall k, l \in \mathbb{Z} : a^k a^l = a^{k+l}$
- $\forall k, l \in \mathbb{Z} : \left(a^k\right)^l = a^{kl}$
- If $a, b \in G$ commute and $k, l \in \mathbb{Z}$, then a^k and b^l commute and $(ab)^k = a^k b^k$

The proof is trivial with induction on k.

Since groups have a inverse operation, we can reduce equations. So for all $a, b, c \in G$ we have

$$ac = bc \iff a = b \iff ca = cb$$

Also the equation $ax = b$ always has a unique solution, $x = a^{-1}b$.

Now let's look at how Group s relate to another.

Definition Homeomorphism

Let G_1, G_2 be two groups. A **homeomorphism** from G_1 to G_2 is a map $\varphi : G_1 \to G_2$ such that

$$\varphi(ab) = \varphi(a)\varphi(b), \forall a, b \in G$$

The **Kernel** and **Image** of the map are the sets

$$\operatorname{Ker}\varphi = \varphi^{-1}\{e_{G_2}\} = \{a \in G_1 | \varphi(a) = e_{G_2}\}$$
$$\operatorname{Im}\varphi = \varphi(G) = \{b \in G_2 | \exists a \in G_1 : \varphi(a) = b\}$$

We can also talk about (smaller) groups inside groups.

Definition subgroup

Let G be a group. A **subgroup** of G is a non-empty subset $H \subseteq G$ such that for any $a, b \in H$ the element ab^{-1} is also in H. We write $H < G$.

The following are equivalent characterisations of subgroups

(a) $H < G$

(b) $e \in H$ and $a, b \in H \implies ab \in H$, $a \in H \implies a^{-1} \in H$.

(c) H is a group and the inclusion mapping $\iota : H \to G, h \mapsto h$ is a Homeomorphism.

If $|H| < \infty$, then it suffices to show that H is non-empty and $a, b \in H \implies ab \in H$.

If $\varphi : G_1 \to G_2$ is a homemorphism, then both $\operatorname{Ker}\varphi$ and $\operatorname{Im}\varphi$ are subgroups of the respective groups.
Examples:

(a) The group of units in a Ring $R^\times$ is a subgroup.

(b) Let M be a non-empty set. Then the set of bijective maps is a group with respect to composition of maps.

$$\operatorname{Bij}(M) := \{f : M \to M | f \text{ bijective}\}$$

For $M = \{1, \dots, n\}$ we write $S_n = \operatorname{Bij}(\{1, \dots, n\}$.

(c) More generally, if M is a set with "some structure", then the set of structure preserving maps $\mathrm{Aut}(M)$ is a group.

$$\mathrm{Aut}(M) := \{\varphi : M \to M | \varphi \text{ bijective and structure preserving}\}$$

Some examples of Automophisms

M with structure	$\mathrm{Aut}(M)$
Set	$\mathrm{Bij}(V)$
K-Vector spaces	$\mathrm{GL}(V)$
$K \supseteq \mathbb{Q}$	$\mathrm{Gal}(K : \mathbb{Q}) = \{\varphi : K \to K | \varphi\ \mathbb{Q}\text{-linear, bijective and } \varphi(ab) = \varphi(a)\varphi(b)\}$
Grp	$\mathrm{Aut}(G) = \{\varphi : G \to G | \varphi \text{ Isomorphism}\}$
Affine real plane	$\mathrm{GL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$
Euclidean real plane	$\mathcal{O}_2(\mathbb{R}) \ltimes \mathbb{R}^2$
Spherical Geometry S^2	$\mathcal{O}_3(\mathbb{R})$
Hyperbolic plane	$\mathcal{SO}_{2,1}, P\,\mathrm{GL}_2(\mathbb{R})$
Top	$\mathrm{Homeo}(X) := \{\varphi : X \to X | \varphi \text{ bijecive, continous, continous inverse}\}$
Man$^\infty$	$\mathrm{Diffeo}(M) = \{\varphi : M \to M | \varphi \text{ smooth bijective, smooth inverse}\}$
Regular polygon in $\mathbb{R}^2$	Diedral Group D_{2n}
Rubik's Cube	Turns on the Rubiks cube

(d) For a field K the set of invertible $n \times n$ matrices $\mathrm{GL}_n(K)$ is a group. Furthermore, the determinant $\det : \mathrm{GL}_n(K) \to K^\times$ is a group homomorphism and $\mathrm{Ker}\det = \mathrm{SL}_n(K)$

(e) $(0, \infty) < \mathbb{R}^\times$ is a subgroup. And $\exp : \mathbb{R} \to \mathbb{R}^\times$ is a homeomorphism.

(f) If G_1, G_2 is a group, then $G_1 \times G_2$ is a group under component wise operation.

Lemma

Let G be a group and $a \in G$, then the map $\varphi : \mathbb{Z} \to G, k \mapsto a^k$ a group homomorphism.

Proof: The power rule already shows that φ is a homoeomorphism. And since $\varphi(nk) = a^{nk} = \left(a^k\right)^n = e \implies nk \in \mathrm{Ker}\,\varphi$ we know that $\mathrm{Ker}\,\varphi$ is an ideal. Since $\mathbb{Z}$ is a PID, either

$$\mathrm{Ker}\,\varphi = (0) \quad \text{or} \quad \mathrm{Ker}\,\varphi = (n_0), n_0 > 0$$

So if the kernel is zero, it is injective.
The mapping φ allows us to define how the cycles of a behave in the group.

Definition order

Let G be a group, and for $a \in G$, write $\varphi_a : \mathbb{Z} \to G, k \mapsto a^k$. If φ_a is injective, we say a has **order** infinty and if $\mathrm{Ker}\,\varphi_a = (n_0)$ for some $n_0 > 0$ then a is of order n_0

4.2 Conjugation

Lemma

Let G be a Group.

(a) For every $g \in G$, the mapping

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

is an Automorphism on G. This is called a **inner Automorphism**.

(b) The mapping $\Phi : g \in G \mapsto \gamma_g \in \mathrm{Aut}(G)$ is a homomorphism. The Kernel of Φ is called the **center**

$$Z_G = \{g \in G | \forall x \in G : gx = xg\}$$

Proof: For $g, x, y \in G$ we have that

$$\gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y)$$

And for $g, h, x \in G$ we have

$$\gamma_g(\gamma_h(x)) = g\gamma_h(x)g^{-1} = ghx^{-1}g^{-1} = ghx(gh)^{-1} = \gamma_{gh}(x)$$

The mapping is bijective, since

$$(\gamma_g \circ \gamma_{g^{-1}})(x) = \gamma_{gg^{-1}}(x) = \gamma_e(x) = \mathrm{id}(x)$$

For b) we already have shown that Φ is a homeomorphism, since $\Phi(gh) = \gamma_{gh} = \gamma_g \circ \gamma_h = \Phi(g)\Phi(h)$ Furthermore, we have

$$\mathrm{Ker}\,\Phi = \{g \in G | \gamma_g = \mathrm{id}\} = \left\{g \in G | gxg^{-1} = x \forall x \in G\right\}$$

And since $gxg^{-1} = x$ if and only if $gx = xg$ the center is indeed Z_G.

Definition

Let G be a group and $g \in G$. The set of Fixpoints of γ_g is the called the **centralizer** of g

$$\mathrm{Cent}_G(g) = \{x \in G | gx = xg\}$$

Definition

Let G be a group and $x, y \in G$. We say that xy are **conjugate**, if there exsts a $g \in G$ such that $\gamma_g(x) = gxg^{-1} = y$

Note: This defines an equivalence relation on G, since

$$\gamma_e(x) = x, \quad \gamma_g(x) = y \implies \gamma_{g^{-1}}(y) = x, \quad \gamma_g(x) = y, \gamma_h(y) = z \implies \gamma_{hg}(x) = z$$

Examples:

(a) For $G = \mathrm{GL}_n(\mathbb{C})$, two matrices A, B are conjugates, if and only if A and B have the same Jordan-Normal Form.

(b) For $G = \mathcal{U}_n(\mathbb{C})$ the group of unitary matrices: $A^H A = AA^H = I$, every $g \in G$ is diagonalizable. Therefore we can represent the conjugation classes through the elements of $\left(S^1\right)^n$ modulo permutation of coordinates.

If our Group is too large to study on its own, we might want to understand the conjugation classes first. The group S_n has $n! \simeq \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ elements. But the number of conjucation classes is much smaller, about $\frac{1}{4\sqrt{3}n} e^{2\pi\sqrt{\frac{n}{6}}}$ (Hardy-Ramanujan 1918).

Examples:

(a) The center of S_n for $n \geq 3$ is $\{1\}$

(b) The center of $\mathrm{GL}_n(K)$ is the set $\{t \cdot I | t \in K^\times\}$

(c) The center o $\mathrm{SL}_n(K)$ is the set $\{t \cdot I | t \in K^\times, t^n = 1\}$

4.3 Subgroups and Generators

Recall that a subset $H \subseteq G$ is called a **subgroup** of G, if for all $a, b \in H : ab^{-1} \in H$.

Definition

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

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

We call X the generating set of $\langle X \rangle$. If $\langle X \rangle = G$, we say that G is **generated** by X. If $\langle X \rangle = \langle g \rangle$ for some $g \in G$, we call it the **cyclic subgroup** generated by g

Note: The generated subgroup can be written as the set of elements

$$\langle X \rangle = \left\{ x_1^{k_1} \dots x_n^{k_n} \middle| n \in \mathbb{N}, x_1, \dots, x_n \in X, k_i \in \{\pm 1\} \right\}$$

Lemma

Let G be a group and $a \in G$. Then $\langle a \rangle \simeq \mathbb{Z}/(n_0)$ for some $n_0 \in \mathbb{N}$.

Proof: we define the Homomorphism $\varphi : n \in \mathbb{Z} \mapsto a^n \in G$, which has Kernel $\operatorname{Ker} \varphi = I = (n_0)$. Then we can write

$$\Phi : \mathbb{Z}/(n_0) \to \langle a \rangle, \quad k + (n_0) \mapsto a^k$$

which is well defined and injective, since

$$k + (n_0) = l + (n_0) \iff k - l \in (n_0) = \operatorname{Ker} \varphi \iff a^{k-l} = e \iff a^k = a^l$$

Example: The symmetric Group S_n is generated by two elements

$$\tau_{1,2} : 1 \mapsto 2, 2 \mapsto 1, n \mapsto n, \quad \text{and} \quad \sigma : n \mapsto n+1$$

Which have order 2 and n respectively. Notice that

$$\sigma\tau_{1,2}\sigma^{-1} : 1 \mapsto n \mapsto n \mapsto 1 \quad 2 \mapsto 1 \mapsto 2 \mapsto 3, \quad 3 \mapsto 2 \mapsto 1 \mapsto 2$$
$$\implies \sigma\tau_{1,2}\sigma^{-1} = \tau_{2,3}$$

By iteration, we can obtain $\tau_{k,k+1}$. Using those we obtain

$$\tau_{i,j} = \tau_{i,i+1}\tau_{i+1,i+2}\dots\tau_{j-1,j}\tau_{j-2,j-1}\dots\tau_{i,i+1}$$

which clearly generates all of S_n.

Unlike Subvectorspaces, there is no good way to define **basis** or **dimension** for a subgroup. But in S_6 there exists a subgroup that is generated by 3 or more elements and no less.

$$\langle H\rangle = \langle \tau_{1,2}, \tau_{3,4}, \tau 5, 6\rangle \simeq \mathbb{F}_2^3$$

Definition

Let G be a group. The **commutator** of $a, b \in G$ is

$$[a, b] := aba^{-1}b^{-1}$$

and the **commutator group** is

$$[G, G] = \langle [a, b], a, b \in G\rangle$$

The commutator group "measures" how un-abelian the group is.

4.4 Quotients

Definition

Let G be a group and $H < G$. We define the two relations on G

$$a \sim_H G \iff b^{-1}a \in H$$
$$a \;{}_H\!\sim b \iff ba^{-1} \in H$$

We call the set $aH := \{ah | h \in H\}$ the **left-subclassses** with left representant a and we also write

$$G/H = aH | a \in G$$

and anlogosly we define the **right-subclasses** Ha and $H \setminus G$

Lemma

Let G be a group and $H < G$. Then $\sim_H$ defines an equivalence relation on G and G/H is the Quotient of G with respect to $\sim_h$ and $[a]_{\sim_H} = aH$.

Proof: We have reflexivity since $a^{-1}a = e \in H$. Symmetry since $b^{-1}a \in H \implies (b^{-1}a)^{-1} = a^{-1}b \in H$. And transivity because

$$b^{-1}a, c^{-1}b \in H \implies c^{-1}bb^{-1}a = c^{-1}a \in H$$

Furthermore

$$[a]_{\sim_H} = \{b | b \sim_H a\} = \{b | b^{-1}a \in H\} = aH$$

For example let $G = S_3$ and set $H =< \tau_{12} >= \{e, \tau_{12}\}$. Then for some cyclic $\sigma \in S_3$ the left and right subclasses are not equal: $\sigma H \neq H\sigma$

Definition

The **cardinaliy** of G is also called the **order** of G. And the cardinality of G/H is also called the **index** $[G : H]$ of H in G.

Theorem

Let G be a group and $H < G$. Then

(a) The groups G/H and $H \setminus G$ have equal cardinality.

