Algebra

Universität Braunschweig, SS 2008
Universität Siegen, WS 2005

Jürgen Müller

Contents

1 Groups and actions 1
2 Homomorphisms and subgroups 6
3 Rings and domains 14
4 Factorial and Euclidean rings 20
5 Field extensions 27
6 Galois theory 34
7 Applications 41
8 Exercises (in German) 51
9 References 61

1 Groups and actions

(1.1) Monoids. a) A set G together with a **multiplication** $\cdot\colon G \times G \to G\colon [g,h] \mapsto gh$ fulfilling the following conditions is called a **monoid**:
i) There is a **neutral element** $1 \in G$ such that $1 \cdot g = g = g \cdot 1$ for all $g \in G$,
ii) and we have **associativity** $(fg)h = f(gh)$ for all $f, g, h \in G$.

If $gh = hg$ for all $g, h \in G$ then G is called **commutative** or **abelian**.

In particular we have $G \neq \emptyset$. The neutral element is uniquely defined: If $1' \in G$ also is a neutral element then we have $1 = 1 \cdot 1' = 1'$. The product $g_1 g_2 \cdots g_n \in G$ is well-defined independently from the bracketing for all $g_1, \ldots, g_n \in G$, and if G is commutative then the product $g_1 g_2 \cdots g_n \in G$ is independent from the order of its factors. For $g \in G$ let $g^0 := 1$, and recursively $g^{n+1} := g^n g$ for all $n \in \mathbb{N}_0$. Then we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{N}_0$. If $g, h \in G$ **commute**, i. e. we have $gh = hg$, then $(gh)^n = g^n h^n = h^n g^n$ for all $n \in \mathbb{N}_0$.

A subset $U \subseteq G$ is called a **submonoid**, if $1 \in U$ and multiplication restricts to a map $\cdot\colon U \times U \to U$. Then U with the restricted multiplication again is a monoid; e. g. $\{1\}$ and G are submonoids of G.

If G and H are monoids, a map $\varphi\colon G \to H$ is called a **(monoid) homomorphism**, if $1\varphi = 1$ and $(gg')\varphi = g\varphi \cdot g'\varphi$ for all $g, g' \in G$; hence $\mathrm{im}(\varphi) \subseteq H$ is a submonoid. If φ is surjective it is called an **epimorphism**, if φ is injective it is called a **monomorphism**, if φ is bijective it is called an **isomorphism**; in this case φ^{-1} is an isomorphism, we write $G \cong H$. If $G = H$, then φ is called an **endomorphism**, and a bijective endomorphism is called an **automorphism**.

(1.2) Groups. a) Let G be a monoid. An element $g \in G$ is called **right invertible** if there is a **right inverse** $h' \in G$ such that $gh' = 1$, it is called **left invertible** if there is a **left inverse** $h'' \in G$ such that $h''g = 1$.

If $g \in G$ is both right and left invertible then it is called **invertible** or a **unit**. If $h' \in G$ is a right inverse and $h'' \in G$ is a left inverse, then we have $h'' = h'' \cdot 1 = h''(gh') = (h''g)h' = 1 \cdot h' = h'$. Thus in this case there is a unique **inverse** $g^{-1} := h' = h'' \in G$ such that $gg^{-1} = 1 = g^{-1}g$.

Let $G^* \subseteq G$ be the set of units. Then we have $1 \in G^*$, where $1^{-1} = 1$. For all $g, h \in G^*$ we from $gh(h^{-1}g^{-1}) = 1 = (h^{-1}g^{-1})gh$ conclude $(gh)^{-1} = h^{-1}g^{-1}$ and thus $gh \in G^*$; hence G^* is a submonoid of G. For $g \in G^*$ we have $(g^{-1})^{-1} = g$, thus $g^{-1} \in G^*$, hence $(G^*)^* = G^*$.

For $g \in G^*$ and $n \in \mathbb{N}$ we let $g^{-n} := (g^{-1})^n$. Then we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$. If $g, h \in G^*$ commute the we have $(gh)^n = g^n h^n = h^n g^n$ for all $n \in \mathbb{Z}$.

b) A monoid G such that $G = G^*$ is called a **group**. If G is finite then $|G| \in \mathbb{N}$ is called its **order**, and G is called **commutative** or **abelian** if the underlying monoid is. For any monoid G the set G^* is called the **group of units** of G.

A submonoid U of a group G such that for all $g \in U$ we also have $g^{-1} \in U$, is

called a **subgroup**; we write $U \leq G$. Then U with the restricted multiplication again is a group; e. g. we have the **trivial** subgroup $\{1\} \leq G$ and $G \leq G$.

If G and H are groups, a map $\varphi\colon G \to H$ is called a **(group) homomorphism**, if $(gg')\varphi = g\varphi \cdot g'\varphi$ for all $g, g' \in G$. From $1\varphi = (1 \cdot 1)\varphi = 1\varphi \cdot 1\varphi$ we get $1 = 1\varphi \cdot (1\varphi)^{-1} = 1\varphi \cdot 1\varphi \cdot (1\varphi)^{-1} = 1\varphi$, hence φ also is a monoid homomorphism. For $g \in G$ we have $1 = 1\varphi = (gg^{-1})\varphi = g\varphi \cdot (g^{-1})\varphi$, hence $(g^{-1})\varphi = (g\varphi)^{-1}$, and thus we have $(g^n)\varphi = (g\varphi)^n$ for all $n \in \mathbb{Z}$. We have $\mathrm{im}(\varphi) \leq H$, and for any $U \leq H$ we have $\varphi^{-1}(U) \leq G$.

(1.3) Example. a) $\mathbb{Z}$ is an abelian additive group with neutral element 0, and a commutative multiplicative monoid with neutral element 1 and group of units $\mathbb{Z}^* = \{\pm 1\}$. For $n \in \mathbb{Z}$ the set $n\mathbb{Z} \leq \mathbb{Z}$ is an additive subgroup, and $\{2^n \in \mathbb{N}; n \in \mathbb{N}_0\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$ are multiplicative submonoids.

b) Let K be a field. Any K-vector space is an abelian additive group with neutral element 0. The set $K^{n\times n}$ of $(n \times n)$-matrices with matrix multiplication is a monoid with neutral element E_n. Since for $n \geq 2$ we have

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

the monoid $K^{n\times n}$ is commutative if and only if $n = 1$. Its group of units is called the **general linear group** $\mathrm{GL}_n(K) := (K^{n\times n})^* = \{A \in K^{n\times n}; A \text{ invertible}\} = \{A \in K^{n\times n}; \mathrm{rk}_K(A) = n\} = \{A \in K^{n\times n}; \det(A) \neq 0\}$, which is abelian if and only if $n = 1$; the latter case coincides with $K^* = K \setminus \{0\}$.

(1.4) Symmetric groups. a) Let $X \neq \emptyset$ be a set, let $\mathrm{Maps}(X, X) := \{f\colon X \to X\}$, and let $\cdot\colon \mathrm{Maps}(X, X) \times \mathrm{Maps}(X, X) \to \mathrm{Maps}(X, X)\colon [f, g] \to fg$ be the composition of maps, i. e. $fg\colon X \to X\colon x \mapsto xfg = g(f(x))$. Then $\mathrm{Maps}(X, X)$ is a monoid with neutral element $\mathrm{id}_X\colon X \to X\colon x \mapsto x$: We have $f \cdot \mathrm{id}_X = \mathrm{id}_X \cdot f = f$ for all $f \in \mathrm{Maps}(X, X)$, and $x^{(fg)h} = (x^{fg})^h = ((x^f)^g)^h = (x^f)^{gh} = x^{f(gh)}$ for all $x \in X$, thus $(fg)h = f(gh)$ for all $f, g, h \in \mathrm{Maps}(X, X)$.

$f \in \mathrm{Maps}(X, X)$ is right invertible if and only if f is injective: Let f be right invertible with right inverse $g \in \mathrm{Maps}(X, X)$. Then for $x, y \in X$ such that $xf = yf$ we have $x = x \cdot \mathrm{id}_X = xfg = yfg = y \cdot \mathrm{id}_X = y$, hence f is injective. Let conversely f be injective. Then we define $g \in \mathrm{Maps}(X, X)$ by $yg := x \in X$ whenever $y = xf \in \mathrm{im}(f)$, and $yg := y$ whenever $y \in X \setminus \mathrm{im}(f)$. Then we have $xfg = (xf)g = x$ for all $x \in X$, hence $fg = \mathrm{id}_X$, thus g is a right inverse of f.

$f \in \mathrm{Maps}(X, X)$ is left invertible if and only if f is surjective: Let f be left invertible with left inverse $g \in \mathrm{Maps}(X, X)$. Then for all $x \in X$ we have $x = x \cdot \mathrm{id}_X = xgf$, hence $x \in \mathrm{im}(f)$, thus f is surjective. Let conversely f be surjective. Then for all $y \in X$ we have $f^{-1}(\{y\}) := \{x \in X; xf = y\} \neq \emptyset$. Hence for all $y \in X$, by the **Axiom of Choice** we pick an element $x_y \in X$ such that $x_y f = y$. This defines a map $g\colon X \to X\colon y \mapsto x_y$, and for all $y \in X$ we have $ygf = (yg)f = x_y f = y$, hence $gf = \mathrm{id}_X$, thus g is a left inverse of f.

Hence f is invertible if and only if f is bijective, the inverse of $f \in \mathrm{Maps}(X,X)$ being the inverse map $f^{-1} \in \mathrm{Maps}(X,X)$. The set $\mathcal{S}_X := \mathrm{Maps}(X,X)^* = \{f\colon X \to X; f \text{ bijective}\}$ is called the **symmetric group** on X; its elements are called **permutations**. In particular, if $X = \{1,\dots,n\}$ for some $n \in \mathbb{N}$ we write $\mathcal{S}_n := \mathcal{S}_{\{1,\dots,n\}}$; for $X = \emptyset$ we let $\mathcal{S}_0 := \{1\}$.

b) For $n \in \mathbb{N}$ we have $|\mathcal{S}_n| = n! := n(n-1)\cdots 1$, a **factorial**, as is seen by induction: For $n = 1$ we have $\mathcal{S}_1 = \{\mathrm{id}_{\{1\}}\}$. For $n \geq 2$ and $\pi \in \mathcal{S}_n$ we have $n\pi = m$ for some $m \in \{1,\dots,n\}$, and hence $\pi\colon \{1,\dots,n-1\} \to \{1,\dots,n\} \setminus \{m\}$ is bijective as well. Since there are n possibilities to choose m, there are $n \cdot |\mathcal{S}_{n-1}| = n!$ possibilities for π.

E. g. for $n = 3$ we have the following 6 permutations, where in the second row we record the images of the elements given in the first row:

$$\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}, \begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}, \begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}, \begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}, \begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}, \begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}.$$

More space saving is the **cycle notation**, where permutations are written as products of **disjoint cycles** and 1-cycles typically are left out. Due to bijectivity any permutation can be written uniquely this way, up to reordering the factors, where due to disjointness the order of the factors does not matter. If the cycles of a permutation have lengths $n_1 \geq n_2 \geq \cdots \geq n_r > 0$, where $r \in \mathbb{N}$, the partition $[n_1, n_2, \dots, n_r] \vdash n$ is called the associated **cycle type**.

E. g. we have $\mathcal{S}_1 = \{()\}$ and $\mathcal{S}_2 = \{(), (1,2)\}$, and ordering the elements as above $\mathcal{S}_3 = \{(1,2,3), (1,3), (2,3), (1,3,2), (), (1,2)\}$. Inverses are given by reading cycles backwardly, e. g. we have $(1,2,3)^{-1} = (1,3,2)$ and $(1,3,2)^{-1} = (1,2,3)$, while the other elements of $\mathcal{S}_3$ are their own inverses. While $\mathcal{S}_1$ and $\mathcal{S}_2$ are abelian, we from $(1,2,3)(1,2) = (1,3) \neq (2,3) = (1,2)(1,2,3)$ deduce that for $n \geq 3$ the group $\mathcal{S}_n$ is not abelian.

(1.5) Actions. a) Let G be a group, and let $X \neq \emptyset$ be a set. Then G is called to **act** on the G**-set** X, if there is an **action map** $X \times G \to X\colon [x,g] \mapsto xg$ such that **i)** $x1 = x$, and **ii)** $x(gh) = (xg)h$ for all $g, h \in G$ and $x \in X$.

Given an action of G on X, for $g \in G$ let $\varphi_g\colon X \to X\colon x \mapsto xg$. Hence from $\varphi_g\varphi_{g^{-1}} = \mathrm{id}_X = \varphi_{g^{-1}}\varphi_g$ we infer $\varphi_g \in \mathcal{S}_X$ for all $g \in G$, and since $\varphi_g\varphi_h = \varphi_{gh}$ for all $g, h \in G$ we have an **action homomorphism** $G \to \mathcal{S}_X\colon g \mapsto \varphi_g$. Conversely, if $\varphi\colon G \to \mathcal{S}_X\colon g \mapsto \varphi_g$ is a homomorphism, then $X \times G \to X\colon [x,g] \mapsto x\varphi_g$ defines an action of G on X: We have $\varphi_1 = \mathrm{id}_X \in \mathcal{S}_X$, and $\varphi_g\varphi_h = \varphi_{gh}$ implies $(xg)h = x(gh)$ for all $g, h \in G$ and $x \in X$.

