Abstract Algebra II

—

A Continuation of Abstract Algebra I

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University
2019

Contents

1 Further Elements of Group Theory

In this first chapter we will give an introduction to group theory. Our main results will be the characterization of finitely generated Abelian groups, and Sylow's theorems. Finally we will talk about solvable groups which will turn out to be important for our study of field extensions in a later chapter.

1.1 Basic Notions

Definition 1.1 A group is a triple $(G, \cdot, e)$, where G is a non-empty set and $\cdot$ is a binary operation on G, i.e. a mapping $G \times G \longrightarrow G$ such that the following is true:

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.

(ii) $e \cdot a = a$ for all $a \in G$.

(iii) For every $a \in G$ there exists $b \in G$ with $b \cdot a = e$.

If, in addition,

(iv) $a \cdot b = b \cdot a$ for all $a, b \in G$.

then G is called an Abelian group. If G is finite, then $|G|$ is called the order of G, otherwise we say G has infinite order.

By abuse of notation we usually write G instead of $(G, \cdot, e)$. Moreover, we will omit the operation symbol $\cdot$, i.e. we write ab instead of $a \cdot b$. Finally we point out that the identity e is often written as 1. In case of Abelian groups people mostly use the operation symbol $+$, and in this case 0 takes the role of the identity.

Remark 1.2 For every group G there holds:

(a) $g1 = g$ for all $g \in G$.

(b) The identity 1 is uniquely determined by its properties.

(c) If $ba = 1$ then $ab = 1$ for $a, b \in G$.

Proof: **(a)** Let $g \in G$ be arbitrary, there are elements $h, f \in G$ with $hg = 1$ and $fh = 1$. From this we get $f1 = f(hg) = (fh)g = 1g = g$, and hence $g1 = (f1)1 = f(1 \cdot 1) = f1 = g$.
(b) If $1'$ were a further identity, then we would have $1 = 1'1 = 1'$ by **(a)**.
(c) As we have already seen in **(a)** for $a, b, c \in G$ with $ba = 1 = cb$ we have the equality $c = c1 = a$, and this means $1 = cb = ab$. □

Definition 1.3 A non-empty subset U of a group G is called a subgroup, if the operation of G can be restricted to U and U is a group with respect to this operation. We then write $U \leq G$

Remark 1.4 Let G be a group with identity 1.

(a) If U is a subgroup of G then $1 \in U$. This can be verified as follows: if f is the identity of U then $f = f1 = f(ff^{-1}) = f^2f^{-1} = ff^{-1} = 1$.

(b) $\{1\}$ and G are subgroups of G.

Examples 1.5 **(a)** The most natural examples of (Abelian) groups are $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$ and $(\mathbb{C}, +, 0)$, but also $(\mathbb{Z}/n\mathbb{Z}, +, 0)$. Moreover $(\{-1, 1\}, \cdot, 1))$, $(\mathbb{Q}^\times, \cdot, 1)$, $(\mathbb{R}^\times, \cdot, 1)$ as well as $(\mathbb{C}^\times, \cdot, 1)$ are Abelian groups, where we abbreviate $F^\times := F \setminus \{0\}$.

(b) If F is a field and n a positive integer, then $\mathrm{GL}(F, n)$, the set of all invertible $n \times n$-matrices, forms a group. A well-studied subgroup of this group is $\mathrm{SL}(F, n)$, the set of all invertible matrices with determinant 1.

(c) The set $S(X)$ of all bijective mappings (permutations) of a set X onto itself forms a group with respect to the composition of mappings. If $X = \{1, \ldots, n\}$ then this group is denoted by S_n and possesses $n!$ elements. An important subgroup of S_n is A_n, the set of all even permutations. Its order is given by $n!/2$ for all $n \geq 2$.

We are now interested in an "easy-to-apply criterion" for the subgroup property.

Lemma 1.6 *Let G be a group and U a subset of G. Then U is a subgroup of G if and only if:*

(a) $U \neq \emptyset$.

(b) *If $a, b \in U$, then also $ab \in U$.*

(c) *If $a \in U$, then also $a^{-1} \in U$.*

Proof: If $U \leq G$ then certainly **(a)** and **(b)** are satisfied. Taking into consideration that $1 \in U$ by 1.4(a) we then find that also **(c)** holds.
Conversely, assuming these conditions, the operation on G allows for restriction to U by **(b)**, and associativity does not require a proof. For a given $u \in U$ we have $u^{-1} \in U$ by **(c)** and hence $1 = uu^{-1} \in U$ by **(b)**. All in all this shows the claim. □

The criteria that we have discussed so far allow for a further simplification. Its proof is left to the reader.

Lemma 1.7 *Let U be a subset of a group G. Then U is a subgroup of G if and only if:*

(a) $U \neq \emptyset$.

(b) *If* $a, b \in U$ *then also* $ab^{-1} \in U$.

If G is finite, then **(b)** *can be replaced by*

(b*) *If* $a, b \in U$, *then also* $ab \in U$.

If G is a group and $(U_i)_{i \in I}$ is a family of subgroups of G, then $\bigcap_{i \in I} U_i$ is also a subgroup of G. This is easily verified and justifies the following definition.

Definition 1.8 Let G be a group and M a subset of G. We call

$$\langle M \rangle := \bigcap \{U \mid M \subseteq U \leq G\}$$

the subgroup generated by M in G. It is the smallest subgroup of G which contains M, and we mention that $\langle \emptyset \rangle = \{1\}$.

A more constructive description of the subgroup generated by M is given by the following proposition. The proof is left as an exercise.

Proposition 1.9 *Let G be a group.*

(a) *For every subset M of G there holds*

$$\langle M \rangle = \{x_1^{n_1} \dots x_k^{n_k} \mid k \in \mathbb{N}, n_i \in \mathbb{Z} \text{ and } x_i \in M\}.$$

In particular, for arbitrary $g \in G$ we have $\langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

(b) *If U and V are subgroups of G, then*

$$\langle U \cup V \rangle = \{u_1 v_1 \dots u_k v_k \mid k \in \mathbb{N}, u_i \in U \text{ and } v_i \in V\}.$$

If the subgroup generated by a single element $g \in G$ is finite, then the order of this subgroup is also called the order of g, i.e. $\mathrm{o}(g) := \langle \{g\} \rangle$.

From Linear Algebra we are used to the fact that for two subspaces U and W of a vector space $(V, +, 0, F)$ there holds

$$\langle U \cup V \rangle = U + V = \{u + v \mid u \in U, v \in V\}.$$

In light of the foregoing proposition this is not a surprise since it is true for Abelian groups in general. In the following we will discuss in how far we can state a similar fact in the context of arbitrary groups.

Definition 1.10 If U, V are subgroups of a group G, we define

$$UV := \{uv \mid u \in U, v \in V\}.$$

Clearly we have $U\{e\} = UU = U = \{e\}U$ und $GU = G = UG$, however $UV \neq VU$ in general.

Proposition 1.11 *Let U, V be subgroups of the group G.*

(a) *$UV = VU$ holds if and only if UV is a subgroup of G.*

(b) *If $UV = VU$, then $UV = \langle U \cup V \rangle$.*

Proof: **(a)** Assume that UV is a subgroup of G and let g be an element of UV. Then also $g^{-1} \in UV$ and of the form $g^{-1} = uv$ for suitable $u \in U$ and $v \in V$. Consequently $g = v^{-1}u^{-1}$ is an element of VU, which shows $UV \subseteq VU$. Conversely, if $g \in VU$, then $g = vu$ for suitable $v \in V$ and $u \in U$. Hence $g^{-1} = u^{-1}v^{-1}$ is an element of UV. As UV is a subgroup we therefore have $g \in UV$.
Assume now that $UV = VU$; we apply criterion 1.7 and first observe that $UV \neq \emptyset$. Let $g, h \in UV$, then there exist $u_1, u_2 \in U$ und $v_1, v_2 \in V$ with $g = u_1v_1$ und $h = u_2v_2$. We then have $gh^{-1} = u_1v_1v_2^{-1}u_2^{-1} = u_1vu_2$, where $v = v_1v_2^{-1}$. Now we have $u_1v = v'u_1'$ for suitable $v' \in V$ and $u_1' \in U$, and this leads to $gh^{-1} = v'u_1'u_2^{-1} \in VU = UV$. For this reason we finally see that UV is a subgroup.
(b) If $UV = VU$, then multiple applications of the ideas in **(a)** lead to

$$\begin{aligned} \langle U \cup V \rangle &= \{u_1v_1 \dots u_kv_k \mid k \in \mathbb{N}, u_i \in U \text{ und } v_i \in V\} \\ &= \{uv \mid u \in U, v \in V\} = UV, \end{aligned}$$

which shows the claim. □

Let G be a group and U a subgroup of G. We consider the relations $\sim_L$ and $\sim_R$, with $g \sim_L h$ if and only if $gU = hU$, and $g \sim_R h$ if and only if $Ug = Uh$. These relations are equivalence relations and their equivalence classes are of the form gU (respectively Ug) with $g \in G$. These are called left cosets (or right cosets, respectively) of U in G. A simple proof shows that there is a bijection between the set of all left cosets and the set of all right cosets. This justifies the following definition.

Definition 1.12 Let U be a subgroup of the group G. If U has finitely many left cosets (right cosets) in G then we call the number of these the *index* of U in G, denoted by $[G : U]$. If this number is not finite, then we say U is of infinite index in G.

If U is a subgroup of the finite group G then the relations $G = \bigcup_{g \in G} gU$ and $|gU| = |U|$ imply what is called Lagrange's theorem.

Theorem 1.13 *Let U be a subgroup of the finite group G. Then there holds*

$$|G| = [G : U] \cdot |U|.$$

In particular we see that the order and index of a subgroup of a finite group are divisors of the order of the given group.

Remark 1.14 A converse of the foregoing statement is wrong in general, i.e. for a given divisor d of the group order there does not necessarily exist a subgroup of order d. However, in the context of Abelian groups and when dealing with Sylow's theorems we will see in how far such results can be stated.

Similar to what we learned in Linear Algebra we will now find out how we can compute with cosets of a subgroup in a given group. For this we need some preparation.

Definition 1.15 A subgroup U of a group G is called a normal subgroup (in short form $U \trianglelefteq G$) if each of its left cosets is at the same time a right coset.

Clearly $\{1\}$ and G are normal subgroups of a group G. In an Abelian group every subgroup is normal. The following proposition gives information about the immediately arising question for normality criteria.

Proposition 1.16 *For a subgroup U of a group G the following are equivalent:*

- **(a)** *U is normal in G.*
- **(b)** *Every right coset of U in G is also a left coset.*
- **(c)** *For all $g, h \in G$ the set $gUhU$ is a left coset of U in G.*
- **(d)** *For all $g, h \in G$ there holds $gUhU = ghU$.*
- **(e)** *$gUg^{-1} \subseteq U$ for all $g \in G$.*
- **(f)** *$gUg^{-1} = U$ for all $g \in G$.*
- **(g)** *$gU = Ug$ for all $g \in G$.*

Proof: To show that **(a)** implies **(b)** let R be a transversal of all left cosets of U in G, i.e. $R \subseteq G$ and $G = \bigcup\limits_{g \in R} gU$. As U is normal, we know that for every $g \in R$ there exists $h(g) \in G$ with $gU = Uh(g)$. For this reason we have $G = \bigcup\limits_{g \in R} gU = \bigcup_{g \in R} Uh(g)$, and here

every right coset must have occured. Hence every right coset is at the same time a left coset.
Next we show that **(b)** implies **(c)**. For arbitrary $h \in G$ we know that Uh is a right coset and hence a left coset, i.e. there exists $k \in G$ such that $Uh = kU$. This shows that $gUhU = gkUU = gkU$, which is clearly a left coset of U in G.
To see that **(c)** implies **(d)** let $gUhU = \ell U$ for some $\ell \in G$. Note, that $gh = g1h1 \in gUhU = \ell U$ and hence gh may be taken as representative for ℓU. Consequently we have $ghU = \ell U$.
Let us now show that **(d)** implies **(e)**. For $g \in G$ we have $gUg^{-1}U = gg^{-1}U = U$ and therefore immediately $gUg^{-1} \subseteq U$.
To show that **(e)** implies **(f)** let $gUg^{-1} \subseteq U$ for all $g \in G$. Then this must clearly also be true for all $g^{-1} \in G$. Consequently $g^{-1}Ug \subseteq U$ which by multiplication with g and g^{-1} respectively can be transformed to $U \subseteq gUg^{-1}$.
To prove that **(g)** follows from **(f)** we get by multiplication from the right with g immediately that from $gUg^{-1} = U$ there follows the relation $gU = Ug$.
It is finally clear that **(g)** implies **(a)**. □

Definition 1.17 If $\{1\}$ and G are the only normal subgroups of a group G then we call G a simple group.

If G is of prime order then G is Abelian and simple. We will see later that the finite Abelian groups are simple if and only they are prime.

A characterization of all finite (non-Abelian) simple groups was initiated by the so-called Hölder program and was completed in the 80's of the previous century. This result is one of the most complicated and rich mathematical works that has ever been published.

In the following we give further properties of normal subgroups.