(b) Lagrange: If $|G| < \infty$, then $|G| = |G/H| \cdot |H|$

Proof: We define the mappings

$$\varphi : G/H \to H \setminus G, \quad aH \mapsto (aH)^{-1} = Ha^{-1}$$
$$\psi : H \setminus G \to G/H, \quad Ha \mapsto (Ha)^{-1} = a^{-1}H$$

These mappings are inverse, i.e. $\psi \circ \varphi = \mathrm{id}_{G/H}$ and $\varphi \circ \psi = \mathrm{id}_{H \setminus G}$

To show Lagrange's Theorem we chose from every left subclass aH for $a \in G$ one left representant $x \in aH$ and we call the set of lef representants X. Then $|G/H| = |X|$. Furthermore we can show that the mapping

$$\Psi : X \times H \to G, \quad (x, h) \mapsto xh$$

is bijective. Surjectivity holds since for any $g \in G$, $gH \in G/H$. and from construction of X there is one $x \in X$ such that $x \in gH$. In particular, there exists an $h \in H$ such that $g = xh = \Psi(x, h)$.
Injectivity follows from the fact that the equivalence classes are mutually disojoint: Let (x_1, h_1) and (x_2, h_2) such that they get mapped to the same element. Then

$$\Psi(x_1, h_1) = \Psi(x_2, h_2) \iff x_1h_1 = x_2h_2 \implies x_1H = x_2H \implies x_1 \sim_h x_2$$

But since we only chose one representant of each equivalence class, we have $x_1 = x_2$. From this, it follows that

$$|G| = |X \times H| = |X| \cdot |H| = |G/H| \cdot |H|$$

Corollary

Let G be a finite group and $g \in G$. Then the order of an element $g \in G$, divides $|G|$.

Proof: Let $m := |G|$ and $n := |< g >|$ be the order of g. Then $n|m$ from Lagrange's theorem. Let $k = \frac{m}{n}$, then

$$g^{|G|} = g^m = g^{nk} = (g^n)^k = e^k = e$$

Corollary

In $\mathbb{F}_p = \mathbb{Z}/(p)$. Then

$$a^{p-1} = \begin{cases} 0 & \text{for } a = 0 \\ 1 & \text{for } a \in \mathbb{F}_p^\times \end{cases}$$

Proof: The Group $G = \mathbb{F}_p^\times$ has order $p - 1$.

Corollary First classification of groups

Let G be a finite group and $|G| = p \in \mathbb{N}$ prime. Then G is isomorphic to $\mathbb{Z}/(p)$

Proof: Let $g \in G \backslash \{e\}$. Then $n = |< g >| > 1$ and divides p. Since p is prime, $n = p$, which means $< g >= G$.

In general, the subsets G/H and $H \setminus G$ are not groups.

Definition

Let G be a group and $H < G$. IfG/H is a group such that the projection $\pi : G \to G/H$, $\pi(g) = gH$ is a group homomorphism, we say H is **normal** in G or is a **normal divosor** of G and we write $H \lhd G$ and we call G/H the **factor group** of G modulo H.
We say that G **simple**, if only $\{e\}$ and G itself are the only normal divisors of G.

Theorem

Let G be a group and $H < G$. Then the following are equivalent:

(a) $xH = hX$ for all $x \in G$

(b) $xHx^{-1} = H$ for all $x \in G$

(c) There exists a group G_1 and a group homomorphism $\varphi : G \to G_1$ such that $H = \operatorname{Ker} \varphi$

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

(e) $H \lhd G$

Proof: Missing:
For example an abalien group is simple if and only if $G \simeq \mathbb{Z}/(p)$ for a prime $p \in \mathbb{N}$.
On S_n, the sign is a homomorphism: $\text{sgn} : S_n \to \{\pm 1\}$, whose kernel is called the **alternating group** A_n, which is non-abelian for $n \geq 5$

First Isomorphism Theorem

Let $\varphi : G \to H$ be a homomorphism for two groups G, H. Then φ induces an Isomorhpism $\overline{\varphi} : G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$ 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.

Proof: We show that $\overline{\varphi}(x\operatorname{Ker}\varphi) = \varphi(x)$ on $G|_{\operatorname{Ker}\varphi}$ is well defined and injective:
Missing 30 mins.

Corollary Second Isomorphism Theorem

Let G e a group and $H \lhd G$ and $K < G$. Then

$$KH = HK < G, \quad H \lhd KH, \quad H \cap K \lhd K, \quad \text{and} \quad K/(H \cap K) \simeq KH/H$$

Proof: For $k \in K$ we have $kH = Hk$. By taking the union of all k we know $KH = HK$. If $k_1, k_2 \in K$ and $h_1, h_2 \in H$, then

$$\begin{aligned} (k_1h_1)(k_2h_2) \in KHKH = HKKH = HKH = KHH = KH \\ (k_1h_1)^{-1} = h_1^{-1}k_1^{-1} \in HK = KH \end{aligned}$$

which shows that $KH < G$ is a subgroup. Furthermore, since $H < KH$ and for any $x \in KH \subseteq G$ we know that ### Missing 10 ins

Corollary Third Isomorphism Theorem

Let G be a group, $H \lhd G, K \lhd G$ and $K < H$. Then

$$H/K \lhd G/K \quad \text{and} \quad (G/K)/(H/K) \simeq G/H \quad \text{where} \quad (xK)(H/K) \simeq xH$$

Proof: Since $K \subseteq H$ we can define the mapping

$$\varphi : G/H \to G/H, \quad gK \mapsto gH$$

Since the group structures of G/K and G/H are defined by multiplication wit the representant, we also know that φ is a Group homomorphism:

$$\varphi\left((g_1K)(g_2K)\right) = \varphi\left((g_1g_2)K\right) = (g_1g_2)H = \varphi(g_1K)\varphi(g_2K).$$

φ is also surjective because ### Therefore

$$(G/K)\operatorname{Ker}\varphi \simeq G/H \quad \text{and} \quad \operatorname{Ker}\varphi = \{gK | gH = eH\} = \{hK | h \in H\} = H/K$$

Corollary Modulus-Hom Adjunction

Let G be a group and $H \lhd G$. For any other Group K there exists a natural isomorphism

$$\mathrm{Hom}(G/H, K) \simeq \{\varphi \in \mathrm{Hom}(G, K) | \varphi|_H \equiv e_K\}$$

Corollary

Let G be a group and $H \lhd G$. Then the following mappins are in inverse relation to eachother:

$$(K < G \text{ with } H < K) \mapsto K/H < G/H$$

Proof: Exercise
Examples:

- $C_n \lhd D_{2n}$ since rotations are in C_n and a reflection will be conjugated to a rotation: $TRT^{-1} = R^{-1} \in C_n$ nd every subgroup $H < C_n$ is also a normal divisor of D_{2n}
- The center Z_G and the commutator grop $[G, G]$ are always normal.
- The affine group $G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in K^\times, b \in K\}$ for a field K.

$$H_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in K \right\} \lhd G$$
$$H_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} | a \in K^\times \right\} < G$$

- Exercise: Let G be a group and $H < G$ with index 2. Then $H \lhd G$
- Exercise: classify/describe all groups of order $\leq 7, 8, 10$

4.5 Group actions

We noticed that many groups can be understood not just through the group itself, but how other objects “transform”. In this section, we will learn how to better understand groups by studying how groups can “act” on other objects.

Definition

Let G be a group and T a set. A **Group action** (or **left action**) of G on T is a morphism

$$\cdot : G \times T \to T, \quad (g, t) \mapsto g \cdot t$$

such that for any $t \in T, g_1, g_2 \in G$

$$e \cdot t = t \quad \text{and} \quad g_1 \cdot (g_2 \cdot t) = (g_1 g_2) \cdot t$$

In this case we call T a G-Set

Note: The definition is equivalent to the following:
There exists a group homormophism

$$\alpha : G \to \mathrm{Bij}(T), \quad g \mapsto \alpha g, \quad \text{where} \quad \alpha_g(t) = g \cdot t$$

Example

- Let T be a set and G a group, then we have the trivial group action $g \cdot t = t$
- The group $G = S_n$ can be though of as *acting* on $T = \{1, \dots, n\}$ with $\sigma \cdot t = \sigma(t)$.
- $G = \mathrm{GL}(V)$ can act on a vector space V through $A \cdot v = Av$ for $A \in \mathrm{GL}(V)$ and $v \in V$
- Let G be a group and $H < G$. We can define $T = G/H$ and

  $$g \cdot (xH) = gxH \text{ for } g \in G, xH \in G/H$$

  We can also define a group action on $H \setminus G$ but this time with $g \cdot (Hx) = HXg^{-1}$
- For a group G, se can set $T = G$ and see conjugation as a group action

  $$g \cdot x = gxg^{-1}, \text{ for } g \in G, x \in T = G$$

- Let G be a group and set $T = \mathcal{P}(G)$ as the power set. Define the group action

  $$g \cdot A = gA = \{ga | a \in A\}$$

- For a group G and T the set of subgroups of G, $T = \{H < G\}$ define

  $$g \cdot H = gHg^{-1}$$

  which is well-defined.

Definition

Let G be a set and T a G-set.

- We say $S \subseteq T$ is **invariant**, if $g \cdot S = S$ for all $g \in G$
- $t_0 \in T$ is called a **fixpoint** of the group action, if $g \cdot t_0 = t_0$ for all $g \in G$. We denote the set of all fixpoints as

  $$\mathrm{Fix}_G(T) = \{t_0 \in T | t_0 \text{ is fixpoint}\}$$

- For $t_0 \in T$ we call the the set

  $$G \cdot t_0 = \{g_0 \cdot t | g \in G\}$$

  the G-**(orbit)** of t_0.
- For $t_0 \in T$, the **stabilizer** of t_0 is the subset

  $$\mathrm{Stab}_G(t_0) = \{g \in G | g \cdot t_0 = t_0\}$$

  which can be shown to be a subgroup of G
- If the mapping $\alpha : g \in G \mapsto \alpha_g \in \mathrm{Bij}(T)$ is injective, we call the group action **faithful**.

- We call the group action **transitive**, if for every pair $t_1, t_2 \in G$ there exists a $g \in G$ such that $g \cdot t_1 = t_2$.
- Wa transitive group action is called **sharply transitive**, if such a g is uniquely determined.
- The set of G-orbits is written as

$$G \setminus T = \{G \cdot t_0 | t_0 \in T\}$$

Lemma

Let G be a group and T a G-set. Then the relation

$$t_1 \sim_G t_2 \iff \exists g \in G \text{ such that } g \cdot t_1 = t_2$$

is an equivalence relation. The orbits are exactly the equivalence classes and $G/\sim_G = G \setminus T$ is the quotient space

Proof: Reflexivity follos from using $g = e$. Symmetry follows by taking the inverse g:

$$t_1 \sim t_2 \iff \exists g \in G : g \cdot t_1 t_2 \implies t_1 = e \cdot t_1 = (g^{-1}g)t_1 = g^{-1} \cdot (g \cdot t_1)) = g^{-1} \cdot t_2$$

For transitivity, there exist $g_1, g_2 \in G$ such that $g_1 \cdot t_1 = t_2$ and $g_2 \cdot t_2 = t_3$. Then

$$(g_2 g_1) \cdot t_1 = g_2 \cdot (g_1 \cdot t_1) = g_2 \cdot t_2 = t_3$$

Definition

Let G be a group and T_1, T_2 two G-sets. A ***G*-Morphism** from T_1 to T_2 is a mapping $f : T_1 \to T_2$ that respects the group actions:

$$f(g \cdot t) = g \cdot f(t), \quad \forall g \in G, t \in T_1$$

We further say f is a G-Isomorphism, if f is also bijective.

Theorem

Let G be a group and T a G-set, $t_0 \in T, T_0 = G \cdot t_0$ and $H = \mathrm{Stab}_G(t_0)$. Then $H < G$, T_0 is invariant and the mapping

$$f : G/H \to T_0, \quad gH \mapsto g \cdot t_0$$

is a (well-defined) G-isomorphism. So the orbit is isomorph to the the modulo group of the stabilisator.

Proof: Let $h_1, h_2 \in H$. Then

$$(h_1 h_2) \cdot t_0 = h_1 \cdot (h_2 \cdot t_0) = h_1 \cdot t_0 = t_0 \quad \text{and} \quad h_1^{-1} \cdot t_0 = t_0$$

since also $e \in H$, it is non empty so $H < G$. Now let $g \in G$ and $g' \cdot t_0 \in T_0 = G \cdot t_0$. T_0 is invariant since

$$g \cdot (g' \cdot t_0) = (gg') \cdot t_0 \in T_0 = G \cdot T_0$$

If $g_1, g_2 \in G$. Then

$$g_1 \cdot t_0 = g_2 \cdot t_0 \iff (g_2^{-1} g_1) \cdot t_0 = t_0 \iff g_2^{-1} g_1 \in H \iff g_1 H = g_2 H$$

Reading it from right to left show that f is well-defined and from left to right shows that f is injective. Surjectivity is also true, since

$$T_0 = G \cdot t_0 = f(G) = \operatorname{Im} f$$

Now let $g_1, g_2 \in G$ then f is a G-Morphism, since

$$f(g_1 \cdot (g_2 H)) f(g_1 g_2) H) = (g_1 g_2) \cdot t_0 = g_1 (g_2 \cdot t_0) = g_1 f(g_2 H)$$

Corollary

Let G be a group and T a G-set. If $|G| < \infty$, then

$$|G| = |G \cdot t_0| \cdot |\operatorname{Stab}_G(t_0)|$$

Proof: It follows from the theorem, that $G \cdot t_0 \simeq G/\operatorname{Stab}_G(t_0)$ therefore, using Lagrange's theorem, the formula holds.