If X and Y are G-sets, then a map $\alpha\colon X \to Y$ such that $(xg)\alpha = (x\alpha)g$ for all $x \in X$ and $g \in G$ is called a **(G-set) homomorphism**.

b) The relation $\mathcal{O} := \{[x,y] \in X \times X; y = xg \text{ for some } g \in G\}$ is an equivalence relation on X: From $x1 = x$ we infer that $\mathcal{O}$ is reflexive; from $y = xg$ we get $yg^{-1} = x$, implying that $\mathcal{O}$ is symmetric; and from $y = xg$ and $z = yh$ we get $z = xgh$, implying that $\mathcal{O}$ is transitive.

Given $x \in X$, its equivalence class $xG := \{xg \in X; g \in G\}$ again is a G-set, called the **(G-)orbit** of x; its cardinality $|xG|$ is called its **length**, and a subset $T \subseteq G$ such that $T \to xG\colon t \mapsto xt$ is a bijection is called a **transversal** of xG with respect to x; transversals exist by the Axiom of Choice.

Let $X/G := \{xG \subseteq X; x \in X\}$. A subset $S \subseteq X$ such that $S \to X/G\colon x \mapsto xG$ is a bijection is called a set of **orbit representatives** of X; orbit representatives exist by the Axiom of Choice, and we have $X = \coprod_{x \in S} xG$. If $X = xG$ for any and thus all $x \in X$, then X is called a **transitive** G-set.

For $x \in X$ let $\mathrm{Stab}_G(x) := G_x := \{g \in G; xg = x\} \subseteq G$ be the **stabiliser** of x in G. Then $\mathrm{Stab}_G(x) \leq G$: We have $1 \in \mathrm{Stab}_G(x) \neq \emptyset$, and for $g, h \in \mathrm{Stab}_G(x)$ from $xg = x = xh$ we get $xg^{-1} = x = xgh$, hence $g^{-1}, gh \in \mathrm{Stab}_G(x)$ as well. For $g \in G$ we have $\mathrm{Stab}_G(xg) = g^{-1}\mathrm{Stab}_G(x)g$: For $h \in \mathrm{Stab}_G(x)$ we have $(xg)g^{-1}hg = xg$, and the other inclusion follows from $x = (xg)g^{-1}$.

E. g. any group G acts **trivially** on any set $X \neq \emptyset$ by $\varphi_g\colon X \to X\colon x \mapsto x$ for all $g \in G$. The associated action homomorphism is $G \to \mathcal{S}_X\colon g \mapsto \mathrm{id}_X$, the orbits are the singleton subsets of X, and we have $\mathrm{Stab}_G(x) = G$ for all $x \in X$.

The group $\mathcal{S}_n$, for $n \in \mathbb{N}$, acts **naturally** on $\{1, \ldots, n\}$ by $\varphi_\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}\colon i \mapsto i\pi$ for all $\pi \in \mathcal{S}_n$. The associated action homomorphism is $\mathrm{id}_{\mathcal{S}_n}$, the action is transitive, and we have $\mathrm{Stab}_{\mathcal{S}_n}(n) = \{\pi \in \mathcal{S}_n; n\pi = n\} \cong \mathcal{S}_{n-1}$.

(1.6) Dihedral groups. Let $\mathbb{R}^2$ be the Euclidean plane equipped with the standard scalar product, and let $O_2(\mathbb{R}) := \{g \in \mathbb{R}^{2\times 2}; gg^{tr} = E_2\} \leq \mathrm{GL}_2(\mathbb{R})$ be the associated **orthogonal group**. We have $O_2(\mathbb{R}) = \{g \in O_2(\mathbb{R}); \det(g) = 1\} \dot\cup \{g \in O_2(\mathbb{R}); \det(g) = -1\}$, where the elements of the **special orthogonal group** $\mathrm{SO}_2(\mathbb{R}) := \{g \in O_2(\mathbb{R}); \det(g) = 1\} \leq O_2(\mathbb{R})$ are called **rotations**, while those of $O_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$ are called **reflections**.

For $n \geq 3$ let $\mathcal{D} \subseteq \mathbb{R}^2$ be a regular n-gon centred at the origin, and let $G := \{g \in O_2(\mathbb{R}); \mathcal{D}g = \mathcal{D}\} \leq O_2(\mathbb{R})$ be its **group of symmetries**, where $G \cap \mathrm{SO}_2(\mathbb{R}) = \{g \in \mathrm{SO}_2(\mathbb{R}); \mathcal{D}g = \mathcal{D}\}$ is called its **group of rotations**. Hence G acts transitively on the n vertices of $\mathcal{D}$, and numbering the vertices counterclockwise yields an action homomorphism $\varphi\colon G \to \mathcal{S}_n$. The image $D_{2n} := \mathrm{im}(\varphi) \leq \mathcal{S}_n$ is called the associated **dihedral group**. Since the vertices contain an $\mathbb{R}$-basis of $\mathbb{R}^2$, we conclude that $\varphi\colon G \to D_{2n}$ is an isomorphism.

We describe the elements of D_{2n}, showing that $|D_{2n}| = 2n$: Since rotations in $O_2(\mathbb{R})$ are determined by their rotation angle, the rotations in D_{2n} are those with angle $\frac{2\pi k}{n}$ for $k \in \{0, \ldots, n-1\}$. Thus D_{2n} contains precisely n rotations, given as $\tau_n^k \in \mathcal{S}_n$ for $k \in \{0, \ldots, n-1\}$, where $\tau_n := (1, 2, \ldots, n) \in \mathcal{S}_n$. Since reflections in $O_2(\mathbb{R})$ are determined by their reflection axis, we distinguish the cases n odd and n even:

For n odd the axis of a reflection in D_{2n} runs through one of the vertices of $\mathcal{D}$ and the edge opposite. Thus in this case D_{2n} contains precisely n reflections, one of them being $\sigma_n := (1)(2, n)(3, n-1)\cdots(\frac{n+1}{2}, \frac{n+3}{2}) \in \mathcal{S}_n$. For n even the axis of a

reflection in D_{2n} either runs through a pair of opposite vertices, or runs through a pair of opposite edges. Thus in this case D_{2n} contains precisely $\frac{n}{2} + \frac{n}{2} = n$ reflections, one of the former being $\sigma_n := (1)(\frac{n+2}{2})(2,n)(3,n-1)\cdots(\frac{n}{2},\frac{n+4}{2}) \in \mathcal{S}_n$ and one of the latter being $(1,2)(3,n)(4,n-1)\cdots(\frac{n+2}{2},\frac{n+4}{2}) \in \mathcal{S}_n$; e. g. the elements of $D_6 = \mathcal{S}_3$ and D_8 are given in Table 1. In both cases we have $|\mathrm{Stab}_{D_{2n}}(1)| = |\{(), \sigma_n\}| = 2$.

(1.7) Cosets. Let G be a group, and let $U \leq G$. Then U acts on G by **left multiplication** $\lambda_u \colon G \to G \colon x \mapsto u^{-1}x$ for all $u \in U$: We have $x\lambda_1 = 1^{-1}x = x$ and $x\lambda_{uv} = (uv)^{-1}x = v^{-1}u^{-1}x = (x\lambda_u)\lambda_v$ for all $x \in G$ and $u, v \in U$. Hence the U-orbit of $x \in G$ is the **(right) coset** $Ux := \{ux \in G; u \in U\} \subseteq G$.

The group G acts transitively on $U\backslash G := \{Ux \subseteq G; x \in G\}$ by **right multiplication** $\rho_g \colon U\backslash G \to U\backslash G \colon Ux \mapsto Uxg$ for all $g \in G$: We have $(Ux)1 = Ux$ and $(Ux)gh = (Uxg)h$ for all $g, h, x \in G$, and $Ux = (U \cdot 1)x$. Since $ug \in U$ if and only if $g \in U$, for $g \in G$, we have $\mathrm{Stab}_G(U \cdot 1) = U$.

A subset $T \subseteq G$ such that $T \to U\backslash G \colon t \mapsto Ut$ is a bijection is called a **(right) transversal** for U in G; in particular we have $G = \coprod_{t \in T} Ut$. The cardinality $[G \colon U] := |U\backslash G| = |T| \in \mathbb{N} \dot\cup \{\infty\}$ is called the **index** of U in G.

Similarly, we get **left cosets** and **left transversals**. If $T \subseteq G$ is a right transversal, from $G = \coprod_{t \in T} Ut$ by inversion $G \to G \colon g \mapsto g^{-1}$ we get $G = \coprod_{t \in T} t^{-1}U$, hence $T^{-1} := \{t^{-1} \in G; t \in T\}$ is a left transversal. Thus $[G \colon U]$ is independent from whether right or left cosets are considered. In general, left and right cosets do not coincide, and left transversals are not right transversals: E. g. for $U := \{(), (1,2)\} \leq G := \mathcal{S}_3$ we have $\mathcal{S}_3 = \{(), (1,2)\} \dot\cup \{(1,2,3), (2,3)\} \dot\cup \{(1,3,2), (1,3)\} = \{(), (1,2)\} \dot\cup \{(1,2,3), (1,3)\} \dot\cup \{(1,3,2), (1,3)\}$ as right and left cosets, respectively, hence a right transversal is $\{(), (1,2,3), (1,3)\}$, which is not a left transversal.

$U \leq G$ is called **normal**, if $gU \subseteq Ug$ for all $g \in G$; we write $U \trianglelefteq G$. In this case, from $Ug^{-1} \subseteq g^{-1}U$ we get $gU = Ug$, equivalently $g^{-1}Ug = U$. E. g. we have $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$, any subgroup of an abelian group is normal, and any subgroup of index 2, since $G = U \dot\cup Ug = U \dot\cup gU$ for any $g \in G \setminus U$, is normal.

(1.8) Theorem. Let G be a group, let X be a transitive G-set, and let $x \in X$. Then $\alpha \colon \mathrm{Stab}_G(x)\backslash G \to X \colon \mathrm{Stab}_G(x)g \mapsto xg$ is a G-set isomorphism.

Proof. For $g \in G$ and $u \in \mathrm{Stab}_G(x)$ we have $xug = xg$, hence α is well-defined. Since X is transitive α is surjective. For $g, g' \in G$ such that $xg = xg'$ we have $g'g^{-1} \in \mathrm{Stab}_G(x)$, hence $g' \in \mathrm{Stab}_G(x)g$, thus α is injective. We have $(\mathrm{Stab}_G(x)gh)^\alpha = xgh = (xg)h = (\mathrm{Stab}_G(x)g)^\alpha h$ for all $g, h \in G$. ♯

(1.9) Corollary: Lagrange. Let G be a finite group.
a) Let $U \leq G$. Then we have $[G \colon U] = \frac{|G|}{|U|}$; in particular we have $|U| \mid |G|$.

b) Let X be a transitive G-set. Then we have $|X| = [G\colon \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|}$ for any $x \in X$; in particular we have $|X| \mid |G|$.

Proof. a) Let $T \subseteq G$ be a transversal for U in G, hence $G = \coprod_{t\in T} Ut$. For the U-orbit Ut we have $\mathrm{Stab}_U(t) = \{u \in U; u^{-1}t = t\} = \{1\}$. Hence $U \to \{1\}\backslash U \to Ut\colon u \mapsto \{1\}u \mapsto u^{-1}t$ is a bijection, thus $|Ut| = |U|$ and $|G| = |T| \cdot |U|$. ♯

(1.10) Corollary: Cayley. G is isomorphic to a subgroup of $\mathcal{S}_G$.

Proof. Let G act **regularly** on G, i. e. by right multiplication, thus $G \cong \{1\}\backslash G$ as G-sets, and let $\rho\colon G \to \mathcal{S}_G$ be the associated action homomorphism. Since $g\rho = h\rho$ for $g, h \in G$ implies $g = 1 \cdot g = 1 \cdot h = h$, we infer that ρ is injective. ♯

(1.11) Theorem: Cauchy-Frobenius-Burnside Lemma. Let G be a finite group, and let X be a finite G-set. Then we have $|X/G| = \frac{1}{|G|} \cdot \sum_{g\in G} |\mathrm{Fix}_X(g)|$, where $\mathrm{Fix}_X(g) := \{x \in X; xg = x\}$ is the set of **fixed points** of $g \in G$.

Proof. Letting $\mathcal{O} := \{[x, g] \in X \times G; xg = x\}$ we use **double counting**: On the one hand we have $|\mathcal{O}| = \sum_{g\in G} |\{x \in X; xg = x\}| = \sum_{g\in G} |\mathrm{Fix}_X(g)|$. On the other hand we have $|\mathcal{O}| = \sum_{x\in X} |\{g \in G; xg = x\}| = \sum_{x\in X} |\mathrm{Stab}_G(x)|$. For $y \in xG$ we have $|yG| = |xG|$, and thus $|\mathrm{Stab}_G(x)| = |\mathrm{Stab}_G(y)|$. Letting $T \subseteq X$ be a set of orbit representatives, we get $\sum_{x\in X} |\mathrm{Stab}_G(x)| = \sum_{x\in T} \sum_{y\in xG} |\mathrm{Stab}_G(y)| = \sum_{x\in T} |xG| \cdot |\mathrm{Stab}_G(x)| = \sum_{x\in T} |G| = |X/G| \cdot |G|$. ♯

(1.12) Example. A **necklace** with $n \geq 3$ pearls having $k \in \mathbb{N}$ colours is a map $\eta\colon \{1, \ldots, n\} \to \{1, \ldots, k\}$. The set $\{1, \ldots, n\}$ may be considered as the set of vertices of a regular n-gon $\mathcal{D}$, and necklaces are called **equivalent** if they arise from each other by a symmetry of $\mathcal{D}$.