Proposition 1.18 *Let G be a group:*

- **(a)** *If $(N_i)_{i\in I}$ is a family of normal subgroups of G, then $\bigcap_{i\in I} N_i$ is normal, too.*
- **(b)** *If N is a normal subgroup of G and U a subgroup of G, then NU is a subgroup of G.*
- **(c)** *If N is a normal subgroup of G and U a subgroup of G, then $N \cap U$ is a normal subgroup of U.*
- **(d)** *If N_1, N_2 are normal subgroups of G, then so is N_1N_2.*
- **(e)** *If N_1, N_2 are normal subgroups of G with $N_1 \cap N_2 = \{1\}$, then $n_1n_2 = n_2n_1$ for all $n_1 \in N_1$ and $n_2 \in N_2$.*

Proof: **(a)** The subgroup property of the intersection is not an issue here. For the remaining property we immediately verify that

$$g(\bigcap_{i\in I} N_i)g^{-1} \;=\; \bigcap_{i\in I}(gN_ig^{-1}) \;=\; \bigcap_{i\in I} N_i.$$

(b) This follows from $NU = UN$ and 1.11.
(c) On the one hand we have $u(N \cap U)u^{-1} \subseteq N$ for all $u \in U$, since N is a normal subgroup of G. On the other hand it is trivial that $u(N\cap U)u^{-1} \subseteq U$, and this yields the claim.
(d) According to **(b)** we know that N_1N_2 is a subgroup of G. We then compute $gN_1N_2g^{-1} = gN_1g^{-1}gN_2g^{-1} = N_1N_2$ and this yields the claim.
(e) Let $n_1 \in N_1$ and $n_2 \in N_2$. Then on the one hand we have $n_1n_2n_1^{-1}n_2^{-1} \in N_2$, since $n_1n_2n_1^{-1}$ and n_2 are contained in N_2. On the other hand we have $n_1n_2n_1^{-1}n_2^{-1} \in N_1$, since n_1 and $n_2n_1^{-1}n_2^{-1}$ are contained in N_1. For this reason $n_1n_2n_1^{-1}n_2^{-1} \in N_1 \cap N_2 = \{1\}$ and this finishes the proof. □

Let's come to a further central aspect of this section: the quotient group.

Definition 1.19 Let N be a normal subgroup of the group G. Then according to the above the set $G/N := \{gN \mid g \in G\}$ together with the operation

$$G/N \times G/N \longrightarrow G/N,\ (gN, hN) \mapsto ghN$$

is a group. This group is called the quotient group of G by N and its identity is given by $1N = N$. For $g \in G$ the inverse of gN in G/N is given by $g^{-1}N$.

If G is Abelian, then so are N and G/N the converse of which however is not true in general. If G is finite then so are N and G/N, and by Lagrange's theorem (cf. 1.13) we have $|G/N| = [G : N] = \frac{|G|}{|N|}$.

Definition 1.20 Let G and H be groups. A mapping $\alpha : G \longrightarrow H$ is called a group homomorphism, if $\alpha(gh) = \alpha(g)\alpha(h)$, for all $g, h \in G$. If α is injective (surjective, bijective), then we call α monomorphism (epimorphism, isomorphism). If there exists an isomorphism of G onto H, then G and H are called isomorphic, and we write $G \cong H$. The set of all homomorphisms of G into H is denoted by $\mathrm{Hom}(G, H)$. Similar definitions are left to the reader for for the set $\mathrm{End}(G)$ of all endomorphisms of G and for $\mathrm{Aut}(G)$ the set of all automorphisms of G.

The proof of the following lemma is easy, so we omit it.

Lemma 1.21 *Let* $\alpha : G \longrightarrow H$ *be a group homomorphism.*

(a) *There holds* $\alpha(1_G) = 1_H$ *and* $\alpha(g^{-1}) = (\alpha(g))^{-1}$ *for all* $g \in G$.

(b) $\mathrm{Im}(\alpha) := \{\alpha(g) \mid g \in G\}$ *is a subgroup of* H.

(c) $\mathrm{Ker}(\alpha) := \{g \in G \mid \alpha(g) = 1_H\}$ *is a normal subgroup of* G.

Now we are ready to state the homomorphism theorem:

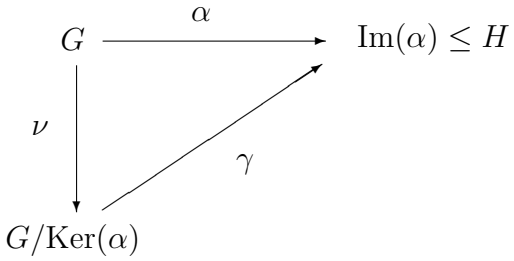
Theorem 1.22 *Let* $\alpha : G \longrightarrow H$ *be a group homomorphism. Then there holds*

$$G/\mathrm{Ker}(\alpha) \;\cong\; \mathrm{Im}(\alpha).$$

Proof: We are looking for an isomorphism $\gamma : G/\mathrm{Ker}(\alpha) \longrightarrow \mathrm{Im}(\alpha)$ and define $\gamma(g\mathrm{Ker}(\alpha)) := \alpha(g)$. This is well-defined because for different g, g' with $g\mathrm{Ker}(\alpha) = g'\mathrm{Ker}(\alpha)$ we have $g'^{-1}g \in \mathrm{Ker}(\alpha)$ and hence immediately $\alpha(g'^{-1}g) = 1_H$ which implies $\alpha(g') = \alpha(g)$. The homomorphism property results from $\gamma(g\mathrm{Ker}(\alpha)h\mathrm{Ker}(\alpha)) = \gamma(gh\mathrm{Ker}(\alpha)) = \alpha(gh) = \alpha(g)\alpha(h) = \gamma(g\mathrm{Ker}(\alpha))\gamma(h\mathrm{Ker}(\alpha))$ for all $g, h \in G$. Now obviously γ is surjective; regarding injectivity we keep in mind that $\gamma(g\mathrm{Ker}(\alpha)) = \gamma(g'\mathrm{Ker}(\alpha))$ immediately implies $\alpha(g) = \alpha(g')$ and therefore $g'^{-1}g \in \mathrm{Ker}(\alpha)$. Hence, $g\mathrm{Ker}(\alpha) = g'\mathrm{Ker}(\alpha)$. □

Remark 1.23 **(a)** For a normal subgroup N of a group G we finally mention the so-called natural epimorphism $G \longrightarrow G/N,\ g \mapsto gN$.

(b) In light of **(a)** we can say that the above homomorphism theorem proves the existence of γ, for which the following diagram commutes.:



Let us discuss two further isomorphy relations which will turn out to be very useful for our later considerations.

Theorem 1.24 *Let* G *be a group, and let* U, N *and* M *be subgroups of* G.

(a) *If* N *is normal in* G, *then so are* N *in* UN *and* $U \cap N$ *in* U, *and there holds* $UN/N \cong U/(U \cap N)$.

(b) *If* M *and* N *are normal in* G *and* $M \leq N$, *then* M *is normal in* N *and there hold* $N/M \trianglelefteq G/M$ *and* $(G/M)/(N/M) \cong G/N$.

Proof: **(a)** We consider the mapping

$$\alpha : UN \longrightarrow U/(U \cap N), \quad un \mapsto u(N \cap U),$$

which is certainly surjective provided we make sure that it is well-defined. For this keep in mind that from $un = u'n'$ we get $u^{-1}u' = nn'^{-1} \in U \cap N$ and hence $u(U \cap N) = u'(U \cap N)$. If we show that α is a homomorphism with $\mathrm{Ker}(\alpha) = N$ then an application of the homomorphism theorem will yield to our claim. α being multiplicative is easy to verify. If now $g = un \in \mathrm{Ker}(\alpha)$ for some $u \in U$ and $n \in N$, then $u \in U \cap N \subseteq N$ which means $g \in N$. If on the other hand $g \in N$, then, via $g = 1g$, we get immediately $\alpha(g) = \alpha(1) = U \cap N$, which shows $\mathrm{Ker}(\alpha) = N$.
(b) We first observe that clearly $M \trianglelefteq N$. If we find a group epimorphism $\beta : G/M \longrightarrow G/N$, the kernel of which is N/M then we get all claims by 1.21 and the homomorphism theorem. Consider

$$\beta : G/M \longrightarrow G/N, \quad gM \mapsto gN.$$

This mapping is clearly well-defined because $\beta(gM) = (gM)N = gN$. Multiplicativity and surjectivity are easy to verify as well. Let us finally determine $\mathrm{Ker}(\beta)$. If $N = \beta(gM) = gN$, then certainly $g \in N$, which means $gM \in N/M$. If on the other hand $gM \in N/M$, then by $g \in N$ we immediately get $\beta(gM) = gN = N$, and hence we see that $\mathrm{Ker}(\beta) = N/M$. □

It might be instructive for a later application that the set of all normal subgroups of a group together with its natural order (set inclusion) satisfies the so-called modular law, also called the Dedekind identity in various places.

Proposition 1.25 *Let* A, B *and* C *be normal subgroups of a group* G *with* $A \leq C$. *Then there holds*

$$(AB) \cap C = A(B \cap C).$$

Proof: First observe that as $A \leq C$ and $B \cap C \leq C$ we immediately get the trivial inclusion $A(B \cap C) \leq C$. Furthermore we have $A \leq AB$ and $B \cap C \leq B \leq AB$, which leads to $(AB) \cap C \geq A(B \cap C)$. For the converse inclusion let $g \in (AB) \cap C$ be given. Then $g = ab$ for suitable $a \in A \cap C$ and $b \in B$, and hence $b = a^{-1}g \in C$. But this means that $b \in B \cap C$, by which we immediately obtain $g = ab \in A(B \cap C)$. □

Definition 1.26 Let $((G_i, \cdot_i, 1_i))_{i\in I}$ be a non-empty family of groups. The Cartesian product

$$\prod_{i\in I} G_i \;=\; \{(g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \in I\}$$

obtains the structure of a group by coordinatewise multiplication. We write $\prod_{i\in I}(G_i, \cdot_i, 1_i)$ and more often $\prod_{i\in I} G_i$ because there will be no danger of ambiguity. A prominent normal subgroup in this group is the so-called direct sum

$$\bigoplus_{i\in I} G_i \;:=\; \{(g_i)_{i\in I} \mid g_i \in G_i \text{ and } g_i = 1_i \text{ for all but finitely many } i \in I\}.$$

Note, that for a finite index set there is no difference between the direct product and the direct sum of groups. Let us restrict ourselves to this case and consider the embedding

$$\begin{aligned} \iota_j : G_j &\longrightarrow \prod_{i=1}^{n} G_i \\ g &\mapsto (1, \ldots, g, \ldots, 1), \end{aligned}$$

where g is in the jth position of the n-tuple. It is easy to verify the following statements.

Lemma 1.27 **(a)** $G_j \cong \mathrm{Im}(\iota_j) \trianglelefteq \prod_{i=1}^{n} G_i$ *for all* $j \in \{1, \ldots, n\}$.

(b) $\mathrm{Im}(\iota_j) \cap (\mathrm{Im}(\iota_1) \cdots \mathrm{Im}(\iota_{j-1})\mathrm{Im}(\iota_{j+1}) \cdots \mathrm{Im}(\iota_n)) = \{(1_1, \ldots, 1_n)\}$ *for all* $j \in \{1, \ldots, n\}$.

This justifies the following definition.

Definition 1.28 Let $N_1, \ldots, N_n$ be a family of normal subgroups of a group G. We call G the (inner) product of the N_i, formally $G = \bigoplus_{i=1}^{n} N_i = N_1 \oplus \ldots \oplus N_n$, if the following hold:

(i) $G = N_1 \cdots N_n$.

(ii) For all $i \in \{1, \ldots, n\}$ there holds $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_n) = \{1\}$.

According to this definition we see that the above (outer) product of a family of groups G_i is the same as the inner product of the $\mathrm{Im}(\iota_i)$. We now give another isomorphism relation which the reader might extend immediately to a finite number of components.

Lemma 1.29 *Let* A_1, A_2, B_1, B_2 *be normal subgroups of a group* G *with* $B_1 \leq A_1$ *and* $B_2 \leq A_2$ *and finally* $A_1 \cap A_2 = \{1\}$. *Then* $B_1 \oplus B_2$ *is a normal subgroup in* $A_1 \oplus A_2$ *and there holds*

$$(A_1 \oplus A_2)/(B_1 \oplus B_2) \cong (A_1/B_1) \oplus (A_2/B_2).$$

Proof: Consider the mapping

$$\varphi : A_1 \oplus A_2 \longrightarrow A_1/B_1 \oplus A_2/B_2, \quad (a_1, a_2) \mapsto (a_1 + B_1, a_2 + B_2).$$

We leave it to the reader to prove that this mapping is an epimorphism and that its kernel is given by $B_1 \oplus B_2$. Our claim then follows by application of the homomorphism theorem. □

1.2 Abelian Groups

In order to completely study the structure of all (finitely generated) Abelian groups, we first need to understand their elementary components, namely the cyclic groups.

Definition 1.30 A group G is called cyclic, if it possesses a one-element generating system, i.e. if there is $g \in G$ such that $G = \langle \{g\} \rangle$. Such an element will be called a generator of G.

Examples 1.31 **(a)** The group $(\mathbb{Z}, +, 0)$ is an infinite cyclic group. It possesses the generating elements 1 and -1.

(b) For $n \in \mathbb{N}$ the group $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ is a cyclic group of order n. All elements $k \in \mathbb{N}$ with $\gcd(k, n) = 1$ are generating elements of $\mathbb{Z}_n$.

The foregoing list is complete, as we can see in theorem 1.33. To get prepared we have a look at the following statement.

Lemma 1.32 *The subgroups of* $(\mathbb{Z}, +, 0)$ *are of the form* $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.