Corollary

Let G be a group and T a finite G-set. Then

$$|T| = |\operatorname{Fix}_G(T)| + \sum_{|G \cdot t| > 1} [G : \operatorname{Stab}_G(t)]$$

Proof: We know that the orbits form a partition on G. So

$$T = \bigsqcup_{\text{Orbits}} G \cdot t = \operatorname{Fix}_G(T) \sqcup \bigsqcup_{\text{non-trivial orbits}} G \cdot t$$

Cayley's Theorem

Let G be a finite group. Then G is isomorphic to a subgroup of the symmetric group S_n for some $n \in \mathbb{N}$

Proof: Set $T = G$ and use group multiplication for the group action. This is equivalent to a Homomorphism

$$\alpha : G \to \operatorname{Bij}(G), \quad g_1 \mapsto \alpha g_1 : (g_2 \mapsto g_1 g_2)$$

α is injective, because its kernel is given by

$$\operatorname{Ker} \alpha = \{g \in G | \alpha_g = \operatorname{id}\} \subseteq \{g \in G | ge = e\} = \{e\}$$

From the first isomorphism theorem, $\operatorname{Im}(\alpha) < \operatorname{Bij}(G) \simeq S_n$, for $n = |G|$.

Note the following

(a) If $H < G$ has finite index, $[G : H]$, there exists a Homomorphism $\alpha : G \to S_n$ for $n = [G : H]$ and $\operatorname{Ker} \alpha < H$.

4.6 Nilpotent and resolvable groups

Definition

Let G be a group. We say G is **nilpotent** of **order** 1, if G is abelian.
We say G is nilpotent of order $n+1$ for $n \geq 1 \in \mathbb{N}$ if G/Z_G is nilpotent of order n.

Let R be a ring. The Heisenberg group

$$H_R = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} | a, b, c \in R \right\}$$

is nilpotent of order 2. We can show that

$$Z_{H_R} = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} | b \in R \right\}$$

and $H_R/Z_{H_R} \simeq R^2$

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 $k \in \mathbb{N}$

Lemma Fixpoints of p-groups

Let $p \in \mathbb{N}$ be prime and G be a p-Group and T be a G-set. Then

$$|\text{Fix}_G(T)| \equiv |T| \mod p$$

Proof: From the corollary on the cardinality of T, we know that

$$|T| = |\text{Fix}_G(T)| + \sum_{\text{non-trivial Orbits}} [G : \text{Stab}_G(t)$$

and since $|G| = p^k$. For non-trivial orbits we know $[G : \text{Stab}_G(t)] = p^l$ for some $l \geq 1$, if t is not a fixpoint. Therefore, p must divide the sum.

Theorem

Every p-Group is nilpotent.

Proof: We set $T = G$ and use konjugation to make G a G-set. Then

$$\text{Fix}_G(T) = \left\{ t \in G | gtg^{-1} = t \right\} Z_G$$

From the lemma above, we konw

$$|\text{Fix}_G(T)| = |Z_G| \equiv |G| = p^k = 0 \mod p$$

Since $e \in Z_G$, we know that $|Z_G| \geq 1$, but since $|G| = |Z_G| \geq p$, the center is non-trivial dn G/Z_G is a smaller p-Group. We can use induction on $|G|$ to show that G/Z_G is nilpotent. Further, if $|G| = p$, $G = Z_G$ is nilpotent and of order 1.

Corollary

Let $p \in \mathbb{N}$ be prime and G a p-Group of order $|G| = p^2$. Then G is abelian.

Proof: From the theorem, we know that Z_G is non-trivial. If $Z_G = G$, it is clearly abelian. If that is not the case, then $|Z_G| = p$. Then G/Z_G is of order p. Therefore there exists a $g \in G$ such that

$$G/Z_G =< gZ_G >= \{g^{kZ_G}\big|^{k=0,\ldots,p-1}\}$$

So we can also write G as being

$$G = \left\{g^k z | k = 0, \ldots p-1, z \in Z_G\right\}$$

but then for $g^{k_1}z, g^{k_2}z_2 \in G$ we have that

$$g^{k-1}z_1 g^{k_2}z_2 = g^{k_1+k_2}z_1 z_2 = g^{k_2}z_2 g^{k_1}z_1$$

which contradictions our assumption $Z_G \neq G$.

Definition

Let G be a group. A **subnormal series** in G is a chain of subgroups, such that

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

such that every Subgroup is normal in the next one.

Definition

Let G be a group. We say G is **resolvable**, if there exsits a subnormal series in G such that G_{k+1}/G_k is an abelian Group for $k = 0, \ldots, n-1$.

Examples:

(a) The dihedral group D_{2n} is resolvable

(b) THe affine group $A_k = \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in R^\times, b \in R\right\}$ is resolvable and is not nilpotent if $|R^\times| > 1$.

Proposition

Let G be a group. Then $[G,G] = \langle\{[a,b] | a,b \in G\}\rangle \lhd G$ and $G/[G,G]$ is abelian.
If H is an abelian Group and $\varphi : G \to H$ is a group homomorphism, then $\varphi([G,G]) = \{e_H\}$ and φ induces a Group homomrophism $\overline{\varphi} : G/[G,G] \to H$ such that the following diagram commutes.

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

In this sense, $G/[G,G]$ is the largest abelian factor group.

Proof: Since $[G, G]$ is a characteristic subgroup (invariant under automorphisms) it is also invariant under conjugation and thus a normal subgroup of G.
Let $a, b \in G$. Then

$$[a[G, G], b[G, G]] = [a, b][G, G] = [G, G]$$

but that just means that $a[G, G]$ and $b[G, G]$ commute in $G/[G, G]$. Now let H be abelian and $\varphi : G \to H$ a homomorphism. For $a, b \in G$ we have

$$\varphi([a, b]) = [\varphi(a), \varphi(b)] = e_H \implies \varphi([G, G]) = \{e_H\}$$

from a corollary of the first isomorphism theorem, the diagram commutes.

Proposition

Let G be a group. Then G is resolvable if and only if the following inductively defined higher commutator groups reach the trivial subgroup $\{e\}$:

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

Proof: If there exists some n, such that $G^{(n+1)} = \{e\}$, then we obtain the following subnormal series

$$\{e\} = \lhd G^{(n+1)} \lhd G^{(n)} \lhd \ldots \lhd G^{(1)} \lhd G^{(0)}$$

From the proposition before, the quotients are abelian each. So G is resolvable.
Now if G is resolvable and the chain is a subnormal series, then the factor groups $G^{(k)}/G^{(k+1)}$ are abelian, so for each k

$$[G^{(k)}, G^{(k)}] = G^{(k+1)} < G^{(k)},$$

Using induction on n, it follows that $G^{(n)} < G_0 = \{e\}$

4.7 Sylow's Theorem

Recall that Lagrange's theorem wsays that for any subgroup $H < G$ both it's order $|H|$ and index $[G : H]$ are divisors of $|G|$.

Lemma

Let $p \in \mathbb{N}$, prime, $n = p^k m$ with (m, p) coprime. Then $\binom{n}{p^k}$ is not divisible by p.

Proof: Set $S := \mathbb{Z}/(p^k) \times \{1, \ldots, m\}$, $G = \mathbb{Z}/(p^k)$ and define a group action from G to S by addition in the first component $(g \cdot (a, j) = (a + g, j))$
Note that the G-orbits in S are of the Form $G \times \{i\}$ for some fixed $i \in \{1, \ldots, m\}$. We then define

$$T := \left\{A \subseteq S \middle| |A| = p^k\right\}$$

Then let define a G action on T with $g \cdot A = \{g \cdot (a, j) \big| (a, j) \in A\}$

Since G is a p-group. We know from the lemma on the cardinality of T that

$$\binom{n}{p^k} = |T| = |\mathrm{Fix}_G(T)|$$

We know the cardiniality of $\mathrm{Fix}_G(T)$ because

$$A \in \mathrm{Fix}_G(T) \iff A \subseteq S, |A| = p^k, g \cdot A = A \forall g \in G$$

which is then the case if A is a union of G-orbits in S. We know how the Orbits look, so there are exactly m of those.

$$\binom{n}{p^k} = |T| = |\mathrm{Fix}| = m$$

and $m \not| p$.

Example: Let $G = \mathrm{SL}_2(\mathbb{F}_p)$ of order $p(p^2-1)$. Then $H_p = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} | a \in \mathbb{F}_p \right\} \simeq \mathbb{F}_p$ is a Sylow p-subgroup.

Sylow's Theorem

Let G be a finite group, $p \in \mathbb{N}$ prime and $n = |G| = p^k m$ for some $k \geq 1$ and (m, p) coprime.

(a) There exists a maximal p-subgroup H_p with $|H_p| = p^k$, which we call **Sylow p-subgroups**.

(b) If $H < G$ is a p-subgroup, there exists a p-Sylow subgroup H_p with $H < H_p$

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

Proof:

(a) Let $T = \left\{ A \subseteq G : ||A| = p^k \right\}$. Then T is a G-set with left multiplikation. From the lemma it follows that $|T| = \binom{n}{p^k} \neq 0 \mod p$. From the corollary on the Orbits and stabilizers, we know that

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

If $n = p^k$, $H_p = G$ is itself a Sylow p-subgroup. Else if $p^k < n$. There doesn't exist a G-invariant subset $A \subseteq G$ with $|A| = p^k$. Since we $gA \in \{\{e\}, G\}$. So there are are no fixpoints of the group action.

Since $|T| \neq 0 \mod p$ the formula on the cardinality says that there exists at least an $A_0 \in T$ such that $[G : \mathrm{Stab}_G(A_0)] \neq 0 \mod p$.

We want to show that $H_o := \mathrm{Stab}_G(A_0)$ is a Sylow p-subgroup with $|H_p| = p^k$. Since

$$|G| = |H_p| \cdot [G : H_p] = p^k m \quad \text{and} \quad p \not|[G \cdot H_p]$$

it must follow that $p^k||H_p|$ from the definition of th stabilizer, $H_p \cdot A_0 = A_0$.

This just means that for $a_0 \in A_0$ and $h \in H_p$ we have $h \cdot a_0 \in A_0$. So $|H_p| = |H_p \cdot a_0| \leq |A_0|$. But from the way we set A_0 its cardinality was p^k. So we have

$$p^k||H_p| \leq p^k \implies |H_p| = p^k$$

(b) Let H be a p-subgroup and H_p be a Sylow p-subgroup. We define $T = T/H_p$ and let H act on T with left multiplication. From the lemma on fixpoints we know that

$$|\mathrm{Fix}_H(T)| = |T| = [G : H_p] = \frac{n}{p^k} = m \neq 0 \mod p$$

In particular there exists a Fixpoint $gH_p \in T$ such that

$$hgH_p = gH_p \implies hg \in gH_p \implies h \in gH_pg^{-1} \implies H < gH_pg^{-1}$$

which shows that gH_pg^{-1} is a Sylow p-subgroup.

(c) Let H, H_p be two Sylow p-subgroups. Then from (b) we know that there exist a $g \in G$ such that $H < gH_pg^{-1}$. Therefore

$$|H| = |H_p| = p^k \implies H = gH_pg^{-1}$$

4.8 Symmetric and Alternating Groups

Theorem

Let $n \geq 1$. We call the elements of $S_n = \mathrm{Bij}(\{1, \ldots, n\})$ **permutations**.
On S_n there exists a Homeomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$ which maps every permuation a sign, where $\mathrm{sgn}(\tau_{ij}) = -1$, for $i \neq j$.
We say $\mathrm{sgn} \in S_n$ is called **even**, if $\mathrm{sgn}(\sigma) = 1$ and **odd**, if $\mathrm{sgn}(\sigma) = -1$.

Proof: see Lineare algebra. We can also prove this by looking at $F \in \mathbb{Z}[X_1, \ldots, X_n]$ and then defining $F^\sigma = F(X_{\sigma(1)}, \ldots X_{\sigma(n)})$ which defines a group action from S_n to $\mathbb{Z}[X_1, \ldots, X_n]$.
Then define $P = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ and we see that

$$P^\sigma = \prod_{1 \leq i < j \leq} (X_{\sigma(i)} - X_{\sigma(j)}) = \mathrm{sgn}(\sigma)P$$

which can be used as a definition of sgn.
Notation: For $\sigma \in S_n$ we often write σ in the following way

$$\sigma =: \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Or we can use the better notation using cycles, where we first find out the first non-fixpoint i_1 of σ. Then look at the sequence

$$\sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{k_1}(i_1) = i_1$$

If these are all non-fixpoints, then we write

$$\sigma = \left(i_1, \sigma(i_1), \sigma^2(i_1), \ldots \sigma^{k_1-1}(i_1)\right)$$

If there are more, then let $i_2 > i_1$ the next non-fixpoint, etc. Then we write

$$\sigma = \left(i_1, \sigma(i_1), \sigma^2(i_1), \ldots \sigma^{k_1-1}(i_1)\right) \left(i_2, \sigma(i_1), \ldots \sigma^{k_2-1}(i_2)\right) \ldots \left(i_r, \sigma(i_r), \ldots \sigma^{k_r-1}(i_r)\right)$$

In this case we also say that σ has cylcestructure $k_1, k_2, \ldots k_r$. (We may also chang the order of the k_i.)