Let $\mathcal{N}_{n,k} := \{\eta\colon \{1, \ldots, n\} \to \{1, \ldots, k\}\}$ be the set of all necklaces, hence we have $|\mathcal{N}_{n,k}| = k^n$. Then $D_{2n} \leq \mathcal{S}_n$ acts on $\mathcal{N}_{n,k}$ by $\eta \mapsto \eta^\pi := \pi^{-1}\eta$ for all $\pi \in D_{2n}$. The equivalence classes of necklaces are precisely the orbits on $\mathcal{N}_{n,k}$, hence $t_{n,k} := |\mathcal{N}_{n,k}/D_{2n}| \in \mathbb{N}$ can be determined using Burnside's Lemma: For $\pi \in \mathcal{S}_n$ and $\eta \in \mathcal{N}_{n,k}$ we have $\eta^\pi = \eta$ if and only if $i\pi^{-1}\eta = i\eta$ for all $i \in \{1, \ldots, n\}$. This holds if and only if η is constant on the $r \in \mathbb{N}$ disjoint cycles of π, where 1-cycles count, yielding $|\mathrm{Fix}_{\mathcal{N}_{n,k}}(\pi)| = k^r$.

E. g. for $n = 3$ and $n = 4$ we from Table 1 get $t_{3,k} = \frac{1}{6} \cdot (k^3 + 3k^2 + 2k) = \frac{1}{6} \cdot k(k+1)(k+2) = \binom{k+2}{3}$ and $t_{4,k} = \frac{1}{8} \cdot (k^4 + 2k^3 + 3k^2 + 2k) = \frac{1}{8} \cdot k(k+1)(k^2+k+2)$.

2 Homomorphisms and subgroups

(2.1) Kernels. Let G and H be groups, let $\varphi\colon G \to H$ be a homomorphism, and let $\ker(\varphi) := \varphi^{-1}(\{1\}) = \{g \in G; g\varphi = 1\} \trianglelefteq G$ be its **kernel**: Since for $g \in G$ and $u \in \ker(\varphi)$ we have $(g^{-1}ug)\varphi = 1$, we infer $g^{-1} \ker(\varphi) g \subseteq \ker(\varphi)$.

Table 1: D_6 and D_8.

$\pi \in D_6$	type	r
()	$[1^3]$	3
$(1,2,3)$	$[3]$	1
$(1,3,2)$	$[3]$	1
$(2,3)$	$[2,1]$	2
$(1,2)$	$[2,1]$	2
$(1,3)$	$[2,1]$	2

$\pi \in D_8$	type	r
()	$[1^4]$	4
$(1,2,3,4)$	$[4]$	1
$(1,3)(2,4)$	$[2^2]$	2
$(1,4,3,2)$	$[4]$	1
$(2,4)$	$[2,1^2]$	3
$(1,3)$	$[2,1^2]$	3
$(1,2)(3,4)$	$[2^2]$	2
$(1,4)(2,3)$	$[2^2]$	2

For $g \in G$ and $h := g\varphi \in \mathrm{im}(\varphi)$, we have $\varphi^{-1}(\{h\}) = \ker(\varphi)g \in \ker(\varphi)\backslash G$: For $k \in \ker(\varphi)$ we have $(kg)\varphi = k\varphi \cdot g\varphi = h$, thus $\ker(\varphi)g \subseteq \varphi^{-1}(\{h\})$, and for $g' \in \varphi^{-1}(\{h\})$ we have $(g'g^{-1})\varphi = 1$, thus $g' = (g'g^{-1})g \in \ker(\varphi)g$. In particular, φ is injective if and only if $\ker(\varphi) = \{1\}$.

(2.2) Homomorphism Theorem. Let G be a group, and let $N \trianglelefteq G$.
a) G/N is a group with respect to $(gN)(hN) := ghN$ for all $g, h \in G$, called the associated **factor group** or **quotient group**, and the **natural map** $\nu_N \colon G \to G/N \colon g \mapsto gN$ is an epimorphism such that $\ker(\nu_N) = N$.
b) Let $\varphi \colon G \to H$ be a homomorphism such that $N \leq \ker(\varphi)$. Then the **induced map** $\varphi^N \colon G/N \to H \colon gN \mapsto g\varphi$ is a homomorphism such that $\ker(\varphi^N) = \ker(\varphi)/N$, yielding a **factorisation** $\varphi = \nu_N\varphi^N$. In particular, $\varphi^{\ker(\varphi)} \colon G/\ker(\varphi) \to \mathrm{im}(\varphi)$ is an isomorphism.

Proof. a) We only have to show that multiplication is well-defined: Let $g' \in gN$ and $h' \in hN$. Then we have $g' = gm$ and $h' = hn$ for some $m, n \in N$, and thus $g'h' = gm \cdot hn = gh \cdot h^{-1}mh \cdot n \in ghN$. For $g \in G$ we have $g \in \ker(\nu_N)$ if and only if $gN = N$, which holds if and only if $g \in N$.
b) The map φ^N is well-defined: Let $g' \in gN$, then we have $g' = gn$ for some $n \in N \leq \ker(\varphi)$, thus $g'\varphi = (gn)\varphi = g\varphi$. We have $(gN)^{\varphi^N} = 1$ if and only if $g\varphi = 1$, if and only if $g \in \ker(\varphi)$, if and only if $gN \in \ker(\varphi)/N$. ♯

(2.3) Corollary: Isomorphism Theorems. Let G be a group, and let $N \trianglelefteq G$.
a) Let $U \leq G$ and $M \trianglelefteq G$ such that $M \leq N$. Then we have $U/(U \cap N) \cong UN/N$ and $(G/M)/(N/M) \cong G/N$.
b) The map $\Phi \colon \{U \leq G; N \leq U\} \to \{V \leq G/N\} \colon U \mapsto U\nu_N = UN/N$ is an inclusion-preserving bijection with inverse $\Phi^{-1} \colon V \mapsto \nu_N^{-1}(V)$. The maps Φ and Φ^{-1} preserve normality, and if $[G \colon N]$ is finite then subgroup indices as well.

Proof. a) Since $NU = UN$ we have $N \trianglelefteq UN \leq G$, hence $\mathrm{im}((\nu_N)|_U) = UN/N$ and $\ker((\nu_N)|_U) = U \cap N \trianglelefteq U$; and we have $\ker(\nu_N^M) = N/M$.

b) Since $N\nu_N = 1$ we have $N \leq \nu_N^{-1}(V) \leq G$, hence Φ and Φ^{-1} are well-defined and inclusion-preserving. From $\nu_N^{-1}(U\nu_N) = \nu_N^{-1}(UN/N) = UN = U$ and $(\nu_N^{-1}(V))\nu_N = V$ we conclude that Φ and Φ^{-1} mutually inverse.

If $N \leq U \trianglelefteq G$, then for $g \in G$ we have $(gN)^{-1} \cdot UN/N \cdot gN = g^{-1}UgN/N = UN/N$, hence $UN/N \trianglelefteq G/N$, thus Φ preserves normality. If $V \trianglelefteq G/N$, then for $g \in G$ we have $(g^{-1}\nu_N^{-1}(V)g)\nu_N = (gN)^{-1} \cdot V \cdot gN = V$, hence $g^{-1}\nu_N^{-1}(V)g \subseteq \nu_N^{-1}(V)$, thus $\nu_N^{-1}(V) \trianglelefteq G$, hence Φ^{-1} preserves normality.

If $[G\colon N]$ is finite, then $[G\colon U]$ is finite as well, and letting $\{s_1, \ldots, s_m\} \subseteq U$ be a transversal for N, and $\{t_1, \ldots, t_n\} \subseteq G$ be a transversal for U, then $\{s_i t_j \in G; i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$ is a transversal for N in G. Hence we have $[G\colon U] = n = \frac{mn}{m} = \frac{[G\colon N]}{[U\colon N]} = \frac{|G/N|}{|UN/N|} = [(G/N)\colon (UN/N)]$. ♯

(2.4) Example. a) For the **trivial** homomorphism $\varphi\colon G \to H\colon g \mapsto 1$ we have $\ker(\varphi) = G$, yielding $G/G \cong \{1\}$. For the identity $\mathrm{id}_G\colon G \to G\colon g \mapsto g$ we have $\ker(\mathrm{id}_G) = \{1\}$, yielding $G/\{1\} \cong G$.
b) For $n \in \mathbb{N}$ we have $n\mathbb{Z} = -n\mathbb{Z} \trianglelefteq \mathbb{Z}$, where the natural homomorphism is given as $\nu_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\colon x \mapsto \overline{x} := x + n\mathbb{Z} = \{y \in \mathbb{Z}; y \equiv x \pmod n\}$. The set $\mathbb{Z}_n := \{0, \ldots, n-1\} \subseteq \mathbb{Z}$ is a transversal for $n\mathbb{Z}$, hence $\mathbb{Z}_n$ becomes an abelian group by using the bijection $\nu_n\colon \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$.
c) Let K be a field. Then $\det\colon \mathrm{GL}_n(K) \to K^*$ is surjective, letting $\mathrm{SL}_n(K) := \ker(\det) \trianglelefteq \mathrm{GL}_n(K)$ be the **special linear group** yields $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^*$.
d) $\exp\colon \mathbb{R} \to \mathbb{R}^*$ is a homomorphism from the additive group $\mathbb{R}$ to the multiplicative group $\mathbb{R}^*$, where $\mathrm{im}(\exp) = \mathbb{R}_{>0}$ and $\ker(\exp) = \{0\}$ yields $\mathbb{R} \cong \mathbb{R}_{>0}$.

(2.5) Lemma. Let $n \in \mathbb{N}$, and let $\pi \in \mathcal{S}_n$ be a product of $r \in \mathbb{N}$ disjoint cycles. If $\pi = \tau_1 \cdots \tau_s \in \mathcal{S}_n$, where $s \in \mathbb{N}_0$ and the $\tau_i \in \mathcal{S}_n$ are **transpositions**, i. e. 2-cycles, then we have $s \equiv n - r \pmod 2$.

Proof. We proceed by induction on $s \in \mathbb{N}_0$: For $s = 0$ we have $\pi = ()$, and hence $r = n$. For $s > 0$ let $\tau_s = (i, j) \in \mathcal{S}_n$, and let $\sigma := \tau_1 \cdots \tau_{s-1} \in \mathcal{S}_n$ be a product of $r' \in \mathbb{N}$ disjoint cycles, hence by induction we have $s - 1 \equiv n - r' \pmod 2$. If i, j occur in the same cycle of σ, then $\pi = \sigma\tau_s = (\ldots)(i, \ldots, k, j, \ldots, l)(i, j) = (\ldots)(i, \ldots, k)(j, \ldots, l)$, where possibly $k = i$ or $j = l$, hence π is a product of $r = r' + 1$ disjoint cycles. If i, j occur in distinct cycles of σ, then we have $\pi = \sigma\tau_s = (\ldots)(i, \ldots, k)(j, \ldots, l)(i, j) = (\ldots)(i \ldots k, j, \ldots, l)$, where possibly $k = i$ or $j = l$, hence π is a product of $r = r' - 1$ disjoint cycles. In both cases we have $n - r \equiv s \pmod 2$. ♯

(2.6) Alternating groups. For a n-cycle, for $n \geq 2$, we have $(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k) \in \mathcal{S}_n$, which is a product of $n - 1$ transpositions. Hence any finite permutation can be written as a product of transpositions. In general this representation is not unique, not even the number of transpositions is: $(1, 2, 3) = (1, 2)(1, 3) = (2, 3)(1, 2) = (1, 2)(2, 3)(1, 3)(1, 2) \in \mathcal{S}_3$.

Thus by (2.5) we for $n \in \mathbb{N}$ have the **sign** homomorphism $\operatorname{sgn}\colon \mathcal{S}_n \to \{\pm 1\}\colon \pi \mapsto (-1)^{n-r} = (-1)^s$, where π is a product of $r \in \mathbb{N}$ disjoint cycles, and a product of $s \in \mathbb{N}_0$ transpositions.

The kernel $\mathcal{A}_n := \ker(\operatorname{sgn}) \trianglelefteq \mathcal{S}_n$ is called the associated **alternating group**; the elements of $\mathcal{A}_n$ and $\mathcal{S}_n \setminus \mathcal{A}_n$ are called **even** and **odd** permutations, respectively. For $n \geq 2$ we from $\operatorname{sgn}((1,2)) = -1$ infer that sgn is surjective, hence we have $\mathcal{S}_n/\mathcal{A}_n \cong \{\pm 1\}$, in particular $|\mathcal{A}_n| = \frac{n!}{2}$; for $n = 1$ we have $\mathcal{A}_1 = \mathcal{S}_1 \cong \{1\}$.