Proof: Let U be a subgroup of $\mathbb{Z}$. If $U \neq \{0\}$ then there exists a non-zero element n of smallest absolute value in U. For every further element $u \in U$ we apply the division algorithm in $\mathbb{Z}$ and find $u = kn + r$ for suitable $k, r \in \mathbb{Z}$ with $|r| < |n|$. This however enforces $r = 0$ because $r = u - kn \in U$ and n was smallest possible in terms of absolute value. Hence we have $u = kn$. □

Theorem 1.33 *Let* G *be a cyclic group.*

(a) *If* $|G| = \infty$, *then* $G \cong \mathbb{Z}$.

(b) *If* $|G| < \infty$, *then* $G \cong \mathbb{Z}/n\mathbb{Z}$ *for a suitable* $n \in \mathbb{N}$.

Proof: We have $G = \{g^i \mid i \in \mathbb{Z}\}$ for some generating element g of G. Consider the mapping $\alpha : \mathbb{Z} \longrightarrow G,\ i \mapsto g^i$, which is an epimorphism, and distinguish two possible

cases: If $\mathrm{Ker}(\alpha) = \{0\}$, then $G \cong \mathbb{Z}$. Otherwise we have according to the foregoing lemma $\mathrm{Ker}(\alpha) = n\mathbb{Z}$ for some $n \in \mathbb{N}$ and the homomorphism theorem yields $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Let us characterize all subgroups of a given cyclic group. For the case of infinite order we already have done this in 1.32: every subgroup U of a cyclic group $G = \langle\{g\}\rangle$ of infinite order is of the form $U = \langle\{g^n\}\rangle$ for some fixed $n \in \mathbb{N}$. The subgroups of a cyclic group of finite order allow for a similarly simple characterization.

Proposition 1.34 *Let G be a cyclic group of order n with generator g. For every divisor d of n there exists exactly one (cyclic) subgroup of order d, and the list of these are all subgroups of G.*

Proof: We first observe that every subgroup of G must be cyclic, because G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and this latter group as a quotient group of $\mathbb{Z}$ has only cyclic subgroups because $\mathbb{Z}$ only has subgroups of this type. If now d is a divisor of n and $c := n/d$, then consider the subgroup $U_d := \langle\{g^c\}\rangle$. As $g^{cd} = g^n = 1$ we see that the order of g^c must divide d. If b is the order of g^c and $b < d$ then $1 = g^{cb} = g^{nb/d}$ and as $nb/d < n$ we would have that the order of g is smaller than n, a contradiction. Hence $b = d$ and so we see $|U_d| = d$. Let now $U = \langle\{g^k\}\rangle$ be some arbitrary subgroup of order d where the order of g^k is (clearly) d. Then we get from $g^{kd} = 1$ immediately $n \mid kd$ and hence $kd = nm$ for suitable $m \in \mathbb{N}$. This however implies $g^k = g^{(n/d)m} \in U_d$ and hence $U \leq U_d$ which implies equality for cardinality reasons. □

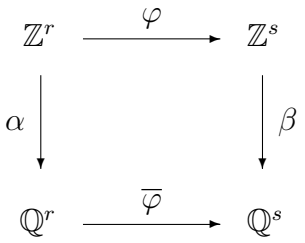
We have just understood that the structure of all cyclic group is completely known. We are now interested in how far this knowledge can be used for the study of more general Abelian groups. In order to do this we first focus on what are called free Abelian groups.

Definition 1.35 A group G is called free Abelian group, if $G \cong \bigoplus_{i \in I} \mathbb{Z}$ for some index set I, i.e. if G is a direct sum of infinite cyclic subgroups of G. A collection of generators of these subgroups is called a basis of G. If $|I| = r < \infty$, we say G is of rank r.

In the following we will see that the rank of a free Abelian group is uniquely determined.

Lemma 1.36 *If G is a free Abelian group of ranks r and s, then $r = s$.*

Proof: Our claim of two different ranks r and s yields an isomorphism $\varphi : \mathbb{Z}^r \longrightarrow \mathbb{Z}^s$. Let α and β be the natural embeddings of $\mathbb{Z}^r$ (resp. $\mathbb{Z}^s$) into the respective direct sums of copies of $\mathbb{Q}$. We will extend φ to a vector space isomorphism $\overline{\varphi} : \mathbb{Q}^r \longrightarrow \mathbb{Q}^s$, in such a way, that the following diagram commutes.



We give here the steps that have to be performed as homework:

(a) Show that for every $x \in \mathbb{Q}^n$ there exists $z \in \mathbb{Z}$ such that $zx \in \mathbb{Z}^n$.

(b) Define $\overline{\varphi} : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$ by $x \mapsto \frac{1}{z}\,\varphi(zx)$ where z is the number that you found in **(a)**. Show that this mapping is well-defined.

(c) Show that $\overline{\varphi}$ is additive and (hence) $\mathbb{Z}$-linear; then show that $\overline{\varphi}$ is $\mathbb{Q}$-linear.

(d) Show that $\overline{\varphi}$ is one-to-one. Show that $\overline{\varphi}$ is onto.

The mapping $\overline{\varphi}$ being a vector space isomorphism enforces that $r = s$, and hence we have obtained our claim. □

We will return to the following statement in the context of the theory of rings and modules.

Proposition 1.37 *Every Abelian group is the homomorphic image of a free Abelian group.*

Proof: Let $\{g_i \mid i \in I\}$ be a generating set for the Abelian group G. Then the mapping

$$\pi : \mathbb{Z}^{(I)} \longrightarrow G, \quad (z_i)_{i\in I} \mapsto \sum_{i\in I, z_i \neq 0} z_i g_i$$

is the epimorphism that we are looking for. Note that by $\mathbb{Z}^{(I)}$ we mean the direct sum rather than the direct product! □

The foregoing proposition has revealed in particular that every finitely generated Abelian group is a homomorphic image of a free Abelian group of finite rank. The following statement is one of the central results of this section. It will help to completely characterize the structure of the finitely generated Abelian groups.

Theorem 1.38 *Let F be a free Abelian group of rank $r < \infty$ and U a subgroup of F. There exists a basis $\{b_1, \ldots, b_r\}$ of F and coefficients $\rho, \varepsilon_1, \ldots, \varepsilon_\rho \in \mathbb{N}$, such that $\{\varepsilon_1 b_1, \ldots, \varepsilon_\rho b_\rho\}$ forms a basis of U. In particular U itself is a free Abelian group of rank $\rho \leq r$.*

Proof: We are going to proceed by induction on the rank r. For $r = 1$ there remains nothing to show by an application of 1.32. Assume now that $r > 1$ and that the statement of this theorem has already been shown for all free Abelian groups of rank $< r$. Let U be a non-trivial subgroup, then the set of coefficients $z \in \mathbb{Z} \setminus \{0\}$ which occur in the representation of arbitrary elements of U with respect to an arbitrary basis of F is non-empty, and contains an element ε_1 that is minimal by absolute value. Attached to this element there is a basis $B_0 := \{w_1, \ldots, w_r\}$ of F and an element $u_0 \in U$ with $u_0 = \sum_{i=1}^{r} z_i w_i$, and after possible rearrangement of B_0 we may assume that $z_1 = \varepsilon_1$. We assume the order of the elements in B_0 to be fixed now, and vary the elements $u \in U$. Then we denote by $z_1(u)$ the coefficient in the representation of u that stands in front of w_1. The set $I_0 = \{z_1(u) \mid u \in U\}$ is a subgroup of $\mathbb{Z}$. This subgroup contains ε_1 which is its minimal element by absolute value. Consequently $I_0 = \varepsilon_1\mathbb{Z}$. In the linear combination $u_0 = \varepsilon_1 w_1 + z_2 w_2 + \ldots + z_r w_r$ we now divide the occuring coefficients with remainder by ε_1 and obtain

$$z_i = q_i\varepsilon_1 + s_i \text{ for } i = 2, \ldots, r \text{ and } q_i, s_i \in \mathbb{Z} \text{ with } 0 \leq s_i < \varepsilon_1.$$

Now also $B_i := \{w_1 + q_i w_i, w_2, \ldots, w_r\}$ is again a basis of F, and with respect to this basis our element u_0 has the representation

$$u_0 = \varepsilon_1(w_1 + q_i w_i) + z_2 w_2 + \ldots + s_i w_i + \ldots + z_r w_r.$$

Our assumption on ε_1 to be minimal by absolute value now enforces that $s_i = 0$ for all $i = 2, \ldots, r$, and hence we have $u_0 = \varepsilon_1 b_1$ with $b_1 = w_1 + q_2 w_2 + \ldots + q_r w_r$. Now $\{b_1, w_2, \ldots, w_r\}$ is again a basis of F and because of $I_0 = \mathbb{Z}\varepsilon_1$ we first have

$$U \;\leq\; \mathbb{Z}\varepsilon_1 b_1 + \mathbb{Z}w_2 + \ldots + \mathbb{Z}w_r,$$

which yields

$$U \;=\; (\mathbb{Z}\varepsilon_1 b_1 + \mathbb{Z}w_2 + \ldots + \mathbb{Z}w_r) \cap U \;=\; \mathbb{Z}\varepsilon_1 b_1 \oplus (\mathbb{Z}w_2 + \ldots + \mathbb{Z}w_r) \cap U,$$

by the Dedekind Identity. This shows, that we can write $U = \mathbb{Z}\varepsilon_1 b_1 \oplus U_1$ where U_1 is a subgroup of the free Abelian group $F_1 := \mathbb{Z}w_2 + \ldots + \mathbb{Z}w_r$ that is of rank $r-1$. By induction, there exist $\rho, \varepsilon_2, \ldots, \varepsilon_\rho \in \mathbb{N}$, and a basis $\{c_2, \ldots, c_r\}$ of F_1, such that $\{\varepsilon_2 c_2, \ldots, \varepsilon_\rho c_\rho\}$ is a basis of U_1. All in all we obtain $\{\varepsilon_1 b_1, \varepsilon_2 c_2, \ldots, \varepsilon_\rho c_\rho\}$ to be a basis of U, and this completes the induction. □

We now come to the main result of this paragraph.

Theorem 1.39 *Every finitely generated Abelian group decomposes as a direct sum of (finitely many) cyclic subgroups.*

Proof: If $\alpha : F \longrightarrow G$ denotes the epimorphism that we found in 1.37 then we may assume (as indicated earlier) that F is of finite rank r. By homomorphism theorem we then get $F/\mathrm{Ker}(\alpha) \cong G$. According to the previous theorem we then obtain a basis $\{b_1, \ldots, b_r\}$ of F and natural numbers $\rho, \varepsilon_1, \ldots, \varepsilon_\rho$ with $\rho \leq r$ such that $\{\varepsilon_1 b_1, \ldots, \varepsilon_\rho b_\rho\}$ forms a basis of $\mathrm{Ker}(\alpha)$. All in all we then obtain

$$G \;\cong\; (\bigoplus_{i=1}^{r} \mathbb{Z}b_i)/(\bigoplus_{i=1}^{\rho} \mathbb{Z}\varepsilon_i b_i) \;\cong\; (\bigoplus_{i=1}^{\rho} \mathbb{Z}b_i/\mathbb{Z}\varepsilon_i b_i) \;\oplus\; (\bigoplus_{i=\rho+1}^{r} \mathbb{Z}b_i)$$

which was our claim. □

From here there naturally arises the question in how far the foregoing decomposition can be beautified. An important tool will be the following statement which is also known as the Chinese Remainder Theorem. Its generalization from 2 components to general n components is left as an exercise.

Proposition 1.40 *Let n, k be coprime natural numbers. Then*

$$\mathbb{Z}/nk\mathbb{Z} \;\cong\; (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/k\mathbb{N}).$$

Proof: We consider the homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}, \quad z \mapsto (z + n\mathbb{Z}, z + k\mathbb{Z}).$$

Careful inspection shows that this is an epimorphism, and we compute its kernel as $n\mathbb{Z} \cap k\mathbb{Z} = nk\mathbb{Z}$, which finally yields the claim by homomorphism theorem. □

Corollary 1.41 *Every cyclic group of order $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$ (where p_i are different primes, and k_i are natural numbers) is isomorphic to a direct product of the cyclic groups $\mathbb{Z}/p_i^{k_i}\mathbb{Z}$ for $i = 1, \ldots, \ell$.*

According to the previous statements we can arrange the cyclic groups occuring in the decomposition of an arbitrary finitely generated Abelian group by suitable prime powers.

Corollary 1.42 *Every finite Abelian group G is isomorphic to $\bigoplus_{i=1}^{n} U_{p_i}$ with $|U_{p_i}| = p_i^{s_i}$, and each of these U_{p_i} is of the form $U_{p_i} \cong \mathbb{Z}/p_i^{k_1} \oplus \ldots \oplus \mathbb{Z}/p_i^{k_{\ell_i}}\mathbb{Z}$ where $\sum_{j=1}^{\ell_i} k_j = s_i$.*

Remark 1.43 It might be plausible that the decomposition that we just discussed is unique up to isomorphism and arrangement of the components. We will omit a more careful proof of this statement and finish our analysis with an example.

Example 1.44 Determine all non-isomorphic Abelian groups of order 9000.

1.3 p-Groups and Sylow's Theorems

Definition 1.45 Let G be a group and M a set. An action of G on M is a group homomorphism $\alpha : G \longrightarrow S(M)$, where $S(M)$ is the set of all permutations of M. We call this action faithful if α is a monomorphism.

Examples 1.46 Let G be a group and g an element of G.

(a) The so-called left translation $\tau_g : G \longrightarrow G$ with $x \mapsto gx$ is a permutation on G. Therefore $\tau : G \longrightarrow S(G)$ with $g \mapsto \tau_g$ is an action of G on itself.