Proposition

Two permuatations are conjuagates in S_n if and only if they have the same cycle structure.1

Proof: See page 122: let $\sigma \in S_n$ and $(i_1, \dots, i_k)$ a cycle. Then

$$\sigma\ (i_1, \dots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \dots \sigma(i_k))$$

Theorem

For $n \le 4$, A_n and S_n are resolvable and A_n is simple for $n \ge 5$

Proof: For $n = 1, 2, 3$ we trivally have

$$A_1 \simeq A_2 \simeq \{e\} \quad \text{and} \quad A_3 \simeq \mathbb{Z}/(3) \text{ is abelian}$$

For $n = 4$ we look at the subgroup

$$V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

wher every non-trivial Element has order 2. It follows that $V_4 \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. And since V_4 contains all the elements of cycletype $2, 2$ we have a subnormal sequence $V_4 \lhd A_4$, which shows that A_4 is resolvable. For $n \ge 5$ we look at a group action on $\{1, \dots, n\}$ with the following Lemma

Lemma

Let $g \ge 3$, then the Group action of A_n to $\{1, \dots, n\}$ is transitive

Proof: This follows directly from the fact that the orit of 1 is $\{1, \dots, n\}$, since

$$(1, 2, 3) : 1 \mapsto 2, \quad (1, i, 2) : 1 \mapsto i$$

Lemma

Let $n \ge 5$ and $H \lhd A_n$ nontrivial. Then H contains a permutation $\sigma \ne e$ with at least one fixpoint.

Proof: Let $\sigma \in H$ and $\tau \in A_n$. Then the commutator of them is in H, since $[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in H$. Let σ be non-trivial. If it has a fixed points, we're done. If it has none, then we can find a $\sigma' \in H$ that has a fixed point. We consider the following cases

- σ Has a cycle $(i_1, i_2, i_3, \dots i_k)$ of length $k \ge 4$. Then we can chose $\tau = (i_1, i_2, i_3) \in A_n$ and $\sigma' = [\tau, \sigma]$. Then

  $$\sigma' = (i_1, i_2, i_3)\sigma(i_1, i_2, i_3)^{-1}\sigma^{-1}$$

  which maps

  $$i_1 \mapsto i_k \mapsto i_k \mapsto i_2 \quad \text{and} \quad i_3 \mapsto i_2 \mapsto i_1 \mapsto i_2 \mapsto i_3$$

  which shows that it is non-trivial and has a fixpoint.

- σ has cycles of length 2 and 3. Then $\sigma' = \sigma^2$ has cycles of length 3 and fixpoints.
- If σ only has cycles $(i_1, i_2, i_3), (i_4, i_5, i_6), \ldots$ of length 3, then chose $\tau = (i_1, i_2, i_4)$ and $\sigma' = [\tau, \sigma]$, which maps

  $$i_1 \mapsto i_3 \mapsto i_3 \mapsto i_1 \mapsto i_2 \quad \text{and} \quad i_6 \mapsto i_5 \mapsto i_5 \mapsto i_6 \mapsto i_6$$

  which shows non-triviality and the existence of a fxpoint.
- σ only has cycles $(i_1, i_2), (i_3, i_4), (i_5, i_6), \ldots$, of which there are at least 3, since $n \geq 5$. Then chose $\tau = (i_1, i_2, i_3)$ and $\sigma' = [\tau, \sigma]$, which maps

  $$i_1 \mapsto i_2 \mapsto i_3 \mapsto i_1 \mapsto i_2, \quad \text{and} \quad i_5 \mapsto i_6 \mapsto i_6 \mapsto i_5 \mapsto i_5$$

which show all possible cases for σ.
Now we can prove that A_5 is simple:
Let $H \lhd A_5$ be nontrivial and $\sigma \in H \setminus \{e\}$ the permutation with a fixpoint from the lemma. In particular, σ cannot be a 5-cycle (or it would have no fixed points) and it since $\sigma \in H$ it also cannot have 4-cycles (### why?)
So it must either have cycletype 3 or $2, 2$. If $\sigma = (i_1, i_2)(i_3, i_4)$, then chose $\tau(i_1, i_2, i_5)$, then

$$\tau\sigma\tau^{-1} = (i_2, i_5)(i_3, i_4) \quad \text{and} \sigma\tau\sigma\tau^{-1} = (i_1, i_2)(i_3, i - 4)(i_2, i_5)(i_3, i_4) = (i_1, i_2, i_5) \in H$$

So H also contains a 3 cycle.
We then show that all 3-cycles in A_5 are conjugates, which means that H must contain all 3-cycles.
Let $\sigma = (i_1, i_2, i_3)$ then define τ as

$$1 \mapsto i_1, \quad 2 \mapsto i_2, \quad 3 \mapsto i_3, \quad 4 \mapsto x, 5 \mapsto y$$

By swapping x and y, we can always assume that $\tau \in A_n$. Then

$$\tau(1, 2, 3)\tau^1 = (i_1, i_2, i_3)$$

which shows that indeed all 3 cycles are conjugates and thus from the previous calculation are in H.
Then we know that

$$(i_1, i_2, i_3)(i_3, i_4, i_5) = (i_1, i_2, i_3, i_4, i_5) \in H \implies H = A_5$$

which shows that A_5 is simple.
For $n > 5$ we use induction on n. Let $H \lhd A_n$ and $\sigma \in H \setminus \{e\}$ have a fixpoint.
We can assume without loss of generality, that $\sigma(n) = n$ is the fixpoint. From the induction step we can write $\{e\} \neq H \cap A_{n-1} = A_{n-1} \lhd A_{n_1}$ From the first lemma, we know that every Element of A_n with a fixpoint is conjugate to an element of A_{n-1}.
This shows that H contains every element with a fixpoint. Then take any $\sigma \in A_n$.

- If σ has a fixpoint, it is in H. If
- If a cycle τ of σ has odd length $< k$, then $\tau^{-1}\sigma$ in the cycle, so adding τ again, which obvously has fixed points outside of τ,

  $$\sigma = \tau(\tau^{-1}\sigma) \text{ has a fixpoint}$$

  which shows $\sigma \in H$

- If n is odd and $\sigma = (i_1, \dots, i_n)$ we can write
$$(i_1, \dots i_{n-2})(i_{n-2}, i_{n-1}, i_n) \in H$$
where the first term is in H because of induction and the second term is a 3-cycle so is in H.
- If σ has a cycle $(i_1, \dots, i_{2k})$ of even length $2k \geq 4$, then using induction on the following decomposition
$$\sigma = ((i_1, \dots, i_{2k-2}) \dots) (i_{2k-2}, i_{2k-1}, i_{2k}) \in H$$
shows $\sigma \in H$
- If σ only has 2-cycles, we know from $n \geq 6$ and $\sigma \in A_n$ that $n \geq 8$, and we can write σ as a product of an element of A_n of cycle type $2, 2$ and another element of H with fixpoints.

This shows that $H = A_n$ which shows that A_n is simple.

4.9 Classification of groups of small order

Theorem

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

For this theorem we use a colletion of previously known lemmas with higher and higher complexity. Recall that we call a group G resolvable if it as a subnormal series
$$\{e\} = G_0 \lhd G_1 \lhd \dots \lhd G_k = G$$
where the factor groups G_j/G_{j-1} are all abelian.

Proposition

Let G be a group and $N \lhd G$. If N and G/N are resolvable, then so is G

Proof: Since they are resolvable, we have subnormal series
$$\{e\} = G_0 \lhd G_1 \lhd \dots \lhd G_l = N$$
$$\{eN\} = H_0 \lhd H_1 \lhd \dots \lhd H_m = G/N$$
with abelian factorgroups. Let $\pi : G \to G/N$ be the canonical projection. Then define
$$G'_j := \pi^{-1}(H_i) < G \implies G_l = N = \pi^{-1}(eN) = G'_0 < G'_1 < \dots G'_m = G$$
We want to show that the sequence
$$G_0 < G_1 < \dots < G_l = N = G'_0 < \dots G'_m = G$$
is subnormal.
Let $h \in G'_{j-1}, g \in G'_j$. Then because $H_{j-1} \lhd H_j$ we know that
$$\begin{aligned} \pi(h) \in H_{j-1}, \pi(g) \in H_j &\implies \pi(g)\pi(h)\pi(g)^{-1} && \in H_{j-1} \\ &\implies \pi(ghg^{-1}) \in H_{j-1} \\ &\implies ghg^{-1} \in \pi^{-1}(H_{j-1}) = G'_{j-1} \end{aligned}$$

which shows $G'_{j-1} \lhd G'_j$. To show that the factor groups are abelian, we use the third isomorphism theorem to show that

$$G'_j \big/ G'_{j-1} \simeq {}^{G'_j/N} \big/ {}_{G'_{j-1}/N} = {}^{\pi(G'_j)} \big/ {}_{\pi(G'_{j-1})} = H_j \big/ H_{j-1}$$

Which shows that G is resolvable.
From the exercise problems we know the following

- A Group G with $a^2 = e$ for all $a \in G$ is abelian and thus resolvable.
- A subgroup with Index 2 is normal.
- All groups of order ≤ 10 are resolvable.
- All groups or order $p \in \mathbb{N}$ prime are cyclic, abelian and thus resolvable.
- All Groups of order p^2 are abelian and resolvable.
- All p-Groups for $p \in \mathbb{N}$ prime $(|G| = p^k)$ are niltpotent and thus resolvable.

The questions is: how far can we go with this?

Missing first 45 minutes

4.10 Free Groups and Relations

Definition

Let $n \geq 1$

Theorem

Let $n \geq 1$ and $b_1, \dots, b_n$ be pairwise disjoint. THen there exists a free group F_n generated by $b_1, \dots, b_n$ with the universal property:
For every group G with elements $a_1, \dots, a_n \in G$ there exists a unique group homomorphism

$$\Phi : F_n \to G \quad \text{with} \quad \varphi(b_j) = a_j, \quad \forall 1, \dots n$$

We prove this by finding F_n. The construction is as follows

$$F_n = \left\{ \text{reduced words in } b_1, b_1^{-1}, \dots, b_n, b_n^{-1} \right\}$$

where a finite list with entries $b_1^{\pm 1}, \dots, b_n^{\pm 1}$ is called a word.
A word w is called **reduced**, if we never have to immediate entries b_i, b_i^{-1} that cancel eachother out.
Then we can find a group structure on F_n in the following way:
For $w_1, w_2 \in F_n$ we define the group operation as concatenation of the words $w_1 \circ w_2$ with cancellation if neccessary (i.e. if w_1 ends in b_1 and w_2 starts with b_1^{-1}.
The universal property follows by defining ### missing 5 mins

Definition Relations

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

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

be the Normaldivisor of F_n generated by W.
Then ${}^{F_n}\!/_{N}$ is called the group with generators $b_1, \ldots, b_n$ and relations $w \in W$ and is written as

$$\langle b_1, \ldots, b_n | w = e \text{ for} w \in W \rangle$$

Examples:

(a) $\mathbb{Z}^2 \cong \langle a, b | ab = ba \rangle$

(b) $D_6 \cong \langle D, R | D^3 = R^2 = e, RDR = D^{-1} \rangle$

5 Modules

Modules are to Rings what Vector spaces are to Field

5.1 Definitions and Examples

Definition

Let R be a Ring. An R-module M is an abelian Group with a scalar multiplication

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

missing ### 5 mins

Definition

Let R be a Ring and M, N be R-modules. We say $\Phi : M \to N$ is R-linear (or Module morphism over R), if Φ is a group homomorphism and

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

Definition Submodule

missing ### 1 min

Lemma

Let R be a ring, M an R-module and $N < M$ a submodule. Denn the Module structure on M induces a module strucutre on ${}^{M}\!/_{N}$ ### missing 2 mins

Proof trivial
Examples:

(a) If $R = K$ is a field, a module is just a vector space.