(2.7) Generating sets. Let G be a group, and let $\{U_i \leq G; i \in \mathcal{I}\}$ where $\mathcal{I} \neq \emptyset$ is an index set. Then $\bigcap_{i\in\mathcal{I}} U_i \leq G$ is a subgroup, and if $U_i \trianglelefteq G$ for all $i \in \mathcal{I}$, then $\bigcap_{i\in\mathcal{I}} U_i \trianglelefteq G$ as well; in general $\bigcup_{i\in\mathcal{I}} U_i \subseteq G$ is not a subgroup.

Let $S \subseteq G$. Then $\langle S\rangle := \bigcap\{U \leq G; S \subseteq U\} \leq G$ is the smallest subgroup of G containing S, being called the subgroup **generated** by S, where S called a **generating set** of $\langle S\rangle$, and if S is finite then $\langle S\rangle$ is called **finitely generated**. Letting $S^{-1} := \{g^{-1}; g \in S\}$, we conclude that $\langle S\rangle$ consists of all finite products of elements of $S \cup S^{-1}$. E. g. we have $\langle\emptyset\rangle = \langle 1\rangle = \{1\}$ and $\langle G\rangle = G$, hence in particular any finite group is finitely generated.

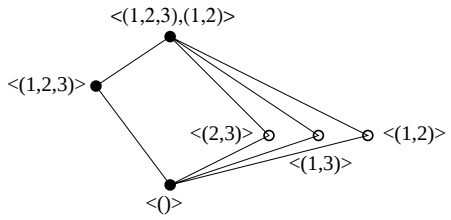
A subgroup $U \leq G$ is called **cyclic**, if there is $g \in U$ such that $U = \langle g\rangle$. For $g \in G$ we have $\langle g\rangle = \{g^k; k \in \mathbb{Z}\}$, where $|g| := |\langle g\rangle| \in \mathbb{N} \dot\cup \{\infty\}$ is called the **order** of g. Hence cyclic groups are abelian; e. g. we have $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$ and for $n \in \mathbb{N}$ we have $\mathbb{Z}/n\mathbb{Z} = \langle 1\rangle$. If G is finite, then we have $|g| \mid |G|$ for all $g \in G$; in particular, if $|G|$ is a prime then G is cyclic.

(2.8) Theorem: Cyclic groups. Let $G = \langle g\rangle$ be a cyclic group.
a) Then $\alpha_g\colon \mathbb{Z} \to G\colon k \mapsto g^k$ is an epimorphism. We have $\ker(\alpha_g)\{0\}$ if and only if G is infinite; in this case we have $\mathbb{Z} \cong G$. If G is finite then we have $\ker(\alpha_g) = |g|\mathbb{Z}$ and thus $\mathbb{Z}/|g|\mathbb{Z} \cong G = \{g^k; k \in \{0,\ldots,|g|-1\}\}$; in particular we have **Euler's Theorem** $g^{|G|} = g^{|g|} = 1$, and for any $n \in \mathbb{N} \dot\cup \{\infty\}$ up to isomorphism there is precisely one cyclic group C_n of order n.
b) Any non-trivial subgroup of G is cyclic of finite index. If G is infinite, then for all $m \in \mathbb{N}$ there is a unique subgroup of index m. If G is finite then there is a subgroup of index m if and only if $m \mid |g|$; in this case it is uniquely determined.
c) A finite group H is cyclic if and only if for any $m \in \mathbb{N}$ there is at most one subgroup of order m.

Proof. a) b) Let $\{0\} \neq U \trianglelefteq \mathbb{Z}$, and let $n \in \mathbb{N}$ be minimal such that $n \in U$, hence $n\mathbb{Z} \leq U$. For $k \in U$ let $i \in \mathbb{Z}$ and $j \in \{0,\ldots,n-1\}$ such that $k = in + j$, then from $j \in U$ and the choice of n we get $j = 0$, hence $k \in n\mathbb{Z}$, thus $n\mathbb{Z} = U$. Thus any non-trivial subgroup of $\mathbb{Z}$ is the form $n\mathbb{Z}$ for some $n \in \mathbb{N}$.

We have $\mathbb{Z}/\ker(\alpha_g) \cong G$, hence if $\ker(\alpha_g) = \{0\}$ then $\mathbb{Z} \cong G$ is infinite. If $\ker(\alpha_g) = n\mathbb{Z}$ for some $n \in \mathbb{N}$, then $\mathbb{Z}/n\mathbb{Z} \cong G$ is finite and $|g| = |\mathbb{Z}/n\mathbb{Z}| = n$, showing a). From $|\mathbb{Z}/n\mathbb{Z}| = n$ we infer that $n\mathbb{Z}$ is the unique subgroup of $\mathbb{Z}$ of

Table 2: Subgroup lattice of $\mathcal{S}_3$.



index n. This shows b) for G infinite, while for $\mathbb{Z}/n\mathbb{Z} \cong G$ finite, using $n\mathbb{Z} \leq m\mathbb{Z}$ if and only if $m \mid n$, the assertion follows from (2.3).

c) For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ the coset $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ is contained in a proper subgroup if and only if there is $1 \neq m \mid n$ such that $k \in m\mathbb{Z}$, i. e. $m \mid k$, which holds if and only if $\gcd(k, n) \neq \{\pm 1\}$, see (4.5). Thus $\langle \overline{k} \rangle = \mathbb{Z}/n\mathbb{Z}$ if and only if $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^* := \{\overline{x} \in \mathbb{Z}/n\mathbb{Z}; \gcd(x, n) = \{\pm 1\}\}$, where $\gcd(x, n)$ is independent of the chosen representative x. Letting $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^*| \in \mathbb{N}$ be **Euler's totient function**, the subgroup structure of $\mathbb{Z}/n\mathbb{Z}$ implies $\sum_{m \in \mathbb{N}, m \mid n} \varphi(m) = n$.

Let $H \neq \{1\}$ fulfil the assumption on subgroups. Then for $m \in \mathbb{N}$ there is an element of order m only if $m \mid n := |H|$, where there at most $\varphi(m)$ of them. Thus by $\sum_{m \in \mathbb{N}, n \neq m \mid n} \varphi(m) = n - \varphi(n) > 0$ there is an element of order n. ♯

(2.9) Example. a) We consider the dihedral group D_{2n} for $n \geq 3$, see (1.6): The subgroup of rotations $T_n := \{\tau_n^k; k \in \{0, \ldots, n-1\}\} = \langle \tau_n \rangle \leq D_{2n}$ is cyclic of order n. Since $[D_{2n} \colon T_n] = 2$ we have $T_n \trianglelefteq D_{2n}$, and from $\sigma_n \notin T_n$ we get $D_{2n} = \langle \tau_n, \sigma_n \rangle$. From $\sigma_n^{-1} \tau_n \sigma_n = (1, n, n-1, \ldots, 2) = \tau_n^{-1}$ we conclude that D_{2n} is not abelian. Any element $\pi \in D_{2n} = T_n \dot{\cup} \sigma_n T_n$ can be written uniquely as $\pi = \sigma_n^i \tau_n^k$, where $i \in \{0, 1\}$ and $k \in \{0, \ldots, n-1\}$, and multiplication is given by $\sigma_n^i \tau_n^k \cdot \sigma_n^{i'} \tau_n^{k'} = \sigma_n^{i+i'} \tau_n^{-ki'+k'}$.
b) We consider the symmetric group $\mathcal{S}_3$: We have $\mathcal{S}_3 = D_6 = \langle (1, 2, 3), (1, 2) \rangle$. As any non-cyclic subgroup coincides with $\mathcal{S}_3$, the only non-trivial proper subgroups are the non-normal cyclic subgroups $\langle (1, 2) \rangle$, $\langle (1, 3) \rangle$ and $\langle (2, 3) \rangle$ of order 2, and the normal cyclic subgroup $\langle (1, 2, 3) \rangle = \langle (1, 3, 2) \rangle$ of order 3. The **lattice of subgroups** is depicted as a **Hasse diagram** in Table 2.

(2.10) Conjugation action. Let G be a group, and let $\mathrm{Aut}(G)$ be the **group of automorphisms** of G, whose multiplication is given by composition of maps.

For $g \in G$ let $\kappa_g \colon G \to G \colon x \mapsto g^{-1} x g =: x^g$ be the associated **conjugation** map. Since $x^1 = x$ and $x^{gh} = h^{-1} g^{-1} x g h = (x^g)^h$, for all $x, g, h \in G$, this induces an action of G on G; in particular κ_g is bijective. The associated orbits are called the **conjugacy classes** of elements of G; the action is transitive if

and only if $G = \{1\}$. The stabiliser $C_G(x) := \mathrm{Stab}_G(x) = \{g \in G; x^g = x\} = \{g \in G; xg = gx\}$, for $x \in G$, is called the **centraliser** of x in G.

Since $(xy)^g = g^{-1}xyg = g^{-1}xg \cdot g^{-1}yg = x^g y^g$, for all $x, y, g \in G$, we conclude that κ_g is a homomorphism, hence $\kappa\colon G \to \mathrm{Aut}(G)\colon g \mapsto \kappa_g$. The image $\mathrm{Inn}(G) := \mathrm{im}(\kappa) \leq \mathrm{Aut}(G)$ is called the group of **inner automorphisms** of G; we have $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$: For all $x, g \in G$ and $\alpha \in \mathrm{Aut}(G)$ we have $x\kappa_g^\alpha = x\alpha^{-1}\kappa_g\alpha = (g^{-1}(x\alpha^{-1})g)\alpha = (g\alpha)^{-1}x(g\alpha) = x\kappa_{g\alpha}$, thus $\kappa_g^\alpha = \kappa_{g\alpha} \in \mathrm{Aut}(G)$.

The kernel $Z(G) := \ker(\kappa) = \bigcap_{x\in G} C_G(x) = \{g \in G; x^g = x \text{ for all } x \in G\} = \{g \in G; xg = gx \text{ for all } x \in G\} \trianglelefteq G$ is called the **centre** of G; hence we have $G/Z(G) \cong \mathrm{Inn}(G)$. The group G is abelian if and only if $G = Z(G)$, which holds if and only if $\mathrm{Inn}(G) = \{1\}$.

Similarly, G acts on the set of its subgroups via $\kappa_g\colon U \mapsto g^{-1}Ug =: U^g$, for all $U \leq G$ and $g \in G$. The associated orbits are called the **conjugacy classes** of subgroups of G; the action is transitive if and only if $G = \{1\}$. The stabiliser $N_G(U) := \mathrm{Stab}_G(U) = \{g \in G; U^g = U\} = \{g \in G; Ug = gU\}$, for $U \leq G$, is called the **normaliser** of U in G. Hence $U \leq N_G(U) \leq G$ is the largest subgroup of G having U as a normal subgroup; in particular $U \leq G$ is a fixed point if and only if $N_G(U) = G$, which holds if and only if $U \trianglelefteq G$.

(2.11) Definition. Let p be a prime, and let G be a finite group. If $|G| = p^d$, for some $d \in \mathbb{N}_0$, then G called a **p-group**; in particular $\{1\}$ is a p-group.

A p-subgroup $P \leq G$ such that $p \nmid [G\colon P] = \frac{|G|}{|P|}$ is called a **Sylow p-subgroup** of G. Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G; if $p \nmid |G|$ then we have $\mathrm{Syl}_p(G) = \{\{1\}\}$.

(2.12) Theorem. Let p be a prime, let G be a p-group, and let $\{1\} \neq N \trianglelefteq G$. Then we have $Z(G) \cap N \neq \{1\}$; in particular we have $Z(G) \neq \{1\}$.

Proof. The normal subgroup N is a union of conjugacy classes, hence let $T \subseteq G$ be a set of representatives of these classes. Since $Z(G) = \{g \in G; |g^G| = 1\} = \{g \in G; C_G(g) = G\}$, we have $Z(G) \cap N = Z(G) \cap T$ and thus $|N| = |Z(G) \cap N| + \sum_{g\in T\setminus Z(G)} \frac{|G|}{|C_G(g)|}$. For all $g \in G \setminus Z(G)$ we have $1 \neq \frac{|G|}{|C_G(g)|} \mid |G|$, thus $p \mid \frac{|G|}{|C_G(g)|}$, and hence $p \mid |N|$ implies $p \mid |Z(G) \cap N|$. ♯

(2.13) Theorem: Sylow [1872]. Let p be a prime, and G be a finite group.
a) If $p^d \mid |G|$ for some $d \in \mathbb{N}$, then $N_d := |\{Q \leq G; |Q| = p^d\}| \equiv 1 \pmod p$.
b) If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q^g \leq P$ for some $g \in G$.

Proof: Wielandt [1959]. a) G acts on $X := \{M \subseteq G; |M| = p^d\}$ by right multiplication. Let $X = \coprod_{i\in\mathcal{I}} X_i$ be its decomposition into orbits, where $\mathcal{I}$ is an index set, let $\{M_i \subseteq G; i \in \mathcal{I}\}$ be a set of orbit representatives, and let $G_i := \mathrm{Stab}_G(M_i) \leq G$. From $M_iG_i = M_i \subseteq G$ we conclude that M_i is a union

of left cosets of G_i in G, and thus $|G_i| \mid |M_i| = p^d$. Hence we have $|G_i| = p^{d_i}$ for some $d_i \in \{0, \ldots, d\}$.