(b) The so-called conjugation $c_g : G \longrightarrow G$ with $x \mapsto gxg^{-1}$ is an automorphism (and hence a permutation) of G. Hence $c : G \longrightarrow \mathrm{Aut}(G) \subseteq S(G)$ with $g \mapsto c_g$ is an action of G on itself.

In the following we will identify the image of an action with the group, since ambiguity will not occur. This means we will write $g(x)$ for $\alpha(g)(x)$.

Definition 1.47 Let the group G act on the set M. The orbit of an element $m \in M$ is given by $Gm := \{g(m) \mid g \in G\}$, and the stabilizer of m in G is defined as $G_m := \{g \in G \mid g(m) = m\}$. Furthermore, $F(g)$ will denote the set $\{m \in M \mid g(m) = m\}$, i.e. the set of fixed points of an element $g \in G$.

The following statement rules the relation between certain cardinalities.

Lemma 1.48 *Let the finite group G act on the set M. Then*

$$|Gx| \cdot |G_x| \;=\; |G|$$

for all $x \in M$.

Proof: For given $x, y \in M$ let $G(x \to y) := \{g \in G \mid g(x) = y\}$ denote the set of permutations that carry x to y. For a particular permutation g with $g(x) = y$ we claim the identity $G(x \to y) = gG_x$. For a proof let $h \in G(x \to y)$. Then $g^{-1}h(x) = x$, and hence $g^{-1}h \in G_x$ which shows that $h \in gG_x$. If conversely $h \in gG_x$ then $h = gu$ for some $u \in G_x$ and hence $h(x) = gu(x) = g(x) = y$ which shows that $h \in G(x \to y)$. Using this identity we immediately find for given $\in M$ that

$$|G| \;=\; |\{(g, y) \in G \times M \mid g(x) = y\}| \;=\; \sum_{y \in Gx} |G(x \to y)| \;=\; \sum_{y \in Gx} |G_x| = |Gx| \cdot |G_x|,$$

which proves the claim. □

The following statement (Burnside's lemma) gives information about the number of distinct orbits of G in M.

Proposition 1.49 *Let the finite group G act on the finite set M. The number ω of orbits of G in M satisfies:*

$$\omega \;=\; \frac{1}{|G|}\sum_{g\in G} F(g).$$

In words: the number of all orbits is given by the average size of the fixed point sets which belong to the elements of G.

Proof: We consider the set $E := \{(g,x) \in G \times M \mid g(x) = x\}$. Its cardinality is given by $\sum_{g\in G} |F(g)|$ which is easy to see by fixing the left entry of such a pair and then counting the number of admissible right entries. Repeating the same procedure by first fixing the right entry and counting the number of admissible left entries, we obtain $|E| = \sum_{x\in M} |G_x|$ and hence the identity

$$\sum_{g\in G} |F(g)| \;=\; \sum_{x\in M} |G_x|.$$

We now partition the set M into orbits, i.e. we write $M = \bigcup_{i=1}^{\omega} Gx_i$ for suitable $x_1, \ldots, x_\omega \in M$. Observing $|G_z| = |G_{x_i}|$ for each $z \in Gx_i$ we then find

$$\sum_{x\in M} |G_x| \;=\; \sum_{i=1}^{\omega} |Gx_i| \cdot |G_{x_i}| \;=\; \omega\,|G|$$

and this finally yields the desired identity. □

Example 1.50 We again look at the conjugation action that we introduced in 1.46, i.e. we consider $c : G \longrightarrow \mathrm{Aut}(G)$. For each $x \in G$ the orbit $Gx = \{gxg^{-1} \mid g \in G\}$ is also called conjugacy class of x in G. It is a singleton if and only if $gxg^{-1} = x$ for all $g \in G$, i.e. if x is an element of the center $C(G)$ of G. From this we immediately obtain the so-called class equation of the group G:

$$|G| = |C(G)| + (n_1 + \ldots + n_k),$$

where the n_i denote the sizes of the non-singleton conjugacy classes. According to 1.48 we have $n_i \mid |G|$ for all $i = 1, \ldots, k$ which has nice applications in combinatorial group theory.

Proposition 1.51 *Let p be a prime and $r \geq 1$ an integer. Then the center of a finite group of order p^r can never be trivial (singleton).*

Proof: The class equation for that group shows $p^r - (n_1 + \ldots + n_k) = |C(G)|$, where all the n_i are non-trivial divisors of p^r. For this reason we find $|C(G)| \equiv 0 \pmod{p}$ which yields the claim. □

We can improve the preceeding argumentation and give the following fundamental lemma which will turn out to be a key step for all further statements.

Lemma 1.52 *(Fundamental Lemma:) Let G be a group of order p^n where p is a prime. Assume G acts on a finite set M, and define $M_0 := \{m \in M \mid g(m) = m \text{ for all } g \in G\}$ to be the set of all fixed points of the action. Then there holds*

$$|M_0| \equiv |M| \pmod{p}.$$

Proof: Certainly M is the disjoint union of all orbits of G in M. Similar to the class equation we therefore have $|M| = |M_0| + |Gx_1| + \ldots + |Gx_k|$, where M_0 is the union of all one-element orbits and $x_1, \ldots, x_k$ are suitable representatives of all larger orbits. As $|Gx_i| > 1$ and $|Gx_i| \mid p^n$ we then find $p \mid |Gx_i|$, and this immediately leads to the fact that $|M| \equiv |M_0| \pmod{p}$. □

Recalling Lagrange's theorem we might find the following statement interesting.

Proposition 1.53 *(Cauchy's Theorem:) For a finite group G and a prime divisor p of $|G|$ there always exists an element $g \in G$ with $\mathrm{o}(g) = p$. In particular for each prime divisor of the group order there exists a subgroup of that prime order.*

Proof: Consider the set $M := \{(a_1, \ldots, a_p) \mid a_i \in G, \quad \prod_{i=1}^p a_i = 1\}$, for which certainly $|M| = |G|^{p-1}$. On M we let $\mathbb{Z}/p\mathbb{Z}$ act by cyclic permutation, i.e. we consider the action

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow S(M), \; z \mapsto \mathrm{shift}_z$$

where $\mathrm{shift}_z : M \longrightarrow M$, $(a_1, \ldots, a_p) \mapsto (a_{z+1}, \ldots, a_p, a_1, \ldots, a_z)$. This definition makes sense because from $1 = \prod_{i=1}^p a_i = (a_1 \cdots a_z)(a_{z+1} \cdots a_p)$ we obtain via 1.2 immediately $(a_{z+1} \cdots a_p)(a_1 \cdots a_z) = 1$. The set of fixed points under this action is given by $M_0 := \{(a, \ldots, a) \mid a \in G \text{ and } a^p = 1\}$. According to the fundamental lemma we have $|M_0| \equiv |M| \pmod{p}$, and because of $(1, \ldots, 1) \in M_0$ we clearly have $|M_0| \neq 0$. For this reason we find $g \in G$ with $g \neq 1$ such that $(g, \ldots, g) \in M_0$ and hence $g^p = 1$. □

Definition 1.54 Let p be a prime. We say a group G is a p-group if the order of each of its elements is a power of p.

According to Lagrange's theorem we know that every group of order p^n must be a p-group. The foregoing theorem of Cauchy gives the converse, i.e. we obtain the following corollary.

Corollary 1.55 *A finite group is a p-group if and only its order is a power of p.*

We are interested in the p-subgroups of finite groups. The most important statements regarding this topic are Sylow's theorems which we will prepare in the following.

Definition 1.56 A Sylow p-subgroup of a group G is a maximal p-subgroup of G.

Remark 1.57 The existence of Sylow p-subgroups does not require a proof in case of finite groups. In the general case it can be proved by an application of Zorn's lemma. We will return to this issue in a later chapter.

The following statement is easy to prove and will be left as an exercise.

Lemma 1.58 *If G is a group and p a prime number then every conjugate of a Sylow p-subgroup is a Sylow p-subgroup. If G possesses just one Sylow p-subgroup then this subgroup must be a normal subgroup of G.*

The following statement and its consequences form the key for a proof of Sylow's theorems.

Proposition 1.59 *Let U be a p-subgroup of the finite group G and let $N_G(U) := \{g \in G \mid gU = Ug\}$ be its normalizer. Then there holds*

$$[N_G(U) : U] \equiv [G : U] \pmod{p}.$$

Proof: We let U act on the set $M := \{gU \mid g \in G\}$ of all left cosets of U in G by left translation, i.e. $u(gU) := ugU$ for all $u \in U$. The set M_0 of all fixed points of this action is given by

$$\begin{aligned} M_0 &= \{gU \mid g \in G \text{ and } ugU = gU \text{ for all } u \in U\} \\ &= \{gU \mid g \in G \text{ and } g^{-1}ug \in U \text{ for all } u \in U\} \\ &= \{gU \mid g \in N_G(U)\} \;=\; N_G(U)/U. \end{aligned}$$

Hence we have $|M_0| = [N_G(U) : U]$ and as $|M| = [G : U]$ we get the claim from the fundamental lemma. □

Corollary 1.60 *If U is a p-subgroup of the finite group G with $p \mid [G : U]$, then there holds $N_G(U) > U$.*

Proof: This is an immediate consequence of the foregoing statement and taking into consideration that $|N_G(U)| \geq 1 > 0$. □

We are now able to prove the famous Sylow theorems. They form a key component of non-commutative finite group theorey and show the power of elementary combinatorial concepts and methods in the context of Modern Algebra.

Theorem 1.61 *(Sylow's first theorem:) Let G be a group of order $p^n m$ where p is a prime that does not divide m.*

- **(a)** *For each $i \in \{0, \ldots, n\}$ there is a subgroup of G of order p^i. For this reason G possesses Sylow p-subgroups of order p^n.*
- **(b)** *Every subgroup of order p^i of G is normal in a subgroup of order p^{i+1} of G for $i = 0, \ldots, n-1$.*

Proof: We assume that $n > 0$. According to Cauchy's theorem G contains a subgroup of order p. We will proceed by induction and assume that we have already shown that G contains a subgroup U of order p^i for an $i \in \{1, \ldots, n-1\}$. Then $[G : U] = p^{n-i}m$, and by 1.60 we find $[N_G(U) : U] \equiv [G : U] \equiv 0 \pmod{p}$ which means that $N_G(U)/U$ contains a subgroup U'/U of order p by Cauchy's theorem. For this reason we see that U' is a p-subgroup of order p^{i+1} of G namely by considering $|U'| = |U'/U| \cdot |U|$ and certainly U is normal in U'. □

We have just understood the existence of p-subgroups of a finite group, and that these p-subgroups form maximal ascending chains of subgroups. The foregoing theorem has shown in particular that the Sylow p-subgroups, i.e. the maximal p-subgroups are at the same time the p-subgroups of maximal order. The following second theorem of Sylow will complement our statements in 1.58 and discuss the relationship between the different Sylow p-subgroups.

Theorem 1.62 *(Sylow's second theorem:) If U is a p-subgroup of the finite group G and P is a Sylow p-subgroup then there exists $g \in G$ such that $gUg^{-1} \subseteq P$. In particular every pair of Sylow p-subgroups is conjugated.*

Proof: We let U act on the set $M := \{gP \mid g \in G\}$ by left translation and like before we have the set of fixed points under this action as $M_0 := \{gP \mid g \in G,\, ugP = gP \text{ for all } u \in U\} = \{gP \mid g \in G,\, g^{-1}Ug \subseteq P\}$. According to the fundamental lemma we again have $|M_0| \equiv |M| \not\equiv 0 \pmod{p}$, as by maximality of P the number p cannot divide $[G : P]$. Hence M_0 is non-empty, i.e. there exists $g \in G$ with $g^{-1}Ug \subseteq P$. The second claim is an immediate consequence. □

Sylow's third theorem gives us some information about the number of different Sylow p-subgroups of a finite group.

Theorem 1.63 *(Sylow's third theorem:) The number s_p of Sylow p-subgroups of a finite group G satisfies the equations*

$$|G| \equiv 0 \pmod{s_p} \qquad \textit{and} \qquad s_p \equiv 1 \pmod{p}.$$

Proof: According to Sylow's second theorem we know that s_p is the length of the orbit of a fixed Sylow p-subgroup under the conjugation action. From this we immediately obtain via 1.48 that $s_p \mid |G|$. On the set $M := \{Q \mid Q \text{ is a Sylow } p\text{-subgroup of } G\}$ we let a fixed Sylow p-subgroup P act by conjugation. Again we consider the set M_0 of fixed points of this action and find $M_0 = \{Q \in M \mid aQa^{-1} = Q \text{ for all } a \in P\}$. This however means that $Q \in M_0$ if and only if $P \leq N_G(Q)$. But P, Q being Sylow p-subgroups of G are also Sylow p-subgroups of $N_G(Q)$. This implies, as Q is normal in $N_G(Q)$, immediately by 1.62 equality of P and Q. For this reason we have $M_0 = \{P\}$ which means $|M_0| = 1$ and hence via $|M| = s_p$ we obtain the claim by application of the fundamental lemma. □

1.4 Solvable Groups

In the preceeding sections we have discussed Abelian and non-Abelian groups, and our discussions have shown how strong commutativity is, and how particular the class of all Abelian group therefore is. For this reason there arises the question in how far there are close relatives of the Abelian groups within the class of all groups. This will lead us to the so-called solvable groups, a class of groups that play a central role in the question of how certain algebraic equations can be solved by radicals.