(b) If M, N are R-modules, then we the Hom-set

$$\mathrm{Hom}_R(M, N) := \#\#\# missing 1 min$$

(c) If $R = \mathbb{Z}$, then every abelian Group M is also a $\mathbb{Z}$-module with the usual additive/multiplicative notation. This means that if we can classify ### missing 1 min

Proposition First Isomorphism Theorem

Let R be a Ring and M, N be R-modules with $\Phi : M \to N$ linear. Then

$$\operatorname{Ker} \Phi < M \quad \text{and} \quad \operatorname{Im} \Phi < N$$

are submodules and Φ induces an Ismorphism

$$\overline{\Phi} : {}^{M}\!/_{\operatorname{Ker} \Phi} \to \operatorname{Im} \Phi$$

Lemma

Let R be a ring and $M_1, \ldots, M_n$ be R-modules. Then $M_1 \times \cdots \times M_n$ is again an R-module with coordinatewise scalar multiplication

Proof: trivial

Lemma

Let R, S be Rings and M be an R-module. Then ### missing 5 mins

Proof: missing
What sort of rings can be Interseting? ## missing 5 mins

Theorem

Let K be field and M a vector space over K. The definition of a module strucutre on M over $K[X]$ is equivalent to chosing a K-linear mapping $\varphi : M \to M$.
If we have a scalar multiplication $\cdot : K[X] \times M \to M$, whose restriction on $K \times M$ is compatible with the given scalar multiplication $\cdot : K \times M \to M$, then we can get a K-linear map given by

$$\varphi : M \to M, \quad \varphi(m) = X \cdot$$

On the other hand, such a linear map φ induces a scalar mulitplication

$$\cdot : K[X] \times M \to M : \quad f \cdot m = (f(\varphi))(m) = \left(\sum_k a_k \varphi^k\right)(m) \quad \text{for} \quad f = \sum_k a_k X^k \in K[X]$$

The way we converted $\cdot$ to φ and back is inverse to how we converted φ to $\cdot$ Proof:
If $\cdot : K[X] \times M \to M$ defines a module strucutre on M over $K[X]$, then $\varphi(m) = X \cdot m$ defines a K-linear mapping on M since

###missing calculation 8 min

On the other hand, if $\varphi : M \to M$ is K-linear, then we the scalar multiplication as defined in the theorem is a Ring homomorphism. This also follows the module axioms.
Now we want to classify Modules over PIDs.
missing ### 8 mins

5.2 Free Modules

Definition

Let I be a set and R a ring. We call

$$R^{(I)} := \{x : I \to R | x_i = 0, \text{for all but finitely many } i \in I\}$$

the **free R-Module** (over I). We call

$$e_i = \mathbb{1}_{\{i\}}, \quad \text{for } i \in I$$

the **standard basis** of $R^{(I)}$. A free module M is a module isomorphic to $R^{(i)}$ for a set.
The cardinality of I is called the **rank** of $M \cong R^{(I)}$.

Lemma

Let $R \neq \{0\}$ ba ring. Then the rank of a module over R is well-defined.

Proof: Let $J_{\max} \subseteq R$. a maximal ideal. For the existence we need Zorn's Lemma.
Let M be a free R-Module. Then

$$J_{\max} \cdot M = \left\{ \sum_k a_k m_k | a_k \in J_{\max}, m_k \in M \right\}$$

is a submodule. Now let I be a set such that $M \cong R^{(I)}$. Then

$$J_{\max} \cdot M \text{ is mapped to } \left\{ \sum_{i \in I} a_i e_i : | a_i \in J_{\max}, a_i = 0 \text{ for all but finitely many } i \in I \right\}$$

Then we can look at the quotient

$$M \big/ J_{\max} \cdot M \cong \left(R \big/ J_{\max} \right)^{(I)}$$

which is a vector space over $R \big/ J_{\max}$ of dimension $|I|$. Using the proof that the dimension of vector spaces is well-defined, the proof follows.
Note: Free modules behave very much like vector spaces.

Proposition

Let $m, n \geq 1$ be natural numbers and R a Ring. Then

$$\mathrm{Hom}(R^n, R^m) \cong \mathrm{Mat}_{mn}(R)$$

Proof: just like in linear algebra, we can use the standard basis.

Definition

Let M be an R-module. We say $x_1, \ldots, x_n \in M$ are **free** or **linearly independent**, if the mapping

$$a \in R^n \mapsto \sum_{i=1}^{n} a_i x_i$$

is injective. If $x_1, \ldots, x_n \in M$ are linearly independent, the image of the mapping above is a free submodule of M.

5.3 Torsion modules

Definition

Let R be a Ring and M and R-module. We say $m \in M$ is a **torsion element** of M, if there exists an $a \in R \setminus \{0\}$ such that $a \cdot m = 0$.

We say M is a **torsion module**, if every $m \in M$ is a torsion element.

We say M is **torsion-free** if $m = 0$ is the only torsion element of M.

Exampels:

(a) If we set $R = \mathbb{Z}$ and $M = G$ an additively closed finite group, then M is a torsion module. Just chose $a = \mathrm{ord}(g)$ for $g \in G$

(b) Let $R = \mathbb{Z}$. Then $M = {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}}$ is a torsion module. We have to multiply by the denominator.

(c) Let V be a finite dimensional vector space over a field k and $A : V \to V$ linear. We use A to make V to a $K[X]$-module. Then V is a torsion module over $K[X]$, since the mapping

$$f \in K[X] \mapsto f \cdot v \in V$$

can't be injective. In particular, if we chose f to be the characteristic polynomial of A, then $f \cdot v = 0$

(d) If R is an integral domain and M is a free module, then M is torsion free.

5.4 Structure of finitely generated modules over PIDs

Definition

Let R be a ring and M an R-module. For a subset $X \subseteq M$ we call

$$< X >_R := \left\{ \sum_{x \in E} a_x x | a_x \in R, \text{ for } x \in E \text{ and } E \subseteq X \text{ finite} \right\}$$

the R-linear **shell** of X or the submodule **generated** by X. If there exists a finite subset $X \subseteq M$ such that $M =< X >_R$, we call M **finitely generated**

Example: For $R = K[X_1, \dots,]$ the submodule $I =< X_1, x_2, \dots >$ is not finitely generated.
From now on we will look at PIDs.

Classification theorem (First part)

Let R be a PID and M a finitely generated module over R. Then M is isomorphic to a direct product

$$M \cong R^n \times T, \quad \text{where} \quad T = M_{\text{tors}} = \{m \in M | m \text{ is torsion element of } M\}$$

and n is the rank of ${}^{M}\!/\!_{M_{\text{tors}}}$
In particular, M is a free module if and only if $M_{\text{tors}} = \{0\}$

Proposition

Let R be a PID and $n \geq 1$. Then every submodule $M \subseteq R^n$ is a free R-module with rank $\leq n$

Proof: Let e_i for $i = 1, \dots, n$ be the standard basis for R^n. We define the submodules

$$M_i = M \cap < e_1, e_2, \dots, e_i >$$

Using induction on i we can show that M_i is a free module of rank $\leq i$.
For $i = 1$ we trivially have $M_1 = M \cap < e_1 > \simeq J \subseteq R$. And because R is a PID, either $J = \{0\}$ or $J = (d_1)$ with rank 1.
If we assume that M_{i-1} is free with rank $\leq i - 1$, then we can look at the mapping

$$\Phi : M_i \to R, \quad (x_1, \dots x_i, 0, \dots, 0) \mapsto x_i$$

Since $\operatorname{Im} \Phi$ is a submodule of R, it follows that either $\operatorname{Im} \Phi = \{0\}$ and $M_i = M_{i-1}$ with rank $\leq i - 1$ or $\operatorname{Im} \Phi = (d_i)$, so $m_i \in M_i$ and $\Phi(m_i) d_i$.
In this case we define

$$\Psi : M_{i-1} \times R \to M_i$$

which is an isomorphism and shows that M_i is free and is of rank $\leq i$
Now we can prove the first part of the classification theorem.

- M_{tors} is a submodule. (We take the product of the $a_1, a_2 \neq 0$)
- Since R is an integral domain, a free module has no torsion elements, because if $x_1, \dots, x_n \in M$ are generators of M, then we take a maximal linearly indepenedent subset $y_1, \dots, y_k \in M$. Then

$$N =< y_1, \dots, y_k > \cong R^k$$

It can be shown that for all x_i in the generating set there exsts an $a_i \in R \setminus \{0\}$ such that $a_i x_i \in N$. If $x_i = y_j$ then just thake $a_i = 1$. On the other hand, if $x_i \neq y_j$ for all j, then we can look at the mapping

$$\varphi : R \times N \to M, \quad (a, m) \mapsto a x_i + m$$

which can't be injective because if $\operatorname{Im} \varphi$ were free, with rank $k+1$, then $y_1, \ldots, y_k$ wouldn't be maximal.

So there would exist som $(a, m) < neq 0$ such that $a x_i + m = 0$. If $a = 0$, then m would also be 0. This means that

$$a + 0, \text{ and } a x_i \in N$$

From this we can show that for $a = a_1 a_2 \ldots a_n$ it follow that $aM \subseteq N \cong R^k$. So aM is isomorpic to a submodule of R^k and is free. Further, $a\cdot : M \to aM$ is an isomorphism, because

$$\operatorname{Ker}(a\cdot) = \{m \in M | am = 0\} \subseteq M_{\text{tors}} = \{0\}$$

so M is free.

This shows the equivalence

$$M \text{ free} \iff M_{\text{tors}} = \{0\}$$

Now let M be a finitely generated R-module. Then $M' := {}^{M}\!/\!_{M_{\text{tors}}}$ is also finitely generated and torsion free.
Ten let $m + M_{\text{tors}} \in M'$ be a torsionelement, and $a \in R \setminus \{0\}$ such that

$$a(m + M_{\text{tors}}) = 0 + M_{\text{tors}}$$

but that would mean that $am \in M_{\text{tors}}$, so there would be a $b \in R \setminus \{0\}$ such that $bam = 0$, which would mean

$$(ab) \cdot m = 0 \implies m \in M_{\text{tors}} \implies (m + M_{\text{tors}}) = 0 + M_{\text{tors}} \in M'$$

which shows that M' is torsion-free. Therefore ${}^{M}\!/\!_{M_{\text{tors}}} \cong R^n$ is a free module.
Now assume $x_1 + M_{\text{tors}}, \ldots, x_n + M_{\text{tors}}$ are free generators of ${}^{M}\!/\!_{M_{\text{tors}}}$. Then also $x_1, \ldots, x_n$ are free (in M) because

$$\sum_{i=1}^{n} a_i x_i = 0 \in M \implies \sum_{i=1}^{n} a_i (x_i + M_{\text{tors}}) = 0$$

We define the mapping

$$\Psi :\in R^n \times M_{\text{tors}} \to M \quad , (a, m') \mapsto \sum_{i=1}^{n} a_i x_i + m' \in M$$

and show that it is an isormorphism. It is injective since it's kernel is zero:

$$\Psi(a, m') = \sum_{i=0}^{n} a_i x_i + m' = 0 \implies \sum_{i=1}^{n} a_i (x_i + M_{\text{tors}}) \implies a = 0, m' = 0$$

to show surjectivity, let $m \in M$. Then there exists an $a \in R^n$ such that

$$m + M_{\text{tors}} = \sum_{i=1}^{n}$$

missing 2 mins

Classification theorem (second part)

Let R be a PID and M_{tors} a finitely generated torsion module. Then there exist $d_1|d_2|\dots|d_n \in R\setminus\{0\}$ such that

$$M_{\text{tors}} \cong R/(d_1) \times \dots \times R/(d_n)$$

alternatively, we can write

$$M_{\text{tors}} \cong \prod_{j=1}^{k} M_{\text{tors}}^{(p_i)}$$

where $p_1,\dots,p_k \in R$ are non-conjugate primes in R and

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

Smith Canonical Form

Let R be a PID, $k,n \geq 1 \in \mathbb{N}$ and $A \in \text{Mat}_{kl}(R)$. Then there exist $g \in \text{GL}_k(R)$ and $h \in \text{GL}_l(R)$ such that

$$gAh^{-1} = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_n & \\ & & & 0 \\ & & & & \ddots \end{pmatrix}, \quad \text{for} \quad d_1|d_2|\dots|d_n \in R\setminus\{0\}$$

We will prove this theorem only for euclidean rings. In the Gaussian elimination algorithm, row operations are left-multiplication with elements of $\text{GL}_k(R)$ and column operations coorrespond with right-multiplication with elements of $\text{GL}_l(R)$

Proof for euclidean rings: We will use induction on $\max(k,l)$.

If $\max(k,l) = 1$, either $A = (0)$ or $A = (d_1)$ for some $d_1 \in R\setminus\{0\}$.