If $Q \leq G$ such that $|Q| = p^d$, then $|\mathrm{Stab}_G(Q)| = |Q| = p^d$, and hence $Q \in X_i$ for some $i \in \mathcal{I}$ such that $d_i = d$. If $Q, Q' \leq G$ such that $|Q| = p^d = |Q'|$ are in the same orbit, then $Q' = Qg$ for some $g \in G$, thus $g \in Q'$, and hence $Q = Q'g^{-1} = Q'$. If $i \in \mathcal{I}$ such that $d_i = d$, then from $|M_i| = p^d = |G_i|$ we infer $M_i = g_i G_i$ for some $g_i \in G$. Thus for $M_i g_i^{-1} \in X_i$ we have $M_i g_i^{-1} = g_i G_i g_i^{-1} \leq G$. In conclusion, there is a bijection between the subgroups $Q \leq G$ such that $|Q| = p^d$ and the orbits X_i such that $d_i = d$.

If $d_i < d$, then $|X_i| = \frac{|G|}{|G_i|} = \frac{|G|}{p^{d_i}} \equiv 0 \pmod{\frac{|G|}{p^{d-1}}}$, yielding $\binom{|G|}{p^d} = |X| = \sum_{i \in \mathcal{I}} |X_i| \equiv \sum_{i \in \mathcal{I}; d_i = d} \frac{|G|}{p^d} = \frac{N_d |G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$. In particular for the cyclic group $C_{|G|}$ we from $|\{Q \leq C_{|G|}; |Q| = p^d\}| = 1$ get $\binom{|G|}{p^d} \equiv \frac{|G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$. This yields $\frac{|G|}{p^d} \equiv \frac{N_d |G|}{p^d} \pmod{\frac{|G|}{p^{d-1}}}$, thus $\frac{|G|}{p^{d-1}} \mid \frac{(N_d - 1)|G|}{p^d}$, hence $p \mid N_d - 1$.

b) Q acts on $P\backslash G$ by right multiplication, the orbits being $(Pg)^Q = \{Pgh \in P\backslash G; h \in Q\}$ for $g \in G$, and $PgQ = \bigcup (Pg)^Q \subseteq G$ is called the associated **P-Q-double coset**. Let $G = \coprod_{i \in \mathcal{I}} Pg_iQ$, where $\mathcal{I}$ is an index set and $g_i \in G$. For $h \in Q$ we have $Pgh = Pg \in P\backslash G$ if and only if $ghg^{-1} \in P$, thus $\mathrm{Stab}_Q(Pg) = Q \cap P^g$, hence $|G| = \sum_{i \in \mathcal{I}} |Pg_iQ| = \sum_{i \in \mathcal{I}} \frac{|Q||P|}{|Q \cap P^{g_i}|}$. Assume that $Q \cap P^{g_i} < Q$ for all $i \in \mathcal{I}$, then $p \mid \frac{|Q|}{|Q \cap P^{g_i}|}$, hence $p \mid \frac{|G|}{|P|}$, a contradiction. Thus there is $i \in \mathcal{I}$ such that $Q \cap P^{g_i} = Q$, implying $Q \leq P^{g_i}$. ♯

(2.14) Corollary. Both $\mathrm{Syl}_p(G)$ and $\{N_G(P); P \in \mathrm{Syl}_p(G)\}$ are a single conjugacy class of subgroups, and we have $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$ and $|\mathrm{Syl}_p(G)| = [G\colon N_G(P)] = \frac{|G|}{|N_G(P)|} \mid \frac{|G|}{|P|}$.

(2.15) Corollary: Cauchy's Theorem. If $p \mid |G|$, then G has an element of order p. Thus G is a p-group if and only if any element of G has p-power order.

(2.16) Example: The alternating group $\mathcal{A}_5$. a) Let $G := \mathcal{A}_5$, hence $|G| = 60 = 2^2 \cdot 3 \cdot 5$, and G contains 24 elements of cycle type $[5]$, 20 elements of cycle type $[3, 1^2]$, 15 elements of cycle type $[2^2, 1]$, and the identity of cycle type $[1^5]$. We determine the Sylow subgroups of G and their normalisers:

Any subgroup $P_5 \in \mathrm{Syl}_5(G)$ contains 4 elements of order 5. Since $P_5 \cap P_5^\pi = \{1\}$ for all $\pi \in G \setminus N_G(P_5)$, we have $|\mathrm{Syl}_5(G)| = 6$ and thus $|N_G(P_5)| = 10$. We have $D_{10} = \langle \tau_5, \sigma_5 \rangle < G$, see (1.6), thus $T_5 := \langle \tau_5 \rangle \in \mathrm{Syl}_5(G)$ and $N_G(T_5) = D_{10}$.

Any subgroup $P_3 \in \mathrm{Syl}_3(G)$ contains 2 elements of order 3. Since $P_3 \cap P_3^\pi = \{1\}$ for all $\pi \in G \setminus N_G(P_3)$, we have $|\mathrm{Syl}_3(G)| = 10$ and thus $|N_G(P_3)| = 6$. We have $\mathcal{A}_3 = \langle (1,2,3) \rangle \in \mathrm{Syl}_3(G)$ and $N_G(\mathcal{A}_3) = \langle (1,2,3), (1,2)(4,5) \rangle$. Since $N_G(\mathcal{A}_3) \to \mathcal{S}_3 \colon \pi \mapsto \pi|_{\{1,2,3\}}$ is an epimorphism we have $N_G(\mathcal{A}_3) \cong \mathcal{S}_3$.

Let $V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq \mathcal{S}_4$ be the **Klein 4-group**, which is a

non-cyclic abelian group of order 4, thus $V_4 \in \mathrm{Syl}_2(G)$. We have $V_4 \lhd \mathcal{A}_4 = \langle (1,2)(3,4), (1,2,3) \rangle < G$, thus $\mathcal{A}_4 \leq N_G(V_4)$. Since G has 15 elements of order 2, we have $|\mathrm{Syl}_2(G)| > 1$, thus $N_G(V_4) < G$, and hence $N_G(V_4) = \mathcal{A}_4$. Thus we have $|\mathrm{Syl}_2(G)| = 5$, implying $V_4 \cap V_4^\pi = \{1\}$ for all $\pi \in G \setminus N_G(V_4)$. ♯

A Sylow-type existence statement does not hold for arbitrary divisors of $|G|$, not even for those $n \mid |G|$ such that $\mathrm{ggT}(n, \frac{|G|}{n}) = 1$: Assume there is $U < G$ such that $|U| \in \{15, 20\}$, and let $P_5 \in \mathrm{Syl}_5(G)$ such that $P_5 < U$. From $|\mathrm{Syl}_5(U)| \mid \frac{|U|}{|P_5|} \in \{3, 4\}$ and $|\mathrm{Syl}_5(U)| \equiv 1 \pmod 5$ we get $|\mathrm{Syl}_5(U)| = 1$, thus $P_5 \lhd U$, hence $U \leq N_G(P_5)$, a contradiction.

b) We consider the **truncated icosahedron (Buckminsterfullerene, soccer ball)**, centred at the origin of the Euclidean space $\mathbb{R}^3$: The **icosahedron** is one of the 5 regular **platonic solids**, next to the **tetrahedron**, the **cube**, the **octahedron**, and the **dodecahedron**. The icosahedron has 20 triangular faces, and 12 vertices at each of which 5 of the faces meet. Truncating at the 12 vertices yields a regular solid having 60 vertices, and 12 pentagonal and 20 hexagonal faces, where each pentagonal face is surrounded by hexagonal ones, and each hexagonal face is surrounded by hexagonal and pentagonal ones.

We consider its group $G \leq \mathrm{SO}_3(\mathbb{R})$ of rotational symmetries, which acts regularly on the $12 \cdot 5 = 60$ pairs of adjacent pentagon-hexagon pairs, implying $|G| = 60$. There are 6 pairs of opposite pentagons, giving rise to 6 rotation axes of order 5, yielding 24 elements of order 5; there are 10 pairs of opposite hexagons, giving rise to 10 rotation axes of order 3, yielding 20 elements of order 3; and there are 30 hexagon-hexagon edges, giving rise to 15 opposite pairs, yielding 15 rotation axes of order 2, hence 15 elements of order 2.

We show that $G \cong \mathcal{A}_5$: Fixing a rotation axis of order 2, there are precisely two other rotation axes of order 2 orthogonal to the given one. The associated rotations $\tau_1, \tau_2 \in G$ and $\tau_3 = \tau_1\tau_2 \in G$ generate a non-cyclic abelian subgroup $V_4 \cong V := \langle \tau_1, \tau_2 \rangle \in \mathrm{Syl}_2(G)$. Moreover, the orthogonality argument implies $V \cap V^\pi = \{1\}$ for all $\pi \in G \setminus N_G(V)$, hence we have $|\mathrm{Syl}_2(G)| = 5$ and $|N_G(V)| = 12$. Thus the conjugation action of G on $\mathrm{Syl}_2(G)$ yields an action homomorphism $\varphi\colon G \to \mathcal{S}_5$. Then φ is injective such that $\mathrm{im}(\varphi) \leq \mathcal{A}_5$:

There is a rotation axis of order 3 such that conjugation with the associated rotation $\rho \in G$ yields $\kappa_\rho\colon \tau_1 \mapsto \tau_2 \mapsto \tau_3 \mapsto \tau_1$. Hence $N_G(V) = \langle V, \rho \rangle = \coprod_{k=0}^{2} \rho^k V$, thus any $\pi \in N_G(V)$ can be written uniquely as $\pi = \rho^k \tau_1^i \tau_2^j$, where $i, j \in \{0, 1\}$ and $k \in \{0, 1, 2\}$. Multiplication is determined by κ_ρ and V being abelian, thus $N_G(V) \to \mathcal{A}_4\colon \rho \mapsto (1,2,3), \tau_1 \mapsto (1,2)(3,4), \tau_2 \mapsto (1,4)(2,3)$ is an isomorphism. Hence $N_G(V)$ is generated by elements of order 3, and joining an element of order 5 shows that G is generated by elements of odd order, thus $\mathrm{im}(\varphi) \leq \mathcal{A}_5$. Assume that $\{1\} \neq \ker(\varphi) \trianglelefteq G$. Since $V \lhd N_G(V)$ is the only non-trivial proper normal subgroup, we get $V \leq \ker(\varphi) \leq N_G(V)$, hence $V^\pi \leq \ker(\varphi)$ and thus $V = V^\pi$, for all $\pi \in G$, contradicting $V \cap V^\pi = \{1\}$ for all $\pi \in G \setminus N_G(V)$. ♯

3 Rings and domains

(3.1) Rings and ideals. a) A set R together with an **addition** $+\colon R \times R \to R\colon [a,b] \mapsto a+b$ and a **multiplication** $\cdot\colon R \times R \to R\colon [a,b] \mapsto ab$ fulfilling the following conditions is called a **ring**:
i) R is an additive abelian group with neutral element 0,
ii) R is a multiplicative monoid with neutral element 1,
iii) and we have **distributivity** $a(b+c) = (ab)+(ac)$ and $(a+b)c = (ac)+(bc)$ for all $a, b, c, \in R$.

If $ab = ba$ holds for all $a, b \in R$ then R is called **commutative**.

For all $a \in R$ we have $0a = (0+0)a = (0a) + (0a)$, hence $0a = 0$, and similarly $a0 = 0$; and we have $a + (-1)a = (1 + (-1))a = 0a = 0$, hence $-a = (-1)a$, and similarly $-a = a(-1)$. Thus for all $a, b \in R$ we have $-(ab) = (-1)ab = (-a)b$ and $-(ab) = ab(-1) = a(-b)$. For all $a, b \in R$ such that $ab = ba$ we have the **binomial formula** $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$ for all $n \in \mathbb{N}$.

E. g. let $R := \{0\}$ with addition and multiplication given by $0 + 0 := 0$ and $0 \cdot 0 := 0$, respectively, and $1 := 0$, then R is a commutative ring, called the **zero ring**. Conversely, for any ring R fulfilling $1 = 0$ we have $a = 1a = 0a = 0$ for all $a \in R$, hence we have $R = \{0\}$. Thus for any ring $R \neq \{0\}$ we have $1 \neq 0$.

Let $R^* \subseteq R$ be the group of multiplicative units. Hence for $R \neq \{0\}$ we have $1 \in R^* \subseteq R \setminus \{0\}$. A ring $R \neq \{0\}$ such that $R^* = R \setminus \{0\}$ is called a **skew field** or **division ring**; a commutative skew field is called a **field**.

A subset $S \subseteq R$ being an additive subgroup and a multiplicative submonoid is called a **subring**; in particular we have $1 \in R$. The pair $S \subseteq R$ is called a **ring extension**. Similarly we have **sub(skew)fields** and **(skew) field extensions**; e. g. $\mathbb{Z} \subseteq \mathbb{Q}$ is a ring extension and $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are field extensions.

If R and S are rings, a map $\varphi\colon R \to S$ which is homomorphism of additive groups and a homomorphism of multiplicative monoids is called a **(ring) homomorphism**; in particular we have $1\varphi = 1$ and thus $\mathrm{im}(\varphi) \subseteq S$ is a subring.