Definition 1.64 A group G is called solvable if there is a chain

$$\{1\} = N_0 \subset N_1 \subset \ldots \subset N_{\ell-1} \subset N_\ell = G$$

of subgroups for which N_{i-1} is normal in N_i and N_i/N_{i-1} is Abelian for $i = 1, \ldots \ell$. Such a chain will be called an Abelian normal series.

It is obvious that Abelian groups are always solvable. Furthermore non-Abelian simple groups are certainly non-solvable.

We will now see in how far the class of all solvable group is closed under subgroups and epimorphic images.

Proposition 1.65 *Every subgroup and every quotient group of a solvable group is solvable.*

Proof: Let U be a subgroup of the solvable group G and let $\{1\} = N_0 \subset \ldots \subset N_\ell = G$ a chain like that of 1.64, then the subgroups $M_i := U \cap N_i$ form a chain of subgroups of U, in which $U \cap N_{i-1}$ is normal in $U \cap N_i$. Using theorem 1.24 we furthermore get

$$\begin{aligned} M_i/M_{i-1} &= (U \cap N_i)/(U \cap N_{i-1}) \\ &= (U \cap N_i)/(U \cap N_i \cap N_{i-1}) \\ &\cong ((U \cap N_i) \cdot N_{i-1})/N_{i-1}, \end{aligned}$$

where the latter group as a subgroup of N_i/N_{i-1} must clearly be Abelian.
If now U is a normal subgroup of G then the above chain induces a new chain $M_i := (UN_i)/U$ of subgroups between U/U and G/U. As U is normal in G we see that U is also normal in UN_i for all $i = 0, \ldots, \ell$. Furthermore we can easily check that UN_{i-1} is normal in UN_i. Applying 1.24 to this situation we obtain first of all normality of UN_{i-1}/U in UN_i/U and furthermore

$$\begin{aligned} (UN_i/U)/(UN_{i-1}/U) &\cong UN_i/UN_{i-1} \\ &= (UN_{i-1}N_i)/(UN_{i-1}) \\ &\cong N_i/(N_i \cap (UN_{i-1}). \end{aligned}$$

According to the Dedekind identity the latter expression is isomorphic with $N_i/(N_{i-1}(U \cap N_i))$ which as a quotient group of the Abelian group N_i/N_{i-1} must again be Abelian. □

More is true, as the following statement shows:

Proposition 1.66 *Let N be a normal subgroup of the group G. Then G is solvable if and only if N and G/N are solvable.*

Proof: If G is solvable then by 1.65 we know that N and G/N are solvable. Conversely, if N and G/N are solvable then we find Abelian normal series $\{1\} = N_0 \subset \ldots \subset N_k = N$ of N and $\{N\} = N_k/N \subset \ldots \subset N_l/N = G/N$ of G/N where because of $(N_i/N)/(N_{i-1}/N) \cong N_i/N_{i-1}$ (in case of $i \geq k+1$), all N_i/N_{i-1} are Abelian for $(i = 1, \ldots, \ell)$. Hence we obtain our claim. □

The reader might be concerned by the question, how a normal series can be formed between N and G, when we are only given by N/N and G/N. For this observe that there is a bijection between the set of subgroups of G/N and the set of subgroups between N and G. Denote the former interval by $[N/N, G/N]$ and the latter by $[N, G]$, then we introduce

$$\varphi : [N, G] \longrightarrow [N/N, G/N], \quad U \mapsto U/N.$$

This mapping indeed satisfies $U \leq V$ if and only if $\varphi(U) \leq \varphi(V)$, and will clarify the above issue.

Proposition 1.67 *If N is a normal subgroup of the solvable group G, then there exists an Abelian normal series $\{1\} = N_0 \subset N_1 \subset \ldots \subset N_{\ell-1} \subset N_\ell = G$, that contains N, and in which all N_i/N_{i-1} are cyclic and of prime order.*

Proof: We can proceed exactly as in the proof of 1.66, and then obtain a chain with finite Abelian quotients. Between any two neighbours of this chain we put the normal series for finite Abelian groups and then we have obtained the desired normal series. □

The prime numbers that occur in the preceding theorem only depend on $|G|$. The according cyclic groups can be understood as smallest components of the structure of finite solvable groups. Such a decomposition in "atoms" can be proved in much more general context, although the structure of these atoms may then be quite different (simple groups). The finite solvable groups are exactly those in which the elementary components are cyclic groups of prime order.

Proposition 1.68 *Every finite p-group is solvable.*

Proof: We proceed by induction on n where $|G| = p^n$. For $n = 0$ or $n = 1$ we do not have to show anything. For larger n we observe that $\{1\} < C(G) \leq G$, because the center of a p-group is never trivial. If $C(G) = G$, then we are done, as the group is already Abelian. Otherwise $C(G)$ and $G/C(G)$ will be non-trivial p-groups of lower order. Hence $C(G)$ and $G/C(G)$ are both solvable, and this proves solvability of G by application of 1.66. □

We conclude this section with a remark of independent interest.

Remark 1.69 **(a)** The symmetric group S_n is not solvable for all $n \geq 5$. We will return to this fact in the next chapter.

(b) A (deep) theorem by Feit and Thompson says that all groups of odd order are solvable.

2 Rings, Fields, and Field Extensions

In this chapter we will deal with classical highlights of the theory of field extensions and their automorphisms. After discussing some preparational issues regarding polynomials we will come to algebraic field extensions and give examples of algebraic proofs for geometric impossibility results.

2.1 Polynomial Rings

Definition 2.1 A unital ring is a quintuple $(R, +, \cdot, 0, 1)$ usually denoted by R, in which $(R, +, 0)$ is an Abelian group and $(R, \cdot, 1)$ is a monoid[1] such that the following distributive laws hold:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

for all $a, b, c \in R$. Usually we omit the multiplication symbol $\cdot$ and write ab for $a \cdot b$. The ring R is called commutative, if $(R, \cdot, 1)$ is a commutative monoid; it is called a domain, if $ab = 0$ implies $a = 0$ or $b = 0$. A commutative ring is called a field, if each of its non-zero elements possesses a multiplicative inverse.

Examples 2.2 **(a)** Every field is a (commutative) domain.

(b) $(\mathbb{Z}, +, \cdot, 0, 1)$ is a commutative domain.

(c) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, 0, 1)$ is a commutative ring, but not a domain in general.

(d) $M_n(R)$, the set of all $(n \times n)$-matrices over the ring R is a ring again. This ring is commutative (and a domain), if and only if R is commutative (and a domain) and $n = 1$.

Let R be a ring. On the set

$$\bigoplus_{n \in \mathbb{N}} R := \{(r_n)_{n \in \mathbb{N}} \mid r_n \in R, r_n = 0 \text{ for all but finitely many } n \in \mathbb{N}\}$$

we define an addition $+$ coordinatewise, and a multiplication $*$ by $(a_n)_{n \in \mathbb{N}} * (b_n)_{n \in \mathbb{N}} = (c_n)_{n \in \mathbb{N}}$ with $c_n = \sum_{i=0}^{n} a_i b_{n-i}$. Abbreviating $\mathbf{0} := (0, 0, \ldots)$ and $\mathbf{1} := (1, 0, \ldots)$, we easily find that $(\bigoplus_{n \in \mathbb{N}} R, +, *, \mathbf{0}, \mathbf{1})$ is a unital ring. Here the element $x := (0, 1, 0, \ldots)$ has the property that $x^i = (0, 0, \ldots, 1, 0, \ldots)$, where 1 resides at the i-th position. For this reason the general element $a := (a_n)_{n \in \mathbb{N}}$ can also be written in the form

$$a = \sum_{i \in \mathbb{N}, a_i \neq 0} a_i x^i.$$

All in all the following definition makes sense:

[1] A monoid is a semigroup with identity.

Definition 2.3 Let R be a ring, then by the above motivation the set $R[x] := \{\sum_{i=0}^{n} r_i x^i \mid n \in \mathbb{N}, r_i \in R\}$ together with the operations

$$\begin{aligned} \sum_{i=0}^{n} r_i x^i + \sum_{i=0}^{n} s_i x^i &:= \sum_{i=0}^{n} (r_i + s_i) x^i \\ \sum_{i=0}^{n} r_i x^i * \sum_{j=0}^{k} s_j x^j &:= \sum_{i=0}^{n+k} (\sum_{j=0}^{i} r_j s_{i-j}) x^i \end{aligned}$$

is a unital ring which is called polynomial ring in the indeterminate x over R . The polynomial ring $R[x]$ is a (commutative) domain if and only if R is so. For $f := \sum_{i=0}^{n} f_i x^i \in R[x]$ with $f_n \neq 0$ we say n is the degree of f, denoted by $\deg(f)$ and agree on the convention that the degree of 0 is given by $-\infty$.

Lemma 2.4 *Let R be a ring and $f, g \in R[x]$.*

(a) *We have $\deg(f+g) \leq \max(\deg(f), \deg(g))$, where $\deg(f) \neq \deg(g)$ already implies equality.*

(b) *We have the inequality $\deg(fg) \leq \deg(f) + \deg(g)$ which turns into an equality, if and only if R is a domain.*

Proof: For **(a)** there is nothing to show and for **(b)** we observe that for $f = \sum_{i=0}^{n} f_i x^i$ and $g = \sum_{j=0}^{k} g_j x^j$ with $f_n \neq 0 \neq g_k$ we obtain via

$$fg = \sum_{i=0}^{n+k-1} (\sum_{j=0}^{i} f_j g_{i-j}) x^i + f_n g_k x^{n+k}$$

immediately our claim. □

Proposition 2.5 *(Division Algorithm) Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Then there are unique polynomials $q, r \in F[x]$ with $\deg(r) < \deg(g)$ uand $f = qg + r$.*

Proof: If $\deg(f) < \deg(g)$ then there is nothing to show because we can choose $q = 0$ and $r = f$. Otherwise we proceed by induction and define $n = \deg(f)$ and $k = \deg(g)$. We then find that

$$f' := f - \frac{f_n}{g_k} x^{n-k} g$$

is a polynomial of properly smaller degree than f. Accordingly we can apply the induction hypothesis and obtain $f' = q'g + r$ with suitable $q', r \in F[x]$ of the desired form. All in all

we therefore have

$$f = \frac{f_n}{g_k} x^{n-k} g + q'g + r = qg + r,$$

where we have set $q = \frac{f_n}{g_k} x^{n-k} + q'$, and this yields the claim. Regarding uniqueness we observe that if $f = qg + r = q'g + r'$, then $(q-q')g = r' - r$ and hence $\deg(g) > \deg(r'-r) = \deg((q-q')g) = \deg(q-q') + \deg(g)$. This clearly implies $r' - r = 0$ and hence we have $q - q' = 0$. □

The property that we have just studied has led to a name for an entire class of rings:

Definition 2.6 A commutative domain R is called Euclidean, if there is a mapping $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ with the following properties.

(i) $\varphi(ab) \geq \varphi(a)$ for all $a, b \in R \setminus \{0\}$.

(ii) For all $a, b \in R \setminus \{0\}$ there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

Examples 2.7 **(a)** Clearly, $(\mathbb{Z}, +, \cdot, 0, 1)$ equipped with the absolute value function is a Euclidean domain. The division algorithm is the usual algorithm that we know from school.

(b) If F is a field, then we see by 2.5 that $F[x]$ equipped with the deg-function is a Euclidean domain.

(c) The set $R = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ together with the operations inherited from $\mathbb{C}$ is a commutative domain. Defining $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ with $a + ib \mapsto a^2 + b^2$, we again find that R is a Euclidean domain. It is also called the ring of Gaussian numbers.

We will see soon that Euclidean domains have strong properties. To get prepared we need the following definition and lemmas.

Definition 2.8 Let $(R, +, \cdot, 0, 1)$ be a ring and S a subset of R. Then S is called left ideal of R if the following hold.

(i) $(S, +, 0)$ is a subgroup of $(R, +, 0)$.

(ii) For all $s \in S$ and $r \in R$ there holds $rs \in S$.

In an analogous way we can define right ideals as those subsets which are subgroups of $(R, +, 0)$ such that

(ii*) for all $s \in S$ and $r \in R$ there holds $sr \in S$.

If S satisfies both conditions (ii) and (ii*), then S is called a two-sided ideal. If $S = Rr$ for some $r \in R$ then S is generated by a single element and we call S a principal left ideal. Analogously we talk about right principal ideal and we clearly see that in a commutative ring these distinctions are not an issue. If in a ring R every left ideal is principal, then we call R a left principal ideal ring.

Obviously $0 = R0 = 0R$ and $R = R1 = 1R$ are always left and right principal ideals of a ring R. Additionally with every family $(S_i)_{i\in I}$ of left ideals of a ring R also $\bigcap_{i\in I} S_i$ and hence

$$\begin{aligned}\sum_{i\in I} S_i &:= \langle \bigcup_{i\in I} S_i \rangle \\ &= \bigcap \{S \mid S \leq {}_R R \text{ and } S \supseteq \bigcup_{i\in I} S_i\} \\ &= \{\sum_{i\in I_0} s_i \mid s_i \in S_i \text{ where } I_0 \text{ a finite subset of } I\},\end{aligned}$$

are left ideals of R. It might be intuitively clear that not every ideal of a ring is necessarily a principal ideal. However, looking for counterexamples one should however avoid the Euclidean domains as the following proposition shows:

Proposition 2.9 *Every Euclidean domain is a principal ideal domain.*

Proof: Let R be a Euclidean domain and let $\varphi : R \setminus \{0\} \longrightarrow \mathbb{N}$ be the attached function. If $S \neq \{0\}$ is an ideal of R then there exists a nonzero element $s_0 \in S$ on which φ takes its minimum. We have $Rs_0 \subseteq S$ and wish to show equality. Let $s \in S$ be an arbitrary element. By definition there exist elements $q, r \in R$ with $s = qs_0 + r$ where $\varphi(r) < \varphi(s_0)$ or $r = 0$. We have however $r = s - qs_0 \in S$, which by the above minimality enforces $r = 0$. Hence we see $s = qs_0$ and consequently $S \subseteq Rs_0$ which had to be shown. □

Examples 2.10 **(a)** All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ where $n \in \mathbb{N}$. We have seen this earlier in the chapter dealing with Abelian and cyclic groups.