Now let $\max(k,l) \geq 2$. If $A = 0$, we're done. Let

$$N := \min_{A_i j \neq 0} \varphi(a_{ij}) \in \mathbb{N} \quad \text{for} \quad \varphi \text{ the norm on } R$$

By swapping rows and columns we can assume that

$$d_1 = A_{11} \neq 0 \quad \text{and} \quad \varphi(d_1) = N$$

then use division with rest to get

$$A_{1j} = a_j d_1 + r_1 \quad \text{for} \quad j = 2,\dots l \quad \text{and} \quad r_i = 0 \quad \text{or} \quad \varphi(r_i) < \varphi(d_1)$$

and subtract a_j time hte first row of the j-th row for $j = 2,\dots,l$ and we obtain the matrix

$$A' = \begin{pmatrix} d_1 & r_1 & \dots & r_l \\ A_{21} & & & \\ \vdots & & & \\ A_{k1} & & & \end{pmatrix}$$

If $r_i \neq 0$, then $N' = \min_{A'_{ij}} \varphi(A'_{ij}) < N$ and w can use Induction to let A' have Smith normalform. Therefore without loss of generality, $r_2 = r_3 = \ldots = r_l = 0$
Analogously we can repeat this argument for the first column to get a matrix

$$A'' = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & & & \\ \ldots & & & \\ 0 & & & \end{pmatrix}$$

If $\max(k, l) = 1$, then A'' is already in smith normalform. Else the submatrix of A'' has dimension $k-1, l-1$. So the maximum decreases and induction step gives us a matrix of the form

$$A''' = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_n & \\ & & & 0_{\ddots} \end{pmatrix}$$

now we have to show that $d_1|d_2|\ldots|d_n$. If $d_1|d_2$ then smith normalform is reached.
If $d_1 \not| d_2$, then we can add the second row to the first and make division with rest and get a matrix of smaller norm to get

$$A''' \mapsto \begin{pmatrix} d_1 & & 0 \\ 0 & d_2 & \\ & & d_{3_{\ddots}} \end{pmatrix} \mapsto \begin{pmatrix} d_1 & r & 0 \\ 0 & d_2 & \\ & & 0 \end{pmatrix} \mapsto A''' \text{ in Smith canonical form.}$$

Now we can prove the second classification theorem.
Let M be a finitely generated module and R a euclidean ring. If we assume $x_1, \ldots, x_k \in M$ generate M, then

$$\Phi : a \in R^k \mapsto \sum_{i=1}^{k} a_i x_i \in M$$

is surjective. Then $N = \operatorname{Ker} \Phi \subseteq R^k$ is a submodule and also a free module itself from a previous proposition. Write $N = < r1, \ldots, r_l >$, so $M \cong R^k \diagup N$.
We define the Matrix

$$A = (r_1, \ldots, r_k) \in \operatorname{Mat}_{kl}(R)$$

and put it in Smith canonical form, so there exist $g \in \operatorname{GL}_k(R), h \in \operatorname{GL}_l(r)$ such that

$$B := gAh^{-1} = \begin{pmatrix} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_{n_{\ddots}} & \\ & & & 0 \end{pmatrix} \quad \text{with} \quad d_1|d_2|\ldots|d_n \in R \setminus \{0\}$$

Since A can be identified with a linear map $R^l \to R^k$, we get that

$$N = \operatorname{Im} A = A(R^l), \quad \text{and} \quad \operatorname{Im} B = B(R^k) = gAh^{-1}(R^l) = g \operatorname{Im} A = gN$$

then let's take a look at what g does to R^k:

$$R^k \xrightarrow{g} R^k, N = \operatorname{Im} A \mapsto gN = \operatorname{Im} B$$

which induces an isomorphism (First isomorphism theorem)

$$M \cong R^m / N \to R^k / gN = R^k / \operatorname{Im} B$$

but since B is diagonal, we know that

$$\operatorname{Im} B = (d_1) \times (d_2) \times \ldots \times (d_n) \times \{0\}^{k-n}$$

so we can extend the isomorphism

$$M \cong R^k / \operatorname{Im} B \cong R/(d_1) \times R/(d_2) \times \ldots \times R/(d_n) \times R^{k-n}$$

which is a decomposition in to a torsion and a free part.

5.5 Finitely generated abelian gruops

Theorem

Let G be a finitely generated abelian group. Then

$$G \cong Z/(d_1) \times \ldots \times \mathbb{Z}/(d_n) \times \mathbb{Z}^k$$

where $1 \leq d_1 | d_1 | \ldots | d_n \neq 0$ and $k \geq 0$. Alternatively we can write

$$G \cong \prod_{p \text{prime}} G_p \times \mathbb{Z}^k \quad \text{for} \quad G_p \cong \mathbb{Z}/(p^{k_{p,1}} \times \ldots \times \mathbb{Z}/(p^{k_{p,n}}$$

This follows directly from the classification theorem because abelian groups are $\mathbb{Z}$-modules.

5.6 Jordan canonical form

Theorem

Let V be a finite-dimensional $\mathbb{C}$-vector space and $\varphi : V \to V$ linear. Then there exists a basis of V such that φ has a matrix representation in jordan canonical form.

Proof: Since V is finite-dimensional and $\mathbb{C}[X]$ is infinitely dimension, V must be a torsion-module over $\mathbb{C}[X]$. Further more, V is a finitely generated $\mathbb{C}[X]$-module. Using the classification theorem for modules, we get that

$$V \cong \prod_{(\lambda,k)} \mathbb{C}[X] / ((X-\lambda)^k)$$

where we used the fundamental theorem of Algebra, to show that the only irreducible elements in $\mathbb{C}[X]$ are of the form $(X - \lambda)$.

We then can describe multiplication with X as aplication of φ to subspaces on V on $M = {}^{\mathbb{C}[X]}\diagup_{((X-\lambda)^k)}$. Which has the basis

$$1, (X-\lambda), (X-\lambda)^2, \dots, (X-\lambda)^{k_1}$$

over $\mathbb{C}$ and so multiplication with X has the following matrix representation with respect to this basis

$$\begin{pmatrix} \lambda & 0 & & & 0 \\ 1 & \lambda & 0 & & \\ 0 & 1 & \ddots & & \\ \vdots & & & & \\ 0 & & 1 & \lambda & \end{pmatrix}$$

6 Field Theory

6.1 Field Extensions

Note: A ring homomorphism between two fields is always injective because it's kernel is always an ideal and there are only two ideals of a field K. K itself and $(0) = \{0\}$

Definition

Let L be a field an $K \subseteq L$ a subring that is also a field. We then say K is a **subfield** of L and we call L a **field-extension** of K.
We also write L/K if L is a field-extension of K, since L can be thought of as a vector space over K. We call the dimension of the vector space L/K the **degree** and denote it with $[L : K]$. If $[L : K] < \infty$, we say L is a **finite** field-extension of K.

Examples

(a) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

(b) $\mathbb{C}/\mathbb{R}$

(c) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \cong {}^{\mathbb{Q}[T]}\diagup_{(T^3-2)}/\mathbb{Q}$

Lemma Multiplicity of degree

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

$$[F : K] = [F : L] \cdot [L : k]$$

Proof: Let $m = [F : L]$ and assume $x_1, \dots, x_m \in F$ are a basis of F over L. Also let $n = [L : K]$ and $y_1, \dots, y_n \in L$ are a basis of L over K. Then we can show that the products

$$x_i y_j \in F, \quad \text{for} \quad i = 1, \dots m, j = 1, \dots n$$

are a basis of F over K.

To show linear independence, let $\alpha_{ij} \in K$ and $\sum_{i,j} \alpha_{ij} x_i y_j = 0$. But because $x_1, \dots, x_m$ are linearly independent over L

$$\sum_{i=1}^{m} \underbrace{\sum_{j=1}^{n} \alpha_{ij} y_i}_{\in L} x_i = 0 \implies \sum_{j=1}^{n} \alpha_{ij} y_j = 0 \implies \alpha_{ij} = 0, \forall i, j$$

which shows that $x_i y_j$ are linearly independent.
To show that they span F, let $z \in F$. Then there exist $\beta_1, \dots, \beta_m \in L$ such that $z = \sum_{i=1}^{m} \beta_i x_i$. And because y_i are a basis of L, for each $\beta_i \in L$ there exist $\alpha_{i1}, \dots, \alpha_{in} \in K$ such that

$$\beta_i = \sum_{j=1}^{n} \alpha_{ij} y_j \implies z = \sum_{i,j} \alpha_{ij} x_i y_j$$

Definition

Let L/K be a field extension and $x \in L$ and

$$\varphi_x : K[T] \to L, \quad f \mapsto f(x)$$

the evaluation mapping.

- If φ_x is injective, we say x is **transcendent** over K
- If φ_x is not injective, we say that x is **algebraic**. In this case $\operatorname{Ker} \varphi_x = (m_x(T))$ is an ideal and we call $m_x(T)$ the **Minimal polynomial** of x and the degree of $m_x(T)$ also the degree of x.

Note that the definition for algebraic is equivalent to saying that $x \in L$ is a root of a polynoial with coefficients in K.
Examples

(a) $e, \pi \in \mathbb{R}$ are transcendent over $\mathbb{Q}$

(b) $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $T^3 - 2$

(c) $\cos(20°) \in \mathbb{R}$ is algebraic because

$$\cos(3\varphi) = \cos^3(\varphi) - 3\cos\varphi \sin^2\varphi = \cos^3\varphi - 3\cos\varphi + 3\cos^3\varphi$$

so for $\varphi = 20°$ we know that

$$\cos(60°)\frac{1}{2} = 4\cos^3\varphi - 3\cos\varphi$$

with minimal polynomial $4T^3 - 3T - \frac{1}{2} \in \mathbb{Q}[T]$

Proposition

Let L/K and $x \in L$. If x is transcendent, then

$$K[X] = \operatorname{Im}\varphi_x \cong L[T]$$

and the smallest subfield $K(x)$ of L tht contains K and x satisfies

$$K(x) \cong K(T)$$

If x is algebraic, then

$$K[X] = \operatorname{Im} \varphi_x \cong L[T]/(m_x(T))$$

is already the smallest subring $K(x)$ that contains K aswell as x. Then also

$$[K(x) : K] = \deg m_x(T)$$

Proof: The isomorphsm follows directly from the first isomorphism theorem.
If x is transcendent, then

$$K(x) = \left\{ \frac{f(x)}{g(x)} | f(T), g(T) \in K[T], g \neq 0 \right\} \cong \left\{ \frac{f(T)}{g(T)} | f, g \in K[T], g \neq 0 \right\}$$

if x is transcendent, then $\operatorname{Ker} \varphi_x = (m_x(T))$ is a prime ideal. Because in a PID, every prime ideal $\neq (0)$ is a maximal ideal, we know that the faktor-ring with the maximal idea $K[T]/(m_x(T))$ is a field, so $K[X]$ is a subfield of L.
Furthermore, in $K[T]/(m_x(T))$ we can use division with rest to show that

$$1 + (m_x(T)), T + (m_x(T)), \ldots, \ldots T^{\deg m_x - 1} + (m_x(T)) \in K[T]/(m_x(T))$$

form a basis.

Definition

Let L/K and $x_1, \ldots, x_n \in L$. We write the smallest subfield of L that contains K aswell as $x_1, \ldots, x_n$ as

$$K(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} | f, g \in K[T_1, \ldots, T_n], g(x_1, \ldots, x_n) \neq 0 \right\}$$

Corollary (Wantzel, 1837)

With ruler and compass, neither the third root of 2 nor an angle of 20° can be constructed.
Furthermore, if $p \in \mathbb{N}, p > 2$ is prime, and the regular p-gon is constructable with ruler and compass, then p is a Farmat-prime: $p = 2^{2^n} + 1$.

Sketch of the proof: Assume that after finitely many constructions step starting from a unit length by intersecting straight lines with circleswe end up with a straight line of length $x = \sqrt[3]{2}$ or $x = \cos(20°)$. Then define $L_0 = \mathbb{Q}$, and then

$$L_{n+1} = \begin{cases} L_n & \text{if in the } n\text{-th construction step two lines are interected.} \\ \text{or} & \end{cases}$$

a quadratic field extension of L_n which contains the coordinates of the intersection betwen a cricle with a line or circle with a circle.

Then we have

$$(x-x_0)^2+(y-y_0)^2=A^2 \quad \text{and} \quad ax+by=c$$

If it has roots in L_n, then set $L_{n+1}=L_n$ and if it has roots, then set $L_{n+1}=L_n(x,y)$. Then

$$x \in L_N/\mathbb{Q} \implies [L_N:\mathbb{Q}]=2^l$$

for some $l \in \mathbb{N}$, but $K=\mathbb{Q}[X]/\mathbb{Q}$ has degree 3. So since

$$[L_N:L_0]=[L_N:L_{N-1}]\dots[L_1:L_0]$$

it would also have to be divisible by three, which is a contradiction.

Definition

A field extensions L/K is called **algebraic**, if every $x \in L$ is algebraic over K

Lemma

Every finite field extension is algebraic.

Proof: For $[L:K]<\infty$ and $x \in L$ the mapping

$$\varphi_x : K[T] \to L, \quad f \mapsto f(x)$$

cannot be injective because $K[T]$ has infinite dimension over K, whereas L by assumption only has finite dimension over K.

Corollary

Let L/K and $x,y \in L$ be algebraic over K. Then so are $x+y, x\cdot y$ and for $x \neq 0, \frac{1}{x}$.

Proof: By supposition we know that $[K(x):K]<\infty$. We can write the minimal polynomial $m_y(T) \in K[T]$ also as a polynomial in $K(x)[T]$.
This implies that y is also algebraic over $K(x)$ and so $[K(x)(y):K(x)]<\infty$.
From the lemma on the multiplicity we know that

$$[K(x,y):K]=[K(x)(y):K]=[K(x)(y):K(x)]\cdot[K(x):K]<\infty$$

so $K(x,y)$, which contains all the elements $x+y, x\cdot y, \dots \in K(x,y)$, is a finite field extension of K, and using the previous lemma, it is algebraic over K.

Corollary

Let F/L and L/K. Then F/K is algebraic if and only if F/L and L/K are algebraic.