For the **kernel** $\ker(\varphi) := \varphi^{-1}(\{0\}) = \{a \in R; a\varphi = 0\}$ we have $\ker(\varphi) \leq R$ as additive groups. If $S \neq \{0\}$ then from $1\varphi = 1$ we deduce that $1 \notin \ker(\varphi)$, hence $\ker(\varphi) \subseteq R$ in general is not a subring. For all $a \in R$ and $b \in \ker(\varphi)$ we have $(ab)\varphi = a\varphi \cdot b\varphi = a\varphi \cdot 0 = 0$ and $(ba)\varphi = b\varphi \cdot a\varphi = 0 \cdot a\varphi = 0$, implying $R\ker(\varphi)R \subseteq \ker(\varphi)$, thus fulfilling the following:

b) An additive subgroup $I \leq R$ such that $RIR := \{abc \in R; a, c \in R, b \in I\} \subseteq I$ is called an **ideal** of R; we write $I \trianglelefteq R$, and if R is commutative then $RIR = RI = IR$. E. g. we have $\{0\} \trianglelefteq R$ and $R \trianglelefteq R$; if $R \neq \{0\}$ and these are the only ideals of R, then R is called **simple**.

Let $\{I_i \trianglelefteq R; i \in \mathcal{I}\}$, where $\mathcal{I} \neq \emptyset$ is an index set. Then $I := \bigcap_{i \in \mathcal{I}} I_i \trianglelefteq R$ is an ideal. Hence for a subset $S \subseteq R$ let $\langle S \rangle = \langle S \rangle_R := \bigcap \{I \trianglelefteq R; S \subseteq I\} \trianglelefteq R$ be the smallest ideal of R containing S, being called the ideal **generated** by S. For $S \neq \emptyset$ the ideal $\langle S \rangle$ consists of all finite sums of elements of $RSR := \{asb \in R; a, b \in R, s \in$

$S\}$; hence we also write $\langle S\rangle = \sum_{s\in S} RsR$, and if $S = \{s_1, \dots, s_n\}$ is finite we also write $\langle S\rangle = \langle s_1, \dots, s_n\rangle = Rs_1R + \dots + Rs_nR$.

Given $I, J \trianglelefteq R$, then $I + J := \langle I, J\rangle = \{a + b \in R; a \in I, b \in J\} \trianglelefteq R$ is called their **sum**, where $I \cup J \subseteq I + J$, and $\langle IJ\rangle \trianglelefteq R$ consisting of all finite sums of elements of $IJ := \{ab \in R; a \in I, b \in J\}$ is called their **product**, where $\langle IJ\rangle \subseteq I \cap J$. Given $a \in R$, the ideal $\langle a\rangle = RaR \trianglelefteq R$ is called the associated **principal ideal**. E. g. we have $\langle\emptyset\rangle = \langle 0\rangle = \{0\}$ and $\langle 1\rangle = R$, and for $n \in \mathbb{Z}$ we have $\langle n\rangle = n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

(3.2) Homomorphism Theorem. Let R be a ring, and let $I \trianglelefteq R$.
a) R/I is a ring with respect to $(a + I)(b + I) := ab + I$ for all $a, b \in R$, called the associated **quotient ring**, and the natural map $\nu_I\colon R \to R/I\colon a \mapsto a + I$ is an epimorphism such that $\ker(\nu_I) = I$.
b) Let $\varphi\colon R \to S$ be a homomorphism such that $I \subseteq \ker(\varphi)$. Then the induced map $\varphi^I\colon R/I \to S\colon a + I \mapsto a\varphi$ is a homomorphism such that $\ker(\varphi^I) = \ker(\varphi)/I$, yielding a factorisation $\varphi = \nu_I\varphi^I$. In particular, $\varphi^{\ker(\varphi)}\colon R/\ker(\varphi) \to \mathrm{im}(\varphi)$ is an isomorphism.

Proof. a) b) By the homomorphism theorem for groups we only have to show that multiplication on R/I is well-defined: For $c, c' \in I$ we have $(a+c)(b+c') = ab + ac' + cb + cc' \in ab + I$. ♯

(3.3) Corollary: Isomorphism Theorems. Let R be a ring, and let $I \trianglelefteq R$.
a) Let $S \subseteq R$ be a subring and $J \trianglelefteq R$ such that $J \subseteq I$. Then we have $S/(S\cap I) \cong (S + I)/I$ and $(R/J)/(I/J) \cong R/I$.
b) The map $\Phi\colon \{J \trianglelefteq R; I \subseteq J\} \to \{Q \trianglelefteq R/I\}\colon J \mapsto J\nu_I = (J + I)/I$ is an inclusion-preserving bijection with inverse $\Phi^{-1}\colon Q \mapsto \nu_I^{-1}(Q)$. If $|R/I|$ is finite then Φ and Φ^{-1} preserve cardinalities of quotient rings.

(3.4) Maximal ideals. Let R be a ring and $I \trianglelefteq R$. Then $I \cap R^* \neq \emptyset$ implies $R \subseteq RIR \subseteq I \subseteq R$ and hence $I = R$, thus we have $I \triangleleft R$ if and only if $I \cap R^* = \emptyset$. An ideal $I \triangleleft R$ is called **maximal**, if for any ideal $I \subseteq J \triangleleft R$ we already have $I = J$. Thus an ideal $I \trianglelefteq R$ is maximal if and only if R/I is simple.

Hence any skew field K is a simple ring; and since for any homomorphism $\varphi\colon K \to R$ we have $\ker(\varphi) \trianglelefteq K$, we conclude that either $\ker(\varphi) = K$ or $\ker(\varphi) = \{0\}$, i. e. either $\varphi = 0$ or φ is injective. Conversely, any commutative simple ring R is a field: For any $0 \neq a \in R$ we have $\{0\} \neq aR \trianglelefteq R$, hence $R = aR$, and thus there is $b \in R$ such that $ab = 1$, hence $a \in R^*$. Thus if R is commutative, then an ideal $I \trianglelefteq R$ is maximal if and only if R/I is a field; in particular R is a field if and only if $I \triangleleft R$ is maximal.

E. g. let K be a field. Then $\mathrm{Maps}(K, K)$ becomes is a commutative ring with respect to **pointwise** addition and multiplication $f+g\colon K \to K\colon x \mapsto f(x)+g(x)$ and $fg\colon K \to K\colon x \mapsto f(x)g(x)$, respectively, for all $f, g \in \mathrm{Maps}(K, K)$, where the neutral elements are $K \to K\colon x \mapsto 0$ and $K \to K\colon x \mapsto 1$, respectively. For

any subset $U \subseteq K$ we have $I_U := \{f \in \mathrm{Maps}(K,K); f(U) = \{0\}\} \trianglelefteq \mathrm{Maps}(K,K)$, where $U \subseteq V \subseteq K$ implies $I_V \subseteq I_U$. Then $I_x := I_{\{x\}} \trianglelefteq \mathrm{Maps}(K,K)$ is maximal for any $x \in K$: Let $\nu_x \colon \mathrm{Maps}(K,K) \to K \colon f \mapsto f(x)$ be the natural **evaluation map**. Then ν_x is an epimorphism such that $\ker(\nu_x) = I_x$, and hence $\mathrm{Maps}(K,K)/I_x \cong K$ is a field, implying that $I_x \lhd \mathrm{Maps}(K,K)$ is maximal.

(3.5) Zorn's Lemma. Let X be a set, let $\leq$ be a **partial order** on X, i. e. $\leq$ is a reflexive, antisymmetric and transitive relation on X, and let $Y \subseteq X$. Then Y is called **totally ordered**, if for all $y, y' \in Y$ we have $y \leq y'$ or $y' \leq y$. An element $x \in X$ such that $y \leq x$ for all $y \in Y$ is called an **upper bound** for Y. An element $y \in Y$ such that for any $y' \in Y$ such that $y \leq y'$ we already have $y = y'$ is called a **maximal element** of Y.

E. g. if M is a set, then its power set is partially ordered by inclusion $\subseteq$. In particular, if R is a ring then the set $\{I \lhd R\}$ is partially ordered by inclusion, and an ideal of R is maximal if and only if it is a maximal element of $\{I \lhd R\}$.

We have **Zorn's Lemma**, actually being equivalent to the Axiom of Choice: If $X \neq \emptyset$ is a partially ordered set, such that any totally ordered subset of X has an upper bound in X, then X has a maximal element.

(3.6) Theorem. Let R be a ring and $I \lhd R$. Then there is a maximal ideal $P \lhd R$ such that $I \subseteq P$. In particular any ring $R \neq \{0\}$ has a maximal ideal.

Proof. Let $\mathcal{X} := \{J \lhd R; I \subseteq J\}$. Hence $I \in \mathcal{X} \neq \emptyset$, and $\mathcal{X}$ is partially ordered by inclusion. Let $\emptyset \neq \mathcal{Y} \subseteq \mathcal{X}$ be totally ordered, and let $M := \bigcup_{J \in \mathcal{Y}} J \subseteq R$. Then $I \subseteq M \lhd R$: Let $J \subseteq J' \in \mathcal{Y}$, and $a \in J$ and $b \in J'$. Hence we have $RaR \subseteq J \subseteq M$ and $a - b \in J' \subseteq M$, implying $M \trianglelefteq R$. Since $1 \notin J$ for all $J \in \mathcal{Y}$, we have $1 \notin M \subset R$. Hence $M \in \mathcal{X}$ is an upper bound for $\mathcal{Y}$, and by Zorn's Lemma $\mathcal{X}$ has a maximal element. ♯

(3.7) Integral domains. Let $R \neq \{0\}$ be a commutative ring. Then $a \in R$ is called a **divisor** of $b \in R$, and b is called a **multiple** of a, if there is $c \in R$ such that $ac = b$; we write $a \mid b$, and we have $a \mid b$ if and only if $bR \subseteq aR \trianglelefteq R$. We have $a \mid 0$ and $a \mid a$, and $u \mid a$ for all $u \in R^*$. Since $aR = R$ if and only if $a \in R^*$, we have $a \mid u$, for any $u \in R^*$, if and only if $a \in R^*$.

An element $0 \neq a \in R$ such that there is $0 \neq b \in R$ such that $ab = 0$ is called a **zero-divisor** in R. If R does not contain any zero-divisors, i. e. if $ab = 0$ implies $a = 0$ or $b = 0$, for all $a, b \in R$, then R is called an **integral domain**. Thus if $0 \neq a \in R$ then $ab = ac$ implies $a(b - c) = 0$ and hence $b = c$, for all $b, c \in R$. If $a \in R^*$ then from $ab = 0$, for any $b \in R$, we get $b = a^{-1}ab = 0$, hence $a \in R$ is not a zero-divisor. In particular any field, and thus any subring of a field, is an integral domain; e. g. $\mathbb{Z}$ is an integral domain.

An ideal $I \lhd R$ is called a **prime ideal**, if $ab \in I$ implies $a \in I$ or $b \in I$, for all $a, b \in R$. Hence an ideal $I \trianglelefteq R$ is prime if and only if R/I is an integral domain;

in particular R is an integral domain if and only if $\{0\} \lhd R$ is prime. If $I \lhd R$ is maximal, then R/I is a field, thus an integral domain, hence $I \lhd R$ is prime.

E. g. let $n \in \mathbb{Z} \setminus \{0,1\}$ be **squarefree**, i. e. in the factorisation of n any prime occurs at most once, see (4.4). Let $\sqrt{n} \in \mathbb{R}_{\geq 0} \subseteq \mathbb{C}$ if $n > 0$, and $\sqrt{n} := \sqrt{-1} \cdot \sqrt{|n|} \in \mathbb{C}$ if $n < 0$, where $\sqrt{-1} \in \mathbb{C}$ is the imaginary unit. Let $\mathbb{Z}[\sqrt{n}] := \{a+b\sqrt{n} \in \mathbb{C}; a, b \in \mathbb{Z}\}$; for $n = -1$ the elements of $\mathbb{Z}[\sqrt{-1}]$ are called **Gaussian integers**. Then $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$ is a subring, thus an integral domain.

(3.8) Fields of fractions. Let R be an integral domain, and let the relation $\sim$ on $R \times (R \setminus \{0\})$ be defined by $[a, b] \sim [a', b']$ if and only if $ab' = a'b \in R$. Then $\sim$ is an equivalence relation, where we only have to show transitivity: Letting $[a, b] \sim [a', b']$ and $[a', b'] \sim [a'', b'']$, then $ab' = a'b$ and $a'b'' = a''b'$ imply $ab'b'' = a'bb'' = a''b'b$, thus $b' \neq 0$ implies $ab'' = a''b$, hence $[a, b] \sim [a'', b'']$.