(b) The polynomial ring $F[x]$ over the field F is a principal ideal ring. The ideals of $F[x]$ are therefore of the form $F[x]f$ for suitable $f \in F[x]$.

For the further discussion we need to introduce the following two notions.

Definition 2.11 Let R be a commutative unital ring and a, b elements of R. Then a is called a divisor of b, denoted by $a \mid b$ if there exists $c \in R$ such that $ac = b$. The divisors

of 1 are called units of R and they form a group which is often denoted by $R^\times$. We call an element $p \in R \setminus R^\times$ irreducible if it does not possess any proper divisor, i.e. for which $ab = p$ always implies $a \in R^\times$ or $b \in R^\times$.

Definition 2.12 Let R be a ring and S a two-sided ideal of R. On the (additive) quotient group R/S we define a multiplication by

$$(r + S) * (r' + S) := rr' + S,$$

by which R/S obtains the structure of a unital ring with identity $1 + S$ and zero-element S. We call R/S the residue ring of R modulo S.

We strongly recommend the reader to check the foregoing statement and determine the point where the two-sidedness of the ideal S is needed.

Definition 2.13 A left ideal S of a ring R is called maximal if for all left ideals S' with $S \subset S' \subseteq R$ there follows $S' = R$.

Lemma 2.14 *A two-sided ideal S of a ring R is a maximal left ideal if and only if R/S is a division ring. It will then also be maximal as a right ideal.*

Proof: The only thing we have to do is to prove that every nonzero element of R/S possesses a multiplicative inverse. Let $r + X$ be a non-zero element of R/S. Then $r \notin S$ which shows that $Rr + S$ is a left ideal that properly contains S. If we assume S to be maximal as a left ideal then be immediately get $Rr + S = R$ and this means we find $r' \in R$ and $s \in S$ with $r'r + s = 1$. From this we get $(r' + S)(r + S) = r'r + S = 1 + S$ which shows that $r + S$ has a left inverse. In the same way we can show that $r' + S$ possesses a left inverse in R/S, and this shows that $r' + S$ is invertible on two sides (as is $r + S$). Conversely, if T is a left ideal with $S \subset T \subseteq R$, and $t \in T \setminus S$, i.e. the element $t + S$ is non-zero in R/S then using the division ring property of R/S we obtain $t' \in R$ with $(t' + S)(t + S) = 1 + S$. This implies $T = T + S \supseteq Rt + S = R + S = R$, and hence we see that S is a maximal ideal. □

The following statement will be important also in a later section.

Proposition 2.15 *If p is an element of a commutative principal ideal domain R, then $R/(pR)$ is a field if and only if p is irreducible.*

Proof: According to the foregoing statement we only have to check if pR is maximal if and only if p is irreducible. If p is reducible then there exist non-units $a, b \in R$ with $ab = p$

and then we obviously have $Rp = Rab \subseteq Rb \subseteq R$. If we assume $Rab = Rb$ here then we would have $s \in R$ with $sab = b$ and hence $(sa-1)b = 0$ which already implies $a \in R^\times$. In a similar way we can show that $Rb \neq R$, and consequently Rp is not maximal. If now p is irreducible and S an ideal of R with $Rp \subset S \subseteq R$. Then there exists $s \in R$ with $S = Rs$ and furthermore $a \in R$ with $p = as$. As p is assumed to be irreducible we have $Rp \neq Rs$ and we can exclude a being a unit of R. Hence s is a unit of R and we see that $S = Rs = R$. □

Let us come to the question in how far arbitrary elements of a commutative ring R can be factorized using irreducible elements of R. For polynomial rings we can give an answer which can even be generalized to Euclidean rings and, moreover, to commutative principal ideal domains. The following lemma serves as a preparation.

Lemma 2.16 *Let F be a field and $a, a_1, \ldots, a_n \in F[x]$ and p an irreducible element of $F[x]$.*

(a) *There holds $p \mid a$ or $pF[x] + aF[x] = F[x]$.*

(b) *If $p \mid (a_1 \cdots a_n)$ then there exists $i \in \{1, \ldots, n\}$ with $p \mid a_i$.*

Proof: **(a)** We know already that $pF[x]$ is a maximal ideal of $F[x]$. For this reason we have $aF[x] \subseteq pF[x]$ or $aF[x] + pF[x] = F[x]$. If the latter is not true then $a \in pF[x]$ and hence $a = pr$, which means $p \mid a$.
(b) We need a proof only for $n = 2$, because the general statement then follows by induction. Assume $p \mid (a_1 a_2)$ and p is not a divisor of a_1. Then via **(a)** we get $pF[x] + a_1F[x] = F[x]$, which means there exist polynomials $r, s \in F[x]$ with $pr + a_1 s = 1$. Multiplying this by a_2 we find $pra_2 + sa_1a_2 = a_2$ where p clearly divides each summand of the left side. For this reason we have $p \mid a_2$ and this was the claim. □

Theorem 2.17 *If F is a field then $F[x]$ is a so-called unique factorization domain, i.e. every nonzero element $f \in F[x]$ is a product of a unit and a finite number of monic irreducible elements of $F[x]$. These factors are uniquely determined up to arrangement.*

Proof: We will prove the first part by induction on the degree of the polynomial. If $\deg(f) = 0$, then f is a constant and hence a unit of $F[x]$ which means there is nothing to show. For $\deg(f) \geq 1$ we distinguish two cases: First, if f is already irreducible then we can factor out its leading coefficient, and we obtain a factorization of the desired type. Otherwise we know that f is a product of two polynomials of properly smaller degree and this yields according to the induction hypothesis that these factors enjoy a factorization of the desired

type. Putting these factorizations together we arrive at a factorization of f of the desired type. To show uniqueness let $f = ap_1 \cdots p_n = bq_1 \cdots q_k$ with monic irreducible polynomials p_i and q_j and units $a, b \in F$. We again proceed by induction on the degree of f and first observe that for $\deg(f) = 0$, we find $n = k = 0$ and there remains nothing to show. If f is not a constant then $n \geq 1$ and $k \geq 1$ and from $ap_1 \cdots p_n = bq_1 \cdots q_k$ we obtain by applicaion of the foregoing lemma that $p_1 | bq_1 \cdots q_k$ and hence without loss of generality $p_1 | q_1$. As these polynomials are monic we see that $p_1 = q_1$. Dividing both sides by p_1 we obtain $ap_2 \cdots p_n = bq_2 \cdots q_k$, and as this is of properly smaller degree we apply the induction hypothesis and see that $a = b$ and up to arrangement $p_i = q_i$ for $i = 1, \ldots, k$ where $k = n$. All in all this finishes the proof. □

We now take care of the interesting question, how we can decide if a given polynomial, say over the field $\mathbb{Q}$, is irreducible. This will lead to two important irreducibility criteria, which we will discuss in the following.

Definition 2.18 A polynomial $f = \sum_{i=0}^{n} f_i x_i \in \mathbb{Z}[x]$ is called primitive, if $\gcd(f_0, \ldots, f_n) = 1$.

An immediate observation is the following lemma:

Lemma 2.19 *If $f, g \in \mathbb{Z}[x]$ are primitive, then so is fg.*

Proof: Primitivity of a (nonzero) polynomial $h \in \mathbb{Z}[x]$ means that the image $\overline{h}$ of h modulo p is nonzero for all primes p. Assume that f, g are primitive and that fg is not. Then there exists a prime $p \in \mathbb{N}$ such that $\overline{fg} = 0$. But moding out p is multiplicative, which means we have $\overline{f}\,\overline{g} = 0$ in $\mathbb{Z}_p[x]$ and this enforces $\overline{f} = 0$ or $\overline{g} = 0$, a contradiction. Hence, fg is primitive. □

Theorem 2.20 *(Gauss' Lemma) Let $f \in \mathbb{Z}[x]$ be a primitive polynomial. If $f = gh$ with $g, h \in \mathbb{Q}[x]$ of positive degree, then there also exist $G, H \in \mathbb{Z}[x]$ of positive degree with $f = GH$.*

Proof: Suppose that $f = gh$ as descrbed in the hypothesis. Let b be the least common multiples of the denominators of coefficients in g and let a be the greatest common divisor of the numerators of coefficients in g. Then $g = \frac{a}{b}G$ where G is a primitive integer polynomial. Doing the same with $h = \frac{c}{d}H$ we end up with the equality

$$f = \frac{a}{b} G \frac{c}{d} H$$

and this can be rewritten as $bdf = acGH$. Knowing that f is primitive, we have bd as the greatest common divisor of coefficients of bdf. By the previous lemma also GH is primitive, and hence ac is the greatest common divisor of $acGH$. This yields $ac = bd$ and consquently $f = GH$. □

The foregoing result can be used to derive what is called Eisenstein's irreducibility criterion:

Theorem 2.21 *Let $f \in \mathbb{Z}[x]$ be a polynomial of positive degree n. If there exists a prime number $p \in \mathbb{N}$ with $p \mid f_i$ for all $i = 0, \ldots, n-1$ but $p \nmid f_n$ and $p^2 \nmid f_0$ then f is irreducible over $\mathbb{Q}$.*

Proof: Dividing out the greatest common divisor of the coefficients of f would not have any effect on whether or not the assumption about p is true because of $p \nmid f_n$. For that reason we will assume that f is primitive, and that p is a prime number satisfying the hypothesis. Assuming that $f = gh$ with g of degree r and h of degree s we first find $f_0 = g_0 h_0$ and hence $p \mid g_0 h_0$ but $p^2 \nmid g_0 h_0$. This implies that $p \mid g_0$ or $p \mid h_0$, but not both. Without loss of generality we assume $p \mid g_0$. If now all of the g_i were divisible by p then $p \mid f_n$, which is not possible. Hence, let k be the smallest subscript for which $p \nmid g_k$ and consider

$$f_k \;=\; g_0 h_k + g_1 h_{k-1} + \ldots + g_{k-1} h_1 + g_k h_0.$$

By the choice of k our prime p divides each of the $g_0, \ldots, g_{k-1}$, and as $k < n$ we know that $p \mid f_k$. But then by subtraction we find that $p \mid g_k h_0$ which eventually enforces $p \mid h_0$, a contradiction. This shows that f is irreducible over the rational numbers. □

Example 2.22 Consider the polynomial $f = 10 - 15x + 25x^2 - 7x^4$. Then $p = 5$ divides all coefficients of f except the leading one, and p^2 does not divide 10. For this reason f is irreducible over $\mathbb{Q}$.

Definition 2.23 Let F be a field and $f = \sum_{i=0}^{n} f_i x^i$ a polynomial over F. An element $a \in F$ is called a zero of f, if $f(a) := \sum_{i=0}^{n} f_i a^i = 0$.

It is easy to check that substituting x by an element of F induces a ring homomorphism $F[x] \longrightarrow F,\ f \mapsto f(a)$. Clearly we have $(f+g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$. This leads to the following statement.

Proposition 2.24 *Let F be a field and $f \in F[x]$ a polynomial. Then $a \in F$ is a zero of f if and only if there exists $g \in F[x]$ with $f = (x - a)g$.*

Proof: If $f = (x-a)g$ then certainly a is a zero of f. If now a is a zero of f then we apply the division algorithm to obtain $g, r \in F[x]$ with $f = g(x-a) + r$, where r must be a constant which is forced to be zero by substitution by a. □

Corollary 2.25 *Let F be a field and $f \in F[x]$ nonzero. Then f possesses at most $\deg(f)$ zeros (including multiple zeros) in F.*

Proof: This can be shown by induction on $\deg(f)$. For $\deg(f) = 0$ there is nothing to show. If $\deg(f) \geq 1$ and $a \in F$ is a zero of f then according to the foregoing proposition we have $f = (x-a)g$ where $\deg(g) = \deg(f) - 1$. For this reason we see by induction hyptothesis that g has at most $\deg(f) - 1$ zeros which finally leads to the claim. □

The following statement will be used in a later application.

Definition 2.26 Let F be a field. We call the mapping

$$D : F[x] \longrightarrow F[x], \quad \sum_{i=0}^{n} f_i x^i \mapsto \sum_{i=1}^{n} i f_i x^{i-1}$$

the formal derivative. Higher derivatives D^k are inductively defined by $D^0 = \mathrm{id}$ and $D^{k+1} = D \circ D^k$.

The proof of the following lemma is left as an exercise.

Lemma 2.27 *The formal derivative is an F-endomorphim of the F-vectorspace $F[x]$. It satisfies the product rule $D(fg) = (Df)g + f(Dg)$ and there holds $\deg(Df) \leq \deg(f) - 1$ where we have equality if, $\mathrm{char}(F)$ does not divide $\deg(f)$.*

Definition 2.28 Let F be a field and $a \in F$ and $f, g \in F[x]$. If $f = (x-a)^m g$ with $g(a) \neq 0$, then m is called the multiplicity of a as a zero of f.