Proof: $\implies$ is an exercise. For the reverse, assume F/L and L/K are algebraic field extensions each. Let $x \in L$. Then there exists a minimal polynomial $m_x^L(t) \in L[T]$. Now assume $y_1,\dots,y_n \in L$ are the coefficients of $m_x^L(T)$. Just like in the prevous corollary, we can show that

$$[K(y_1,\dots,y_n):K]<\infty$$

so since $m_x^L(T)$ has coefficients in $K(y_1, \dots, y_n)$, we know that

$$[K(y_1, \dots, y_n, x) : K(y_1, \dots, y_n)] \leq \deg m_x^L < \infty$$

using multiplicativity of the degrees, it also follows that $[K(y_1, \dots, y_n, x) : K] < \infty$.
And since $x \in K(y_1, \dots, y_n, x)$ and $K(y_1, \dots, y_n, x)/K$ is a finite field extensions, it must be algebraic.
Example: We trivially know that $\sqrt{2}$ and $\sqrt{3} \in \mathbb{R}$ are algebraic over $\mathbb{Q}$. Then

$$x = (\sqrt{2} + \sqrt{3}) \implies x^2 = 5 + 2\sqrt{6}$$
$$(x^2 - 5)^2 = (2\sqrt{6})^2 = 24 \implies m_x = x^4 - 10x^2 + 1$$

6.2 Splitting fields

Theorem (Kronecker)

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

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

for $a \in K, \alpha_i \in L$

Proof: We can assume without loss of generality that f is normed and prove it over induction on n. Since $K[T]$ is a PID, $f(T)$ has an irreducible divisor $p(T)$. We then define.

$$K_1 = K[T_1] \big/ p(T_1)$$

and look at K_1 as a field extension of K. Then in K_1 we have

$$p\left(T_1 + (p_1(T_1))\right) = p(T_1) + (p(T_1)) = 0 + (p(T_1))$$

so $f(T)$ has a root in K_1, namely $T_1 + (p(T_1)) =: \alpha_1$.
So we can write

$$f(T) = (T - \alpha_1) f_1(T) \quad \text{for} \quad f_1(T) \in K_1[T]$$

if $f_1 = 1$, then we are done because we can just set $L = K_1$. Otherwise we can use induction on the degree of f because $\deg f_1 < \deg f$ to get a field extension L/K_1

$$f_1(T) = \prod_{j=2}^{n} (T - \alpha_j), \quad \text{for} \quad \alpha_j \in L$$

Examples:

(a) For $\mathbb{R}$, take the polynomial $f(T) = T^2 + 1$, then $\mathbb{C} = \mathbb{R}[i]$ is such a field extension.

(b) For $K = \mathbb{Q}$ and $f(T) = T^3 - 2$ the field extension is

$$L = \mathbb{Q}[\sqrt[3]{2}, \xi \sqrt[3]{2}, \xi^2 \sqrt[3]{2}$$

for $\xi = \frac{-1+\sqrt{3}i}{2}$ a third root of unity.

Definition Splitting field

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

(a) f can be split into linear factors in $L[T]$

(b) For any field E with $K \subseteq E \subsetneq L$, f does not split over E.

Note: Such a splitting field always exists and is unique up to isomorphism.

- If $f \in K[T]$ then we can use Kronecker's theorem to find a field F/K such that f has roots $\alpha_1, \dots, \alpha_n \in F$. Then $L := K[\alpha_1, \dots, \alpha_n]$ is a splitting field.
- A splitting field is of course an algebraic field extension of K

Examples

(a) For $K = \mathbb{Q}$ and $f(T) = T^2 + 1 \in \mathbb{Q}[T]$ then $\mathbb{C}$ is not a splitting field for this setting, since $Q[i] \subseteq \mathbb{R}[i] = \mathbb{C}$ splits f.

(b) For $K = \mathbb{R}$ and $f(T) = T^2 + 1$ as above, then thesplitting field of f over $\mathbb{R}$ is $\mathbb{C}$.

Note: For a field $K, f \in K[T]$ and L a splittig field of f over K, then

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

if f over K is irreducible, then $[LK] \geq \deg f$.

6.3 Algebraic closure

Definition

A field K is called **algebraically closed**, if every polynomial $f \in K[T]$ with $\deg f > 0$ has a root in K.
It follows on induction that f can be split into linear components.

Note: Every algebraically closed field has ifinitely many elements because if $K = \{k_1, \dots, k_n\}$, then look at

$$f(T) = (T - k_1) \dots (T - k_n) + 1 \in K[T]$$

Proposition

Let L/K be a field extension such that L is algebraically closed. Then the set

$$E = \{x \in L \big| x \text{ is algebraic over } K\}$$

is an algebraically closed field extension of K.
We use this as our definition. We call E the **algebraic closure** $\overline{K}$ of K

Proof: We need to show that E is a field, that it is algebraically closed, and not dependent on L.
It is a field because if $x, y \in L$ are algebraic, then $x + y, x \cdot y$ and $\frac{x}{y}$ are algebraic, for $y \neq 0$
To show that it is algebraically closed, let $f \in E[T]$ with $\deg f > 0$ and let E_1 be an algebraic extension of E such that f has a root $\alpha \in E_1$. (This is possible because Kronecker's theorem). Then E_1/E is algebraically closed. But then $\alpha \in L$ and because L is algebraically closed, $\alpha \in E$.
Note: if K is finite, then $\overline{K}$ is countable because $K[T]$ is countable by going through the polynomials ordered by degree. The same reasoning can show that if K is countable, then so is $\overline{K}$.
In the proposition, we just assumed that K had an algebraically closed field extension L/K but we can show that it always exists and is unique up to isomorphism.

Theorem

Let K be a field. Then there exists a field extension L/K such that L is algebraically closed and L is unique up to isomorphism.

Proof: For every non-constant polynomial $f \in K[T]$, let T_f be a variable. We consider the polynomialring (in possible infinitely many variables)

$$R := K\left[(T_f)_{f \in K[T], \deg f > 0}\right]$$

Let $I \lhd R$ be the ideal generated by the elements $f(T_f)$.

$$I := \left[f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0, \implies f(T_f) = (T_f)^n + a_{n-1}(T_f)^{n-1} + \ldots + a_9\right]$$

Then we can show that $I \neq R$:
Chose $1 \in I$,

$$1 = \sum_{i \in X} g_i f_i(T_{f_i}) \in I, \quad \text{for} \quad g_i \in K[T_{f_i}]$$

then look at the set E such that every f_i has aroot α_i in E. Then evaluate f_i at $T_{f_i} = \alpha_i$. and we get that

$$1 = \sum_{i \in X} \underbrace{g_i(\ldots)}_{\in E} \underbrace{f_i(\alpha_i)}_{=0} = 0 \lightning$$

Since $R \neq \{0\}$, there exists a maximal ideal $M \subseteq R$, that contains I. Then define

$$L_1 := {}^{R}\!/_{M}$$

then L_1 is a field (because M is maximal) and $K \to L_1$ is an injective field homomorphism. By identifiying K with it's image in L_1

$$K \to K[(T_f)_f] \to {}^{K[(T_f)_f]}\!/_{M} = L_1$$

Next we want to show that every $f \in K[T]$ with $\deg f > 0$ has a root in L_1 and that L_1/K is an algebraic field extension.
The image of T_f in L_1 is a root of $f \in L_1[T]$ because

$$f(T_p + M) = \underbrace{f(T_f)}_{\in I \subseteq M} + M = 0 + M$$

and every $x \in L_1$ is in the image of $K[T_{f_1}, \ldots, T_{f_m}]$ for a finite set of variables T_{f_i}. Because every T_{f_i} is algebraic over K, so is x. This shows that L_1/K is an algebraic field extension of K.
Lastly, we repeat this process for L_1 instead of for K and we get an L_2/L_1, and so on to get the stack of field extensions

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots$$

where every $f \in L_i[T]$ iwth $\deg f > 0$ has a root in L_{i+1}.
Then take the union of them all

$$L := \bigcup_{n \geq 0} L_n$$

which can be shown to be a field containing K and being algebraically closed over K.
This follows from the fact that

$$F/L, L/K \text{ algebraically closed} \iff F/K \text{ algebraically closed}$$

To show that L is algebraically closed, let $f \in L[T]$ with $\deg f > 0$.
Because f only has finitely many coefficients, who each lie in some L_i, we can take the maximum of the L_i to find that

$$f = (T - \alpha_1) f_1, \quad \text{for} \quad L_{i+1}[T] f_1 = (T - \alpha_2) f_2, \quad \text{for} \quad L_{i+2}[T]$$

so f splits into linear factors.

6.4 Uniqueness

We have seen that for every $f \in K[T]$ there is a splitting field aswell as an algebraic closure. In this section, we find out if/how they are unique.

Theorem

Let K be a field, L/K a field extensions and L algebraically closed. Then

(a) If $E = K[\alpha]$ is a finite field extension of K, then there is at least one and at most $[E : K]$ field embeddings

$$\sigma : E \to L \quad \text{such that} \quad \sigma | K = \mathrm{id}_K$$

if $\operatorname{char} K = 0$, then there are exactly $[E : K]$ such embeddings.

(b) If E/K is an algebraic field extension, then there exists a K-linear embedding $\sigma : E \to L$.

To prove this, we need the following lemma

Lemma

Let K be a field, $m(T) \in K[T]$ coprime to its derivative $m'(T)$. Then $m(T)$ has exactly $\deg m(T)$ many roots in an algebraic field extension.
This is the case if $\operatorname{char} K = 0$ and $m(T)$ is irreducible in $K[T]$.

Proof: We define the derivative as the linear map given by

$$D : f = \sum_{n=0}^{\infty} a_n T^n \mapsto f' = \sum_{n=1}^{\infty} n a_n T^{n-1}$$

which satisfies the product rule

$$(fg)' = f'g + fg'$$

the product rule itself is a polynomial equation over $\mathbb{Z}$ in the coefficients of f and g. In particular we have

$$\Big((T-\alpha)^2 g(T)\Big)' = 2(T-\alpha)g(T) + (T-\alpha)^2 g'(T) = \big(2g(T) + (T-\alpha)g'(T)\big)$$

so if f has a root with higher multiplicity, then it is also a root of f'
The same holds if $\alpha \in L$ when L/K is a field extension.
Now assume $m(T)$ and $m'(T)$ are coprime, then there exist $h_1, h_2 \in K[T]$ such that

$$1 = h_1(T)m(T) + h_2(T)m'(T)$$

so if L/K is a field extension and $\alpha \in L$ is a root of $m(T)$ such that $m'(\alpha) \neq 0$, then that means that it has to be a root with single multiplicity.

Missing 5 mins

Now can prove the first item from the theorem. Let $m(T)$ be the minimal polynomial of α over K and $\beta = \sigma(\alpha)$ for a k-linear field embedding $\sigma : E \to L$. then

$$m(\beta) = m(\sigma(\alpha)) = \sigma(m(\alpha)) = 0, \quad \text{for} \quad m(T) = \sum_n a_n T^n, a_n \in K$$

but because σ is a ring homormophism, it must map a_n to a_n. Furthermore, if we go the other way around: for a $f(\alpha) \in K[\alpha]$ we know that

$$\sigma(f(\alpha)) = f(\sigma(\alpha)) = f(\beta)$$

so $\beta = \sigma(\alpha)$ is a root and σ is uniquely determined by this root.
Since $m(T)$ has at most $\deg(m(T)) = [E : K]$ roots in L we know that there can be at most this many K-linear field embeddings.
For the converse, let $\beta \in L$ be any root of $m(T)$. Then we can use the lemma to show that the existse excactly $\deg m(T)$ many roots.
We can use β to define a K-linear field inlcusion

$$\sigma = \sigma_\beta : E = K[\alpha] \to L$$

Consider the ways to map $f(T) \in K[T]$ using the evaluation mappings ev_α and ev_β.

$$f(T) \mapsto f(\alpha) \in K[\alpha] = E \quad \text{and} \quad f(T) \mapsto f(\beta) \in K[\beta] \subseteq L$$

Then $\mathrm{Ker}(\mathrm{ev}_\alpha) = (m(T))$ and since $m(\beta) = 0$ we can conlclude that $(m(T)) \subseteq \mathrm{Ker}\,\mathrm{ev}_\beta$. But because $(m(T))$ is a maximal ideal, we even get equality $(m(T)) = \mathrm{Ker}\,\mathrm{ev}_\beta$.
Using the first isomorphism theroem, we get the mappings $\overline{\mathrm{ev}_\alpha}$ and $\overline{\mathrm{ev}_\beta}$.

$$\begin{tikzcd}
& f(\alpha) \in K[\alpha] = E \\
f(T) + (m(T)) \in K[T]/(m(T)) \arrow[ur, "\overline{\mathrm{ev}_\alpha}"] \arrow[dr, "\overline{\mathrm{ev}_\beta}"'] & \\
& f(\beta) \in K[\beta] \subseteq L
\end{tikzcd}$$

so we can set

$$\sigma = \overline{\mathrm{ev}_\beta} \circ (\overline{\mathrm{ev}_\alpha})^{-1} : E \to L$$

as our embedding. And for two different roots $\beta_1 \neq \beta_2 \in L$ we have

$$\sigma_{\beta_1}(\alpha) = \beta_1 \neq \beta_2 = \sigma_{\beta_2}(\alpha) \implies \sigma_{\beta_1} \neq \sigma_{\beta_2}$$

so we see that there exactly as many field embeddings of $E = K[\alpha]$ into L as there roots of $m(T)$ in L.
Example: Consider $K = \mathbb{F}_p((X))$ and $m(T) = T^p - X$ (which is irreducible).
For $E = {}^{K[T]}\!/\!_{(m(T))}$, we have the root $T + (m(T)) = \alpha$ of $m(T)$. Here we have

$$m(T) = (T-\alpha)^p = T^p - \alpha^p = T^p - X$$

so m has α as a root with multiplicity p.
To show the second item in the theorem we will need Zorn's Lemma because the field extension can be infinite dimensional.
We define

$$\mathcal{O} = \{(F,\sigma) | F \text{ field with } K \subseteq F \subseteq E, \sigma : F \to L \text{ is } K\text{-linear field extension}\}$$

Naturally we get the partial ordering on $\mathcal{O}$ give by

$$(F_1, \sigma_1) \leq (F_2, \sigma_2) \iff F_1 \subseteq F_2 \text{ and } \sigma_2 | F_1 = \sigma_1$$

To be able to use Zorn's lemma, we need to show the following

- $\mathcal{O} \neq 0$, because $(K, \mathrm{id}) \in \mathcal{O}$.
- Let $T \subseteq \mathcal{O}$ be a totaly ordered chain in Ω. We define

$$F_T = \bigcup_{(F,\sigma) \in T} F \subseteq E$$

which should be a subfield of E. The proof of this is trivial. For the field embedding, we define

$$\sigma_T : F_T \to L, \quad x \in F \mapsto \sigma(x) \quad \text{for} \quad (F,\sigma) \in T$$

this (just like F_T) is well defined because T is a totally ordered chain: If we had $(F_1, \sigma_1) \leq (F_2, \sigma_2) \in T$, we can pick either of the σ because

$$\sigma_2(x) = \sigma_2 | F_1(x) = \sigma_1(x)$$

σ_T is also a field embedding, because for $x_1, x_2 \in F_T$ there exist

$$(F_1, \sigma_1), (F_2, \sigma_2) \in T \quad \text{such that} \quad x_1 \in F_1, x_2$$

because T is totally ordered, without loss of generality $(F_1, \sigma_1) \leq (F_2, \sigma_2)$, so

$$\sigma_T(x_1 + x_2) = \sigma_2(x_1 + x_2) = \sigma_2(x_1) + \sigma_2(x_2) = \sigma_T(x_1) + \sigma_t(x_2)$$

and analogously for $x_1 \cdot x_2$ and $\frac{1}{x_1}$ if $x_1 \neq 0$.