For $a, b \in R$ such that $b \neq 0$ let $\frac{a}{b} := [a, b]/_\sim \subseteq R \times (R \setminus \{0\})$ denote the associated equivalence class, and let $\mathcal{Q}(R) := \{\frac{a}{b} \subseteq R \times (R \setminus \{0\}); a, b \in R, b \neq 0\}$; be the set of all equivalence classes; e. g. we have $\mathcal{Q}(\mathbb{Z}) = \mathbb{Q}$. Then $\mathcal{Q}(R)$ is a field, called the **field of fractions** of R:

By $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$, for all $a, b, c, d \in R$ such that $b, d \neq 0$, we get an addition and a multiplication on $\mathcal{Q}(R)$, respectively: If $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$ for $a', b', c', d' \in R$ such that $b', d' \neq 0$, then we have $ab' = a'b$ and $cd' = c'd$, and thus $(ad + bc)b'd' - (a'd' + b'c')bd = ab'dd' + bb'cd' - a'bdd' - c'dbb' = 0$ and $acb'd' - a'c'bd = ab'cd' - a'bc'd = 0$. Then $\mathcal{Q}(R)$ is abelian additive group with neutral element $\frac{0}{1}$, the additive inverse of $\frac{a}{b} \in \mathcal{Q}(R)$ given by $\frac{-a}{b} \in \mathcal{Q}(R)$, and a commutative multiplicative monoid with neutral element $\frac{1}{1}$, such that distributivity holds. For $\frac{0}{1} \neq \frac{a}{b} \in \mathcal{Q}(R)$ we have $a \neq 0$, thus $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1} \in \mathcal{Q}(R)$ implies $\frac{a}{b} \in \mathcal{Q}(R)^*$, where $(\frac{a}{b})^{-1} = \frac{b}{a}$. ♯

The map $R \to \mathcal{Q}(R)\colon a \mapsto \frac{a}{1}$ is a monomorphism, hence $R \subseteq \mathcal{Q}(R)$ can be considered as a subring. If $S \neq \{0\}$ is a commutative ring, and $\varphi\colon R \to S$ is a homomorphism such that $\varphi(R \setminus \{0\}) \subseteq S^*$, hence in particular $\ker(\varphi) = \{0\}$, then φ uniquely extends to a monomorphism $\widehat{\varphi}\colon \mathcal{Q}(R) \to S\colon \frac{a}{b} \mapsto a^\varphi (b^\varphi)^{-1}$; in particular if R is a field then $R \cong \mathcal{Q}(R)$: If $\frac{a}{b} = \frac{a'}{b'} \in \mathcal{Q}(R)$, where $a, b, a', b' \in R$ and $b, b' \neq 0$, then $ab' = a'b \in R$ implies $a^\varphi (b')^\varphi = (a')^\varphi b^\varphi \in S$, where $b^\varphi, (b')^\varphi \neq 0$, hence $a^\varphi (b^\varphi)^{-1} = (a')^\varphi ((b')^\varphi)^{-1} \in S$. Thus $\widehat{\varphi}$ is well-defined, and since $\frac{a}{b} = \frac{a}{1} \cdot (\frac{b}{1})^{-1} \in \mathcal{Q}(R)$ we conclude that $\widehat{\varphi}$ is uniquely determined by φ.

E. g. for $n \in \mathbb{Z} \setminus \{0,1\}$ squarefree we have $\mathcal{Q}(\mathbb{Z}[\sqrt{n}]) \cong \mathbb{Q}(\sqrt{n}) := \{a + b\sqrt{n} \in \mathbb{C}; a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$: Since for $a, b \in \mathbb{Q}$ such that $[a, b] \neq [0, 0]$ we have $\frac{1}{a+b\sqrt{n}} = \frac{a-b\sqrt{n}}{(a+b\sqrt{n})(a-b\sqrt{n})} = \frac{a-b\sqrt{n}}{a^2-nb^2} \in \mathbb{C}$, we conclude that $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{C}$ is a subfield containing $\mathbb{Z}[\sqrt{n}]$, hence we have $\mathbb{Q} \dot\cup \{\sqrt{n}\} \subseteq \mathcal{Q}(\mathbb{Z}[\sqrt{n}]) \subseteq \mathbb{Q}(\sqrt{n})$.

(3.9) Monoid rings. Let R be a commutative ring, let G be a monoid, and let $R[G] := \{\rho\colon G \to R; x\rho = 0 \text{ for almost all } x \in G\}$; the elements of $R[G]$ can be written as $\rho = \sum_{x \in G} \rho_x x$, where $\rho_x := x\rho \in R$ and the sum is indeed

finite. For $\rho, \sigma \in R[G]$ we define pointwise addition $\rho + \sigma := \sum_{z \in G}(\rho_z + \sigma_z)z$ and **convolutional** multiplication $\rho\sigma := \sum_{x \in G}\sum_{y \in G}\rho_x\sigma_y xy$. For $x \in G$ let $\delta_x \colon G \to R$ be given by $\delta_{x,x} = 1$ and $\delta_{x,y} = 0$ for all $x \neq y \in G$.

Then $R[G]$ is an abelian additive group with neutral element $\sum_{x \in G} 0_x x$, where $0_x := 0$ for all $x \in G$. Then $R[G]$ is a multiplicative monoid with neutral element δ_1: For all $\rho \in R[G]$ we have $\delta_1\rho = (\sum_{x \in G}\delta_{1,x}x)(\sum_{y \in G}\rho_y y) = \sum_{x \in G}\sum_{y \in G}\delta_{1,x}\rho_y xy = \sum_{y \in G}\rho_y y = \rho$ and similarly $\rho\delta_1 = \rho$. Since convolutional multiplication is associative, $R[G]$ is a multiplicative monoid, and since distributivity holds, $R[G]$ is a ring, called the **monoid ring** of G over R.

Since $\delta_x\delta_y = \sum_{z \in G}\sum_{z' \in G}\delta_{x,z}\delta_{y,z'}zz' = \sum_{z'' \in G}\delta_{xy,z''}z'' = \delta_{xy}$ for all $x, y \in G$, we have a monoid monomorphism $G \to R[G] \colon x \mapsto \delta_x$. Hence $G \subseteq R[G]$ can be considered as a submonoid, and convolutional multiplication is by distributivity determined by multiplication in G; in particular, $R[G]$ is a commutative ring if and only G is a commutative monoid.

We define a **scalar multiplication** $R[G] \times R \to R[G]$ by $\rho r := \sum_{x \in G} r\rho_x x$ for all $\rho \in R[G]$ and $r \in R$. This yields a ring monomorphism $R \to R[G] \colon r \mapsto \delta_1 r$, hence $R \subseteq R[G]$ can be considered as a subring. If K is a field, then $K[G]$ becomes a K-vector space having the submonoid $G \subseteq K[G]$ as a K-basis.

(3.10) Polynomial rings. Let X be a **variable** or **indeterminate**. The set $\{X^i; i \in \mathbb{N}_0\} = \{\epsilon, X, XX, XXX, \ldots\}$ of **words** in X, where $X^0 = \epsilon$ is the **empty word**, is a commutative monoid with respect to **concatenation** of words, having neutral element X^0, being called the **free monoid** over X.

Let R be a commutative ring. The monoid ring $R[X] := R[\{X^i; i \in \mathbb{N}_0\}]$ is called the **(univariate) polynomial ring** in X over R. The elements $f = \sum_{i \geq 0} a_i X^i \in R[X]$ are called **polynomials**, where $a_i \in R$ is called the i-th **coefficient** of f. If $f \neq 0$ let $\deg(f) := \max\{i \in \mathbb{N}_0; a_i \neq 0\} \in \mathbb{N}_0$ be its **degree**; polynomials of degree $0, \ldots, 3$ are called **constant**, **linear**, **quadratic** and **cubic**, respectively. Let $\mathrm{lc}(f) := a_{\deg(f)} \in R$ be its **leading coefficient**; if $\mathrm{lc}(f) = 1$ then f is called **monic**.

For $g = \sum_{j \geq 0} b_j X^j \in R[X]$ we have $fg = \sum_{k \geq 0}(\sum_{l=0}^{k} a_l b_{k-l})X^k \in R[X]$, Hence for the **degree function** $\deg \colon R[X] \setminus \{0\} \to \mathbb{N}_0$ we have either $fg = 0$, or $f, g \neq 0$ and $\deg(fg) \leq \deg(f) + \deg(g)$. If $\mathrm{lc}(f)\mathrm{lc}(g) \neq 0$, then we have $fg \neq 0$ where $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g)$ and $\deg(fg) = \deg(f) + \deg(g)$.

Hence for any $0 \neq f \in R[X]$ such that $\mathrm{lc}(f) \in R$ is not a zero-divisor, $f \in R[X]$ is not a zero-divisor either. Thus, since $R \subseteq R[X]$ is a subring, $R[X]$ is an integral domain if and only if R is; in this case we have $R[X]^* = R^*$. If R is an integral domain $R(X) := \mathcal{Q}(R[X])$ is called the **field of rational functions** in X over R; hence we have $R \subseteq R[X] \subseteq \mathcal{Q}(R)[X] \subseteq R(X)$ as subrings, yielding $\mathcal{Q}(R[X]) = \mathcal{Q}(\mathcal{Q}(R)[X]) = \mathcal{Q}(R)(X) = R(X)$.

More generally, let $\mathcal{X} \neq \emptyset$ be set of **commuting indeterminates**. Then the set of **commutative words** in $\mathcal{X}$ is a commutative monoid with respect to

concatenation of words, having the empty word as neutral element, and being called the **free commutative monoid** over $\mathcal{X}$. The associated monoid ring $R[\mathcal{X}]$ is called the associated **(multivariate) polynomial ring**. For $X \in \mathcal{X}$ we have $R[\mathcal{X}] \cong R[\mathcal{X} \setminus \{X\}][X]$, and if R is an integral domain then $R[\mathcal{X}]$ is as well and $R(\mathcal{X}) := \mathcal{Q}(R[\mathcal{X}])$ is the associated **field of rational functions**.

(3.11) Proposition. Let $R \neq \{0\}$ be a commutative ring, let $f \in R[X]$ and let $0 \neq g \in R[X]$ such that $\mathrm{lc}(g) \in R^*$. Then there are uniquely determined $q, r \in R[X]$, called **quotient** and **remainder**, respectively, such that $f = qg + r$ where $r = 0$ or $\deg(r) < \deg(g)$.

Proof. Let $qg + r = f = q'g + r'$ where $q, q', r, r' \in R[X]$ such that $r = 0$ or $\deg(r) < \deg(g)$, and $r' = 0$ or $\deg(r') < \deg(g')$. Then we have $(q-q')g = r'-r$, where $r' - r = 0$ or $\deg(r' - r) < \deg(g)$, and where $(q - q')g = 0$ or since $\mathrm{lc}(g) \in R^*$ we have $\deg((q - q')g) = \deg(g) + \deg(q - q') \geq \deg(g)$. Hence we have $r' = r$ and $(q - q')g = 0$, implying $q = q'$, showing uniqueness.

To show existence, we may assume that $f \neq 0$ and $m := \deg(f) \geq n := \deg(g) > 0$. We proceed by induction on $m \in \mathbb{N}$: Letting $f' := f - \mathrm{lc}(f)\mathrm{lc}(g)^{-1}gX^{m-n} \in R[X]$, the m-th coefficient of f' shows that $f' = 0$ or $\deg(f') < m$. By induction there are $q', r' \in R[X]$ such that $f' = q'g + r'$, where $r' = 0$ or $\deg(r') < \deg(g)$, hence $f = (q'g + r') + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}gX^{m-n} = (q' + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}X^{m-n})g + r'$. ♯

The above proof is constructive, leading to the division algorithm for polynomials. E. g. for $R := \mathbb{Z}$ and $f := 4X^5 + 6X^3 + X + 2 \in \mathbb{Z}[X]$ and $g := X^2 + X + 1 \in \mathbb{Z}[X]$ we get $f = (4X^3 - 4X^2 + 6X - 2)g + (-3X + 4) \in \mathbb{Z}[X]$.

(3.12) Roots. a) Let R be a commutative ring, let S be a ring, and let $\varphi\colon R \to S$ be a homomorphism such that $r^\varphi \cdot s = s \cdot r^\varphi$ for all $r \in R$ and $s \in S$; the latter in particular holds if S is commutative. For $\xi \in S$ let $\varphi_\xi\colon R[X] \to S\colon f = \sum_{i\geq 0} a_i X^i \mapsto \sum_{i\geq 0} a_i^\varphi \xi^i =: f^\varphi(\xi)$ be the associated **evaluation homomorphism**; if S is commutative, then $\xi \in S$ such that $f^\varphi(\xi) = 0$ is called a **root** or **zero** of f in S. In particular, if S is commutative, regarding $S \subseteq S[X]$ as a subring, we have the evaluation homomorphism $\varphi_X\colon R[X] \to S[X]\colon \sum_{i\geq 0} a_i X^i \mapsto \sum_{i\geq 0} a_i^\varphi X^i$, where φ_X is injective or surjective if and only if φ is injective or surjective, respectively.