Our final statement shows the connection between multiple zeros and the behaviour of the formal derivative.

Proposition 2.29 *Let F be a field of characteristic 0, and a an element of F. For a polynomial $f \in F[x]$ of positive degree the following are equivalent:*

- **(a)** *$f = (x-a)^m g$ with $g(a) \neq 0$.*
- **(b)** *$(D^i f)(a) = 0$ for $i = 0, \ldots, m-1$ and $(D^m f)(a) \neq 0$.*

Proof: It can be shown by application of the product rule that

$$D^k f = (x-a)^{m-k} g_k$$

with $g_k(a) \neq 0$ for $0 \leq k \leq m$, This immediately gives the desired equivalence. □

2.2 Fields and Field Extensions

A field is a commutative division ring. If such a division ring is non-commutative then people usually call it a skew-field.

Definition 2.30 A subset F of a field G which forms a field with respect to the inherited operations is called a subfield of G. The field G is called an extension of F. A pair of fields F and G, in which G is an extension of F is usually denoted by $G : F$. If the kernel of the ring homomorphism $\mathbb{Z} \longrightarrow G,\ z \mapsto z \cdot 1$ is given by $\{0\}$ then we say G is of characteristic zero. Otherwise it will necessarily be given by $p\mathbb{Z}$ where p is a prime, and then G is said to be of characteristic p.

Examples 2.31 **(a)** $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{R}$ is a subfield of $\mathbb{C}$. All these fields are of characteristic 0.

(b) $\mathbb{Z}/p\mathbb{Z}$ is a field of characteristic p for all primes p. In particular for every prime there exists a field that has the given prime as its characteristic.

The intersection of an arbitrary family of subfields of a field is again a subfield. For this reason every field possesses a smallest subfield $P(F)$ which is called the prime field of F.

Lemma 2.32 *Let F be a field of characteristic p.*

(a) *$p = 0$ if and only if $P(F) \cong \mathbb{Q}$.*

(b) *p is a nonzero prime if and only if $P(F) \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof: It is easy to check that $R := \{z \cdot 1 \mid z \in \mathbb{Z}\}$ is a subring of $P(F)$. Now $\mathrm{char}(F) = p \neq 0$ is equivalent to $R \cong \mathbb{Z}/p\mathbb{Z}$ and this is equivalent to $R = P(F)$, since R itself is a field. In case $\mathrm{char}(F) = 0$ we know that this is equivalent to $R \cong \mathbb{Z}$, and the smallest field in which R is contained must be isomorphic with $\mathbb{Q}$. This exactly means $P(F) \cong \mathbb{Q}$. □

The following characterization of the prime field might be of independent interest.

Proposition 2.33 *If F is a field of characteristic $p \neq 0$, then $P(F) = \{x \in F \mid x^p = x\}$.*

Proof: We know that we have $P(F) \cong \mathbb{Z}/p\mathbb{Z}$. In this field we have $x^{p-1} = 1$ for all $x \neq 0$, which means that $x^p = x$ for all $x \in F$. Consequently we know that $P(F) \subseteq \{x \in F \mid x^p = x\}$. On the other hand $\{x \in F \mid x^p = x\}$ is the set of all zeros of the polynomial $x^p - x \in F[x]$, and this set cannot have more than p elements. For this reason the claim follows from cardinality arguments. □

Our knowledge regarding prime fields can be used to find out more about the structure of arbitrary fields.

Proposition 2.34 *Every finite field is a finite (dimensional) vector space over its prime field. In particular there can only exist finite fields of prime power order.*

Regarding the multiplicative group of a finite field we find the following interesting statement. We will return to this later.

Proposition 2.35 *Every finite subgroup of the multiplicative group of a field is cyclic. In particular the multiplicative group of a finite field itself is cyclic.*

Proof: Let F be a finite field and G a finite subgroup of its multiplicative group $F^\times$. According to the main theorem on finite abelian group we know that G decomposes as a direct sum of abelian p_i-groups where the p_i are suitable primes. If we show that these components are cyclic then our claim follows by the Chinese Remainder Theorem. Let G_p be the maximal direct summand belonging to the prime p. Every element of G_p has order a power of p and certainly there is an element $z \in G_p$ that has maximal order, say p^r. All other elements $b \in G_p$ must be of order p^s where s might vary between 0 and r. From this we get $b^{p^r} = (b^{p^s})^{p^{r-s}} = 1$ for all $b \in G_p$, and consequently all $b \in G_p$ are zeros of the polynomial $x^{p^r} - 1 \in F[x]$. According to our earlier results however there are at most p^r such zeros. For this reason we see that $G_p = \langle z \rangle$ as claimed. □

Definition 2.36 If $G : F$ is a field extension then the F-dimension of G is called the degree of the extension, denoted by $[G : F]$. If $[G : F]$ is finite then we say $G : F$ is finite. Extensions of degree 2 are called quadratic extensions.

Examples 2.37 **(a)** $[\mathbb{C} : \mathbb{R}] = 2$ which means that $\mathbb{C}$ is a quadratic extension of $\mathbb{R}$.

(b) Every finite field is a finite extension of its prime field.

Definition 2.38 If $G : F$ is a field extension then a field H with $G \supseteq H \supseteq F$ is called intermediate field of $G : F$.

Intermediate fields satisfy the following degree formula, a formula which rules wide areas of field theory.

Proposition 2.39 *Let H be an intermediate field of the extension $G : F$. Then $[G : F] = [G : H] \cdot [H : F]$. If $[G : F]$ is finite then $[G : H]$ and $[H : F]$ are divisors of $[G : F]$, and in particular $[G : F] = [H : F]$ enforces $G = H$.*

Proof: If $(\alpha_i)_{i \in I}$ is an H-basis of G and $(\beta_j)_{j \in J}$ is an F-basis of H, then a simple computation shows that $(\alpha_i \beta_j)_{i \in I, j \in J}$ is an F-basis of G. This implies all of our claims if the given extensions are finite. For infinite degrees we agree on the formulae $\infty \cdot n = \infty$ for all $n \in \mathbb{N} \cup \{\infty\}$, and then the claims are again true.

2.3 Algebraic Extensions

Definition 2.40 Let $G : F$ be a field extension. An element $a \in G$ is called algebraic over F if there is a polynomial $f \in F[x]$ such that $f(a) = 0$. Otherwise we call a transcendental.

Proposition 2.41 *Let $G : F$ be a field extension and $a \in G$ algebraic over F.*

(a) *There is a unique monic polynomial of minimal degree $m_a \in F[x]$ with $m_a(a) = 0$.*

(b) *m_a is irreducible and a divisor of every polynomial $f \in F[x]$ that satisfies $f(a) = 0$.*

(c) *If $f \in F[x]$ is monic and irreducible with $f(a) = 0$ then $f = m_a$.*

Proof: We again consider the substitution homomorphism $\Phi_a : F[x] \longrightarrow G,\ f \mapsto f(a)$. Assuming that a is algebraic immediately implies that Φ cannot be injective, in other words, $\mathrm{Ker}(\Phi_a) \neq \{0\}$. According to our preparations regarding polynomial rings we then know that $\mathrm{Ker}(\Phi_a) = F[x]m_a$, where m_a is unique up to a constant factor. Assuming m_a to be monic then makes it unique. Certainly m_a divides every polynomial $f \in F[x]$ that satisfies $f(a) = 0$ because such a polynomial is contained in $\mathrm{Ker}(\Phi_a)$. If $m_a = fg$ for $f, g \in F[x]$, then we would have $0 = m_a(a) = f(a)g(a)$ and hence $f(a) = 0$ or $g(a) = 0$, which enforced $m_a | f$ or $m_a | g$ and $\deg(f) = 0$ or $\deg(g) = 0$. Hence m_a is irreducible. Finally, if $f \in F[x]$ is irreducible with $f(a) = 0$, then $m_a \mid f$ and hence $f = cm_a$ by which c immediately results to be a constant polynomial. Assuming f to be monic then shows that $f = m_a$ as claimed. □

Definition 2.42 The polynomial m_a that we have defined in 2.41 is called the minimal polynomial of a over F. The degree of $F(a) : F$ is given by $\deg(m_a)$ and sometimes it is called the degree of a.

Remark 2.43 If H is an intermediate field of $G : F$ and a is algebraic over F, then a is also algebraic over H because $F[x] \subseteq H[x]$. However the minimal polynomial of a over H might be different from the minimal polynomial of a over F. It is however clear that the minimal polynomial of a over H is a divisor of the minimal polynomial over F because of $m_a \in H[x]$ and our statements in 2.41.

In the following we would like to see what the field extension of a single algebraic element looks like. To get prepared, let $G : F$ be a field extensions and $a \in G$ be an algebraic element of G with minimal polynomial $m_a \in F[x]$. Consider the substitution homomorphism

$$\Phi_a : F[x] \longrightarrow G, \quad f \mapsto f(a).$$

We have already understood that its kernel is given by $F[x]m_a$, and for convenience we denote its image by $F[a] := \{f(a) \mid f \in F[x]\}$. By homomorphy we then have the natural isomorphism

$$F[x]/F[x]m_a \;\cong\; F[a].$$

As we learned earlier the irreducibility of m_a shows that $F[a]$ is a subfield of G that clearly contains F and also a.

Theorem 2.44 *Let $G : F$ be a field extension and $a \in G$ an algebraic element. Then $F[a]$ is the smallest subfield of G that contains F and a.*

Proof: The smallest subfield of G that contains F and a is clearly given by

$$F(a) \;:=\; \bigcap\{H \mid H \text{ subfield of } G \text{ and } F \cup \{a\} \subseteq H\},$$

and we wish to show that $F(a) = F[a]$. We have seen above that $F[a]$ is a subfield of G that contains F and also a. For this reason we clearly have $F(a) \subseteq F[a]$. On the other hand $F(a)$ clearly contains all elements of G that are of the form $\sum_{i=0}^{n} f_i a^i$ where $f_i \in F$ and $n \in \mathbb{N}$. In other words $F(a)$ contains $f(a)$ for all $f \in F[x]$, and this shows $F(a) \supseteq F[a]$. □

Another nice characterization of algebraic elements is the following:

Corollary 2.45 *Let $G : F$ be a field extension. An element $a \in G$ is algebraic if and only if $F(a) : F$ is a finite extension.*

Proof: If a is not algebraic then a is trancendental, and we know by 2.40 the kernel of the substitution homomorphism Φ_a is trivial, and hence $F[a] \cong F[x]$. For this reason we find

$\dim_F(F(a)) \geq \dim_F(F[a]) = \dim_F(F[x]) = \infty$. If on the other hand a is algebraic then we know $[F(a) : F] = [F[a] : F] = \deg(m_a) < \infty$. □

Definition 2.46 A field extension $G : F$ is called algebraic if every $a \in G$ is algebraic over F. Otherwise we call it transcendental.

Note that the existence of a single transcendental element in the extension makes us call the extension transcendental.

Proposition 2.47 *Let $G : F$ be a field extension.*

(a) *If $[G : F] < \infty$, then $G : F$ is algebraic.*

(b) *$[G : F] < \infty$ if and only if there exist element $a_1, \ldots, a_n \in G$ such that $G = F(\{a_1, \ldots, a_n\})$.*

Proof: **(a)** If $a \in G$ is transcendental over F, then we immediately have $[G : F] \geq [F(a) : F] = \infty$, by which $G : F$ cannot be finite any more.
If $[G : F] = n$ and $\{a_1, \ldots, a_n\}$ is an F-basis of algebraic elements of G then we certainly have $G = F(\{a_1, \ldots, a_n\})$. Conversely, if $G = F(\{a_1, \ldots, a_n\})$ with algebraic elements $a_1, \ldots, a_n \in G$, then by 2.43 each of the a_i is also algebraic over $F(\{a_1, \ldots, a_{i-1}\})$ for $i = 2, \ldots, n$, and hence $[F(\{a_1, \ldots, a_i\}) : F(\{a_1, \ldots, a_{i-1})] < \infty$ for all $i = 2, \ldots, n$. From this we inductively obtain $[F(\{a_1, \ldots, a_n\}) : F] < \infty$. □

Remark 2.48 Note that the converse of 2.47(a) does not hold in general, i.e. there exist algebraic field extensions of infinite degree. For algebraic a in $G : F$ the statement in 2.47(b) justifies saying that $F(\{a\}) : F$ is a simple algebraic extension.

We would like to know now if the set of all algebraic elements of a field extension allows a characterization.

Proposition 2.49 *Let $G : F$ be a field extensions. Then the set $\{a \in G \mid a$ algebraic over $F\}$ forms an intermediate field of $G : F$.*

Proof: If $a, b \in G$ are algebraic over F, then the elements $a+b, a-b, ab,$ and a/b (if $b \neq 0$) are contained in $F(\{a, b\})$, which is algebraic by 2.47(b). For this reason these elements are clearly algebraic over F. □

The following statement is of interest.