- So (F_T, σ_T) is an upper bound of T.

Zorn's Lemma then says that $\mathcal{O}$ has a maximal Element $(F, \sigma) \in \mathcal{O}$.
With this we set $E = F$ and $\sigma : F \to L$ as the wanted field embedding.
If $E \neq F$, there must be an $\alpha \in E \setminus F$. In this case we use $\sigma : F \to L$ to identify the Elements of F with the elements of $\sigma(F)$. Then

$$F \subseteq F[\alpha] \subseteq E, \text{ and } F \subseteq L$$

and we are in the setting of the first item in the theorem. Using the first part, we know that there is an F-linear field empedding $\varphi : F[\alpha]L$.
Since we used α to identify elements of F with elements of $\sigma(F)$, it means that $\varphi : F[\alpha] \to L$ extends the mapping $\sigma : F \to L$m which means $(F, \sigma) < (F[\alpha], \varphi)$.
But this is a contradiction to the maximality of (F, σ).

Corollary

Let K be a field.

(a) For every $f \in K[T]$, the splitting field is unique up to a K-linear isomorphism.

(b) Every two algebraic closures of K are K-linearly isomorphic.

- Proof: Let $f(T) \in K[T]$ and E_1, E_2 be splitting fields of $f(T)$. Then let L_2 be an algebraic closure of E_2.

  Then we can use the second part of the theorem to get a $\sigma : E_1 \to L_2 \supseteq E_2$

$$\begin{tikzcd}
 & E_1 \arrow[dd, "\sigma"] \\
K \arrow[ur] \arrow[dr] & \\
 & L_2
\end{tikzcd}$$

  so we can write for $\alpha_1, \ldots, \alpha_n \in E_1$ that

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

  so roots get mapped to roots.

But

$$E_1 = K[\alpha_1, \dots, \alpha_n] = \left\{ \frac{q_1(\alpha_1, \dots, \alpha_n)}{q_2(\alpha_1, \dots, \alpha_n)} | q_1, q_2 \in K[T_1, \dots, T_n], q_2(\alpha) \neq 0 \right\}$$

is generated by the roots of f. And because E_2 is a splitting field, the polynomails $(T - \sigma(\alpha_i))$ must lie in E_2, so $E_2 = K[\sigma(\alpha_1), \dots, \sigma(\alpha_n)]$ which is generated by these roots, is the image of σ.

$$\sigma(E_1) = \sigma(K(\alpha_1, \dots, \alpha_n)) = E_2$$

This means that $\sigma : E_1 \to E_2$ must be an isomorphism.

- Let L_1, L_2 be to algebraic closures of K. Using the second part of the Theorem, we get a field embedding

  $$\sigma : L_1 \to L_2 \quad \text{with} \quad K \subseteq \sigma(L_1) \subseteq L_2$$

  further L_2/K is algebraic and $\sigma(L_1)$ is algebraically closed. L_2 being algebraic just means that every element is the root of a polynomial with coefficients in K

  $$\alpha \in L_2 \implies \exists f \in K[T] \setminus \{0\}, f(\alpha) = 0$$

  so $L_2 \subseteq \sigma(L_1) \subseteq L_2$, which shows that $\sigma : L_1 \to L_2$ is an isomorphism.

6.5 Finite Fields

We know that $\mathbb{F}_p = \mathbb{Z}/_{(p)}$ for $p \in \mathbb{N}$ prime is a finite field. Are there more and can we classify them?

Theorem (Galois, Gauss)

(a) If K is a finite field, then $|K| = p^n$ for $p \in \mathbb{N}$ prime and $n \geq 1 \in \mathbb{N}$

(b) For every power of a prime p^n there exists an up to isomorphism unique finite field with p^n elements.

(c) Let $p \in \mathbb{N}$ prime and K an algebraic closure. Then for every $n \geq 1$, K contains an up to isomorphism unique subfield $\mathbb{F}_{p^n}$ with p^n Elements. We can even determine this subfield as

$$\mathbb{F}_{p^n} = \left\{ x \in K | x^{(p^n)} = x \right\}$$

(d) For $m, n \geq 1$ and fields as in (c)

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m | n$$

Proof

(a) Let $|K| < \infty$. Then $\mathbb{Z} \cdot 1_k \cong \mathbb{F}_p = \mathbb{Z}/_{(p)}$ for a prime $p \in \mathbb{N}$. Therefore K is a finite-dimensional vector space over $\mathbb{F}_p$ so

$$K \cong \mathbb{F}_p^{[K:\mathbb{F}_p]} \implies |K| = p^{[K:\mathbb{F}_p]}$$

(b) To construct a field with $q = p^n$ Elements we define it as a splitting field. For the polynomial $T = T^q - T$, let L be the splitting field of f over $\mathbb{F}_p$ and

$$E = \{x \in L | x^q = x\}$$

Consider the **Frobenius-Homomorphism**

$$\Phi : L \to L, \quad x \mapsto x^p \implies \Phi^n : L \to L, \quad x \mapsto (\dots(x^p)^p \dots)^p = x^{np} = x^q$$

Because L is the splitting field of a finite field, L itself is also a finite field. Moreover, Φ is an Automorphism because Φ is injective and $|L| < \infty$, so

$$E = \{x \in L | \Phi^n(x) = x\} = \{x \in L | f(x) = 0\}$$

which means that E is a subfield of L containing all roots of f, which means $E = L$.

Now we need to show that E has p^n Elements. This is equivalent to saying that f doesn't have roots with higher multiplicity. Recall that we can analyze this by looking at the derivative $f'(T)$ and checking if they are co-prime and if $f'(T)$ it has no roots:

$$f'(T) = qt^{q-1} - 1 = -1 \neq 0$$

This means that there are exactly q roots in L, so

$$|L| = |E| = q = p^n$$

Now let F be a finite field with p^n elements. From (a) we know that it extends $\mathbb{F}_p$. Furter, for $x \in F^\times$ that $x^{p^n - 1} = 1$ because $F^\times$ is a group.

Aso $x^{p^n} = x$ for all $x \in F$. So F consists of the roots of the polynomial $F(T) = T^q - 1$ which makes it the splitting field of f.

The previous corollary proves uniqueness up to isomorphism, since $F \cong L$.

(c) Let K be an algebraic closure of $\mathbb{F}_p$. Then

$$\mathbb{F}_{p^n} = \left\{x \in K | x^{p^n} = x\right\} \subseteq K$$

is a subfield. But just like before, we see that it is the splitting field of $T^q - T$ and $|\mathbb{F}_{p^n}| = p^n$

(d) If $m|n$, then $n = m \cdot k$ so $\Phi^n = (\Phi^m)^k$ and

$$\mathbb{F}_p^n = \{x | \Phi^n(x) = x\} \supseteq \{x | \Phi^m(x) = x\} = \mathbb{F}_{p^m}$$

For the other direction, assume $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, then we can view this as a field extension and thus see $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_{p^m}$, so

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^k = p^{mk} \quad \text{for} \quad k = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}$$

which shows divisibility of n by m.

Theorem

Let K be a field and $G \subseteq K^\times$ a finite subgroup. Then G is cyclic.
In particular, $\mathbb{F}_{p^n}^\times$ is cyclic for every power of a prime p^n.

Proof: Using classification of finite abelian groups we have the isomorphism

$$(G, \cdot) \cong \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_1)$$

for $1 < d_1 | d_2 | \ldots | d_n$ with $+$ as its group operation.
It is clear that $x^{d_n} = 1$ for all $x \in G$ because

$$d_1 | \ldots | d_n \implies d_n \cdot (a_1 + (d_1), \ldots, a_n + (d_n)) = (0 + (d_1), \ldots, 0 + (d_n))$$

This is equivalent to saying that every $x \in G$ is a root of the polynomial $T^{d_n} - 1$.
Also $|G| = d_1 d_2 \ldots d_n$. Which can only be true if $n = 1$, or else we would have more roots ($d_1 \ldots d_n$ many) than the degree of this polynomial $\deg(T^{d_n - 1} = d_n$.
But then the isomorphism just says $G \cong \mathbb{Z}/(d)$ which means that G is cyclic.

Corollary

Let $p > 2$ be prime. Then for $a \in \mathbb{F}_p$

$$a^{\frac{p-1}{2}} = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a = b^2, \text{ for } b \in \mathbb{F}_p^\times \\ -1 & \text{else} \end{cases}$$

Sketch of proof. We show

$$\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)$$

and we can give the proof in $\mathbb{Z}/(p-1)$.

Recap

Theorem Smith Canonical Form

For an $A \in \mathrm{Mat}_{mn}(R)$ we can obtain a diagonal matrix $D = gAh^{-1}$ for $g, h \in \mathrm{GL}_m(R), \mathrm{GL}_n(R)$

Theorem

Let G be a finitely generated abelian group, then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k)$$

for $r \geq 0, 1 < d_1 | \ldots | d_n$.

We proved this using the smith normal form where we set

$$\varphi : (a_1, \dots, a_l) \mapsto \sum_{i=1}^{l} a_i g_i$$
$$G =< g_1, \dots, g_l >\cong \mathbb{Z}^l \diagup \operatorname{Ker}\varphi$$

And we could see that $\operatorname{Ker}\varphi = A\mathbb{Z}^n$ setting r to be the number of zeros in the diagonal of D.
Alternatively, we could write

$$G \cong \mathbb{Z}^r \times G_{\text{tors}}$$
$$G_{\text{tors}} \cong \prod_p G_p, \text{ for } G_p \text{ Sylow } p\text{-subgroups}$$
$$G_p \cong \mathbb{Z}\diagup(p^{l_1}) \times \dots \times \mathbb{Z}\diagup(p^{l_k})$$

We can explain this as follows. For the prime factorisation $d_j = p_1^{a_1} \dots p_s^{a_s}$ we can use the chinese remainder theorem to show

$$\mathbb{Z}\diagup(d_j) \cong \mathbb{Z}\diagup(p_1^{a_1}) \times \dots \times \mathbb{Z}\diagup(p_s^{a_s})$$

Then because G_{tors} is a finitely generated Torsion module, it is clear that there exists a $D \geq 1$ with $D \cdot g = 0$ for all $g \in G_{\text{tors}}$, because we can take the product of the finitely many d that eliminate g.
If $D = ab$ for $a, b \in \mathbb{N}$ coprime, then we have the decomposition

$$G_{\text{tors}} \cong G_a \times G_b$$
$$G_a = \{g \in G_{\text{tors}} | a \cdot g = 0\}$$
$$G_b = \{g \in G_{\text{tors}} | b \cdot g = 0\}$$

because we can look at the mapping

$$\Phi : G_a \times G_b \to G_{\text{tors}} \quad (g_1, g_2) \mapsto g_1 + g_2$$

Injectivity is equivalent to $G_a \cap G_b$: Because a, b are coprime, there exist $c, f \in \mathbb{Z}$ such that $ca + fb = 1$.
Then for $g \in G_a \cap G_b$ we have

$$1 \cdot g = eag + fbg = 0 \implies G_a \cap G_b = 0$$

For surjectivity let $g \in G_{\text{tors}}$. Then for $g = eag + fbg$, we just need to show that $eag \in G_b$ and $fbg \in G_a$.
This is true because

$$b(eag) = eabg = eDg = 0$$

and analogously for $fbg \in G_a$.
By iterating this decomposition we get Modules H_p with the property that for some power of a prime we have $p^n h = 0q$ for all $h \in H$.
Using the first part of the theorem we get

$$H \cong \mathbb{Z}\diagup(e_1) \times \dots \times \mathbb{Z}\diagup(e_k)$$

Because $p^n h = 0$ for all $h \in H$, we must have $e_k | p^n \implies e_j = p^{l_j}$ because

$$p^n (0 + (e_1), \dots, 1 + (e_k)) = (0 + (e_1), \dots, p^n + (e_k)) = 0$$

if and only if $e_k | p^n$