Proposition 2.50 *Let $G : F$ and $H : G$ be field extensions. Then $G : F$ and $H : G$ are algebraic if and only if $H : F$ is so.*

Proof: If $H : F$ is algebraic then certainly $G : F$ and also $H : G$ according to the definition and what we have learnt so far. Conversely, if $H : G$ is algebraic and $h \in H$ is an arbitary element then there exists a polynomial $g \in G[x]$ with $g(h) = 0$. The polynomial g is of the form $g = \sum_{i=0}^{n} g_i x^i$ where $g_i \in G$ and it is clear that h is also algebraic over $F(\{g_0, \ldots, g_n\})$. According to the degree formula we get from this immediately $[F(\{h, g_0, \ldots, g_n\}) : F] = [F(\{h, g_0, \ldots, g_n\}) : F(\{g_0, \ldots, g_n\})] \cdot [F(\{g_0, \ldots, g_n\}) : F]$ which is finite and consequently shows that h is algebraic over F. □

2.4 Ruler and Compass Constructions

In the Euclidean plane we are interested in solving certain geometric problems, or to prove the impossibility of a solution. In the following we will give three impressing examples showing that Abstract Algebra can be used to determine if geometric solutions of a problem exist or not.

Given $\mathbb{R}^2$ we will distinguish a unit line by marking its start and end point. Using this unit line we are interested to construct further points by exclusively using a ruler and a compass. Doing so we are restricted to the following rules:

(i) If P and Q are points that we already constructed then we may use the ruler in order to draw the (infinite) line through these points.

(ii) If P is a constructed point and d is a constructed distance (the distance between two constructed points) then we may use the compass in order to draw the circle with radius d around P.

(iii) All intersection points of objects that we got by rule (i) and/or rule (ii) are accepted to be constructible points.

To ease our life we assign coordinates and denote the starting point of our initial line by $(0, 0)$ and its ending point by $(1, 0)$. Elementary ruler and compass manipulations then show that we can (at least theoretically) construct every point $(n, 0)$ where $n \in \mathbb{Z}$. We can do more: having a copy of $\mathbb{Z}$ in the plane we can put a perpendicular line in the point $(0, 0)$ and then put another copy of $\mathbb{Z}$ on that line, i.e. we have two axes of a coordinate

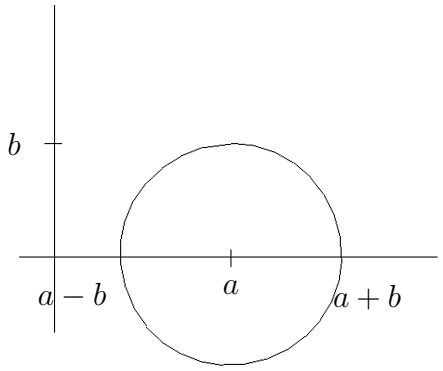
system. Moreover, this shows that (again at least theoretically) every point $(a, b) \in \mathbb{Z}^2$ is constructible by ruler and compass.

Calling an element $a \in \mathbb{R}$ constructible if the point $(a, 0)$ is so in our Euclidean plane, we immediately see that two elements $a, b \in \mathbb{R}$ are constructible if the point $(a, b) \in \mathbb{R}^2$ can be constructed.

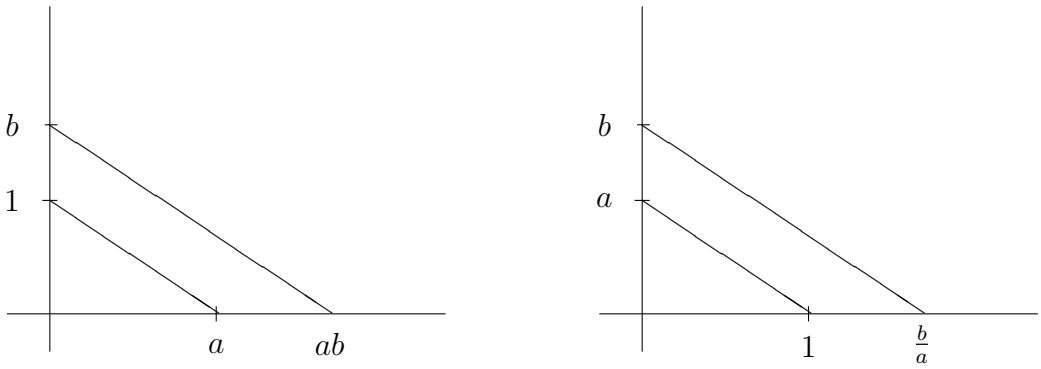
Our goal is to determine which real numbers are constructible.

Lemma 2.51 *If $a, b \in \mathbb{R}$ are constructible the so are $a + b, a - b, ab$ and a/b provided $b \neq 0$.*

Proof: Addition and subtraction of given numbers a, b only require a single ruler and compass step as the following sketch might clarify.



Regarding multiplication we need to remember the ray theorems, which immediately make the following sketches plausible.



This completes the proof. □

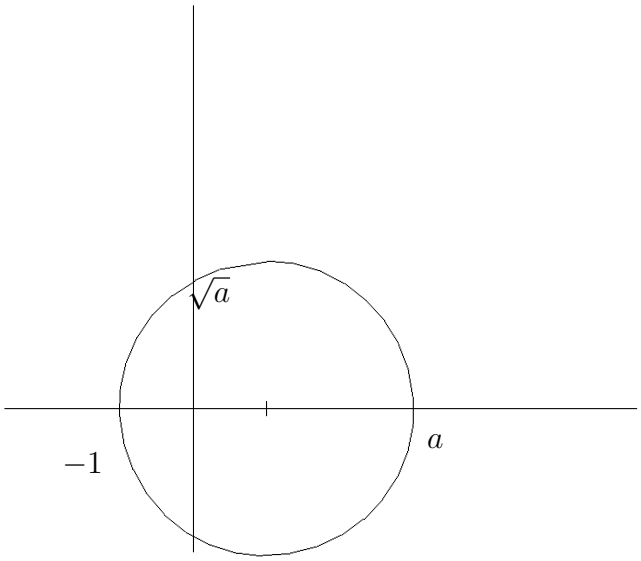
Corollary 2.52 *The set of all points in* $\mathbb{R}^2$ *which can be constructed by the rules that we mentioned form an intermediate field of* $\mathbb{R} : \mathbb{Q}$.

Proof: By the above observations the set of all these points forms a field. As this field contains $\mathbb{Z}$, It must then also contain $\mathbb{Q}$. Hence it is an intermeidate field of $\mathbb{R} : \mathbb{Q}$ as claimed. □

The following statement is of high importance.

Lemma 2.53 *If* $a \in \mathbb{R}_+$ *is constructible then so is* $\sqrt{a}$.

Proof: Given a rectangular triangle we can draw the height. Then our knowledge from elementary geometry says that the product of the hypotenuse section is the square of the height. A square root can then be constructed using the following sketch idea:



Given $a \in \mathbb{R}^+$ assume without loss of generality that $a \geq 1$. Then construct the center $(a-1)/2$ on the x-axis and use the radius $(a+1)/2$ in order to draw a circle around the given center. This circle touches -1 and a on the x-axis and it intersects the y-axis in the point $\sqrt{a}$. This shows the claim. □

Let us denote the intermediate field of $\mathbb{R} : \mathbb{Q}$ that can be constructed by our geometric rules by L ,

If (x_1, y_1) and (x_2, y_2) are constructible points in the plane then the line through these points is given by $G = \{(x, y) \in \mathbb{R}^2 \mid (x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1)\}$. This means all points on G satisfy an equation of the form $ux + vy + w = 0$ where $u, v, w \in L$. A circle C with constructible center (x_1, y_1) and constructible radius $r \in L$ is algebraically given by $C = \{(x, y) \in \mathbb{R} \mid (y - y_1)^2 + (x - x_1)^2 - r^2 = 0\}$. Investigating the intersections of these types of point sets we have to distinguish a few cases:

line-line intersections: The intersection point of the two lines described by the equations $ux+vy+w = 0$ and $u'x+v'y+w' = 0$ is just their simultaneous solution and hence possesses coordinates in $\mathbb{Q}(u, v, w, u', v', w') \subseteq L$. This means the intersection of constructible lines does not generate points beyond the scope of these lines.

line-circle intersections: If the line G is described by the equation $ux+vy+w = 0$ and the circle C is described by the equation $(x-c)^2+(y-d)^2-e^2 = 0$ where $u, v, w, c, d, e \in L$, and if these two objects intersect, then a solution of the line equation (wlog. $v \neq 0$) leads to $y = -\frac{ux}{v} - \frac{w}{v}$. If we substitute y in the circle equation by this value, we obtain the quadratic equation $(x - c)^2 + (\frac{ux}{v} + \frac{w}{v} + d)^2 - e^2 = 0$ which means an equation of type $Ax^2 + Bx + C = 0$, where $A, B, C \in L$. According to the formula that we know we find the solution

$$x_{1/2} = -\frac{B}{2A} \pm \sqrt{\frac{B^2}{4A^2} - \frac{4C}{A}}$$

which means also these elements are contained in L.

circle-circle intersections: Algebraically the interesection of two circles is equivalent with the intersection of a line with a circle, hence we can reduce this case to what we have just learnt.

Theorem 2.54 *An element $a \in \mathbb{R}$ is constructible if and only if there is a series of elements $(\beta_i)_{i=1,\ldots,n}$ and an according tower of field extensions $\mathbb{Q} = L_0 \subseteq \ldots \subseteq L_n \subseteq \mathbb{R}$ such that $L_{i+1} = L_i(\sqrt{\beta_{i+1}})$ for $i = 0, \ldots, n-1$ and $a \in L_n$.*

Proof: If a is constructible then according to the above analysis we add at most squares from construction step to construction step. If a is constructed after finitely many steps, then we immediately obtain the desired tower of field extensions. Conversely, let

$$\mathbb{Q} \;=\; L_0 \;\subseteq \ldots \subseteq\; L_n \;\subseteq\; \mathbb{R}$$

be a tower of field extensions of the mentioned form. If $n = 0$ then there is nothing to show. If we assume that all elements of L_{n-1} are constructible for some $n \geq 1$ then the elements of L_n are of the form $x + y\sqrt{\beta_n}$ with $x, y \in L_{n-1}$. According to our analysis these numbers are constructible as well, and hence we obtain our claim. □

Corollary 2.55 *If an element $a \in \mathbb{R}$ is constructible then there is an intermediate field H of $\mathbb{R} : \mathbb{Q}$ with $a \in H$ and $[H : \mathbb{Q}] = 2^n$ for suitable $n \in \mathbb{N}$.*

Corollary 2.56 **(a)** *Transcendental elements in $\mathbb{R} : \mathbb{Q}$ are not constructible.*

(b) *If $a \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, and $[\mathbb{Q}(a) : \mathbb{Q}]$ is not a power of 2 then a is not constructible.*

Proof: It is quite obvious that only algebraic numbers can be constructed. If now a is algebraic then there is an intermediate field H of $\mathbb{R} : \mathbb{Q}$ with $[H : \mathbb{Q}] = 2^n$ for suitable $n \in \mathbb{N}$ and we have $a \in H$. According to the degree formula we see however that $[\mathbb{Q}(a) : \mathbb{Q}]$ is a divisor of $[H : \mathbb{Q}]$ and this yields the claim. □

Proposition 2.57 *Given a cube it is not possible to construct a new cube (using ruler and compass) that has double the volume of the given one.*

Proof: Without loss of generality our given cube has side length 1 and the problem is to construct a new cube of side length $\sqrt[3]{2}$. This element however is of degree 3 over $\mathbb{Q}$ because $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Hence we have just proved the impossibility of a geometric solution. □

Proposition 2.58 *Squaring the circle by ruler and compass is impossible.*

Proof: Given a circle with radius of a unit length. Its area is, as we know from school, given by π. Constructing a square with this area is the same as solving the equation $x^2 = \pi$. Given that we know that π (and hence $\sqrt{\pi}$) are transcendental, this is impossible by application of 2.56. □

Everybody knows how to construct a $60°$ angle just by using a compass. This shows that it is possible to trisect the angle of $180°$. As we see in the following this geometric task is impossible in general. We will prove this by giving an example of a (constructible) angle that does not allow a trisection by ruler and compass.

Proposition 2.59 *It is not possible in general to trisect a given angle just using ruler and compass.*

Proof: We will show that the $60°$-angle cannot be trisected. Assume that we could trisect it then we would in particular be able to construct the cosine of a $20°$ angle. Using trigonometric identities we see that

$$\cos(3\alpha) \;=\; 4\cos^3(\alpha) - 3\cos(\alpha).$$

For $\alpha = 20°$ this yields by substitution $a = \cos(\alpha)$ the equation

$$4a^3 - 3a \;=\; \frac{1}{2},$$

which means that a is a zero of the rational polynomial $f(x) = 8x^3 - 6x - 1$. Substituting $x := \frac{y+1}{2}$ we are equivalently looking for a zero of the polynomial $g(y) = y^3 + 3y^2 - 3$. This polynomial does not possess rational zeros, and hence is irreducible over $\mathbb{Q}$ as the following consideration proves: if $\frac{p}{q}$ were a rational zero of g in lowest terms, then we would have $p^3 + 3p^q - 3q^3 = 0$, which means

$$p^3 \;\equiv\; 0 \pmod 3$$

and hence also $p \equiv 0 \pmod 3$. For this reason we would have $p = 3k$ for suitable $k \in \mathbb{Z}$ and this gives us the equation $27k^3 + 27k^2q - 3q^3 = 0$, and consequently $q^3 \equiv 0 \pmod 3$. Likewise this leads to $q \equiv 0 \pmod 3$ which induces a contradiction to $\frac{p}{q}$ being in lowest terms. This shows that $[\mathbb{Q}(\cos(20°)) : \mathbb{Q}] = 3$, and hence we see the impossibility of construction. □

Remark 2.60 If we had started with more than just a unit line, say a parabola or an even more complicated curve, and if we had more tools than just ruler and compass then it would be clear that our results had changed considerably. The exercises will contain some material regarding this question.