For $f \in R[X]$ we have the **polynomial map** $\widehat{f}\colon S \to S\colon \xi \mapsto f^\varphi(\xi)$. Then $\widehat{\varphi}\colon R[X] \to \mathrm{Maps}(S, S)\colon f \mapsto \widehat{f}$ is a homomorphism, the latter being a ring with respect to pointwise addition and multiplication. Letting $\nu_\xi\colon \mathrm{Maps}(S, S) \to S\colon \alpha \mapsto \alpha(\xi)$ be the natural evaluation homomorphism, we have $\widehat{\varphi}\nu_\xi = \varphi_\xi\colon f \mapsto \widehat{f}(\xi) = f^\varphi(\xi)$, and $\widehat{\varphi}$ is not necessarily injective, e. g. for $R = S = \mathbb{Z}/2\mathbb{Z}$ and $f = X^2 + X \in (\mathbb{Z}/2\mathbb{Z})[X]$ we have $\widehat{f}(0) = 0 = \widehat{f}(1)$, hence $\widehat{f} = 0 \in \mathrm{Maps}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

b) Let R be an integral domain, let $0 \neq f \in R[X]$ and let $a \in R$. Quotient and remainder yields $f = q_a(X - a) + r_a$, where $q_a \in R[X]$ and $r_a \in R$. Using

$f(a) = q_a(a)(a-a) + r_a = r_a$ we conclude that $a \in R$ is a root of f if and only if $r_a = 0$, which holds if and only if $X - a \mid f$. If $a \neq b \in R$ are roots of f, then $0 = f(b) = q_a(b)(b-a)$ implies that $b \in R$ is a root of $q_a \in R[X]$, and since $\deg(q_a) = \deg(f) - 1$ we by induction conclude that f has at most $\deg(f)$ roots in R. Hence if R is infinite, the map $R[X] \to \mathrm{Maps}(R,R)\colon f \mapsto \widehat{f}$ is injective, thus $R[X]$ and the ring of polynomial maps $R \to R$ are isomorphic.

Let K be a field, and let $G \leq K^*$ be finite. Then we have **Artin's Theorem**: G is cyclic: Given $n \in \mathbb{N}$, any element $g \in G$ such that $|g| \mid n$ is a root of $X^n - 1 \in K[X]$, hence there are at most n of them. Hence G has at most one subgroup of order n, for all $n \in \mathbb{N}$, thus G is cyclic.

4 Factorial and Euclidean rings

(4.1) Divisibility. Let R be an integral domain. Then $a, b \in R$ are called **associate**, if there is $u \in R^*$ such that $b = au \in R$; we write $a \sim b$. We have $a \sim b$ if and only if $aR = bR \trianglelefteq R$, hence $\sim$ is an equivalence relation on R: From $a \sim b$ we have $a \mid b$ and $b \mid a$, being equivalent to $aR = bR$, and conversely if $a, b \in R$ such that $a \mid b$ and $b \mid a$, there are $u, v \in R$ such that $b = au$ and $a = bv$, thus $a = auv$, implying $a(1 - uv) = 0$, hence $a = 0$ or $uv = 1$, where in the first case $a = b = 0$, and in the second case $u, v \in R^*$ and $a \sim b$.

Let $\emptyset \neq S \subseteq R$ be a subset. Then $d \in R$ such that $d \mid a$ for all $a \in S$ is called a **common divisor** of S; any $u \in R^*$ always is a common divisor of S. If for all common divisors $c \in R$ of S we have $c \mid d$, then $d \in R$ is called a **greatest common divisor** of S. Let $\gcd(S) \subseteq R$ be the set of all greatest common divisors of S. In general greatest common divisors do not exist; if $\gcd(S) \neq \emptyset$ then it consists of an associate class: If $d, d' \in \gcd(S)$, then $d \mid d'$ and $d' \mid d$, hence $d \sim d'$. For $a \in R$ we have $a \in \gcd(a) = \gcd(0, a)$; elements $a, b \in R$ such that $\gcd(a, b) = R^*$ are called **coprime**.

An element $0 \neq c \in R \setminus R^*$ is called **irreducible** or **indecomposable**, if $c = ab$ implies $a \in R^*$ or $b \in R^*$ for all $a, b \in R$; otherwise c is called **reducible** or **decomposable**. Hence if $c \in R$ is irreducible then all its associates also are. An element $0 \neq c \in R \setminus R^*$ is irreducible if and only if $cR \lhd R$ is maximal amongst the proper principal ideals of R:

If $c \in R$ is irreducible and $cR \subseteq aR \lhd R$ for some $a \in R$, then we have $c = ab$ for some $b \in R$, and since $a \notin R^*$ we conclude $b \in R^*$, thus $cR = aR$. Conversely, if $cR \lhd R$ fulfils the maximality condition and $c = ab$ for some $a \in R \setminus R^*$ and $b \in R$, then $cR \subseteq aR \lhd R$, hence $cR = aR$, implying $c \sim a$ and $b \in R^*$. ♯

An element $0 \neq c \in R \setminus R^*$ is called a **prime**, if $c \mid ab$ implies $c \mid a$ or $c \mid b$ for all $a, b \in R$. Hence if $c \in R$ is a prime then all its associates also are, and $c \in R$ is a prime if and only if $\{0\} \neq cR \lhd R$ is prime. If $c \in R$ is a prime, then $c \in R$ is irreducible: Let $c = ab$ for some $a, b \in R$, where since $c \mid ab$ we may assume that $c \mid a$, then from $a \mid c$ we get $a \sim c$, hence $b \in R^*$. The converse does not hold, i. e. an irreducible element in general is not a prime:

(4.2) Example. Let $R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \in \mathbb{C}; a, b \in \mathbb{Z}\}$. Then the **norm map** $N\colon R \to \mathbb{Z}\colon a + b\sqrt{-5} \mapsto (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$ is a homomorphism of multiplicative monoids, hence we have $N(R^*) \subseteq \mathbb{Z}^* = \{\pm 1\}$, thus $R^* = \{\pm 1\}$. We have $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) \in R$, where $2, 3, 1 \pm \sqrt{-5} \in R$ are irreducible but not primes: Assume that $2 = ab \in R$, where $a, b \in R \setminus R^*$, hence we have $N(a)N(b) = N(2) = 4$, and since $N(a), N(b) \neq 1$ we conclude $N(a) = N(b) = 2$, a contradiction; since $N(3) = 9$ and $N(1 \pm \sqrt{-5}) = 6$ we for 3 and $1 \pm \sqrt{-5}$ argue similarly. Assume $2 \in R$ is a prime, then we have $2 \mid 1 + \sqrt{-5}$ or $2 \mid 1 - \sqrt{-5}$, thus $4 = N(2) \mid N(1 \pm \sqrt{-5}) = 6$, a contradiction; for 3 and $1 \pm \sqrt{-5}$ we argue similarly.

(4.3) Proposition. Let R be an integral domain. The following are equivalent:
a) Any element $0 \neq a \in R$ is of the form $a = \epsilon \cdot \prod_{i=1}^{n} p_i \in R$, where the $p_i \in R$ are irreducible, $n \in \mathbb{N}_0$ and $\epsilon \in R^*$, and this representation is unique up to reordering and taking associates.
b) Any element $0 \neq a \in R$ is of the form $a = \epsilon \cdot \prod_{i=1}^{n} p_i \in R$, where the $p_i \in R$ are irreducible, $n \in \mathbb{N}_0$ and $\epsilon \in R^*$, and any irreducible element of R is a prime.
c) Any element $0 \neq a \in R$ is of the form $a = \epsilon \cdot \prod_{i=1}^{n} p_i \in R$, where the $p_i \in R$ are primes, $n \in \mathbb{N}_0$ and $\epsilon \in R^*$.

Proof. a)⇒b) Any irreducible element $p \in R$ is a prime: Let $a, b \in R$ such that $p \mid ab$, hence there is $c \in R$ such that $pc = ab$. We may assume that $a, b \notin R^*$, and since p is irreducible we have $c \notin R^*$. Hence let $a = \prod_{i \geq 1} a_i \in R$ and $b = \prod_{j \geq 1} b_j \in R$ as well as $c = \prod_{k \geq 1} c_k \in R$, where the $a_i, b_j, c_k \in R$ are irreducible. This yields $p \cdot \prod_{k \geq 1} c_k = \prod_{i \geq 1} a_i \cdot \prod_{j \geq 1} b_j \in R$, where uniqueness implies $p \sim a_i$ for some i, or $p \sim b_j$ for some j, hence $p \mid a$ or $p \mid b$.

c)⇒a) To show uniqueness let $a = \epsilon \cdot \prod_{i=1}^{n} p_i \in R$, where the p_i are primes. We proceed by induction on $n \in \mathbb{N}_0$, where we have $n = 0$ if and only if $a \in R^*$. Hence let $n \geq 1$, and let $a = \prod_{j=1}^{m} q_j \in R$, where the q_j are irreducible and $m \in \mathbb{N}$. Since $p_n \in R$ is a prime we may assume $p_n \mid q_m$, and since $q_m \in R$ is irreducible we have $p_n \sim q_m$. Thus we have $\epsilon' \cdot \prod_{i=1}^{n-1} p_i = \prod_{j=1}^{m-1} q_j \in R$ for some $\epsilon' \in R^*$, and we are done by induction. ♯

(4.4) Factorial rings. An integral domain fulfilling the conditions of (4.3) is called a **factorial ring** or **Gaussian domain**. In particular, in factorial rings the notions of primality and irreducibility coincide.

Let R be factorial, and let $\mathcal{P} \subseteq R$ be a set of representatives of the associate classes of primes in R; these exist by the Axiom of Choice. Then any $0 \neq a \in R$ has a unique **factorisation** $a = \epsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p}$, where $\epsilon_a \in R^*$, and $a_p \in \mathbb{N}_0$ are the associated **multiplicities**; we have $a_p = 0$ for all almost all $p \in \mathcal{P}$, and if $a_p \leq 1$ for all $p \in \mathcal{P}$ then a is called **squarefree**. Given $0 \neq a = \epsilon_a \cdot \prod_{p \in \mathcal{P}} p^{a_p} \in R$ and $0 \neq b \in \epsilon_b \cdot \prod_{p \in \mathcal{P}} p^{b_p} \in R$, then a and b have greatest common divisors in R, given as $\epsilon \cdot \prod_{p \in \mathcal{P}} p^{\min\{a_p, b_p\}} \in R$ where $\epsilon \in R^*$.

(4.5) Principal ideal domains. An integral domain R such that any ideal of R is principal is called a **principal ideal domain**.

Let R be a principal ideal domain, and let $p \in R$ be irreducible. Since any ideal of R is principal, this implies that the maximal proper principal ideal $pR \lhd R$ is a maximal ideal, and thus a prime ideal, hence $p \in R$ is a prime. Thus for principal ideal domains the notions of primality and irreducibility coincide, and $p \in R$ is a prime if and only if R/pR is a field.

Let $\emptyset \neq S \subseteq R$. Then for $d \in R$ we have $d \in \gcd(S)$ if and only if $dR = \langle S \rangle \trianglelefteq R$; in particular, there are $a_1, \ldots, a_n \in S$ and **Bézout coefficients** $c_1, \ldots, c_n \in R$ such that $d = \sum_{i=1}^n a_i c_i \in R$: Let $dR = \langle S \rangle \trianglelefteq R$. Hence there are $a_1, \ldots, a_n \in S$ and $c_1, \ldots, c_n \in R$ such that $d = \sum_{i=1}^n a_i c_i \in R$. Thus for any $b \in R$ such that $b \mid a$ for all $a \in S$ we have $b \mid d$. Since $aR \subseteq dR$, i. e. $d \mid a$, for all $a \in S$, we have $d \in \gcd(S)$. Let conversely $d \in \gcd(S)$, then letting $c \in R$ such that $\langle S \rangle = cR$, we by the above have $c \in \gcd(S)$, thus $d \sim c$, hence $dR = cR$.

E. g. since the ideals of $\mathbb{Z}$ coincide with its additive subgroups, $\mathbb{Z}$ is a principal ideal domain. Hence for any prime $p \in \mathbb{N}$ there is the **prime field** $\mathrm{GF}(p) = \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ having p elements. For $n \in \mathbb{N}$ we have the **group of prime residues** $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z}; \gcd(x, n) = \{\pm 1\}\}$, where $\gcd(x, n)$ is independent of the chosen representative x.

(4.6) Theorem. Let R be a principal ideal domain. Then R is factorial.

Proof. Let $S := \{a \in R \setminus (R^* \dot\cup \{0\}); a \text{ is not product of irreducible elements}\}$, and assume that $S \neq \emptyset$. Then $\mathcal{X} := \{aR \lhd R; a \in S\} \neq \emptyset$ has a maximal element: Let $\emptyset \neq \mathcal{Y} \subseteq \mathcal{X}$ be totally ordered, and let $I := \bigcup_{J \in \mathcal{Y}} J \subseteq R$. Then we have $\{0\} \neq I \lhd R$, thus there is $b \in S$ such that $I = bR \in \mathcal{Y} \subseteq \mathcal{X}$ is an upper bound for $\mathcal{Y}$. Thus by Zorn's Lemma there is a maximal element $aR \in \mathcal{X}$, for some $a \in S$. Since $a \in R$ is reducible, there are $b, c \in R \setminus R^*$ such that $a = bc$. Since $aR \subset bR, cR \lhd R$, the maximality of $aR \in \mathcal{X}$ implies that both $b, c \in R \setminus S$, hence $a = bc \in R \setminus S$ is a product of irreducible elements, a contradiction. ♯

(4.7) Euclidean rings. An integral domain R is called an **Euclidean ring**, if there is a **degree function** $\delta\colon R \setminus \{0\} \to \mathbb{N}_0$ fulfilling: For all $a, b \in R$ such that $b \neq 0$ there are $q, r \in R$, such that $b = qa + r$ where $r = 0$ or $\delta(r) < \delta(b)$.

E. g. $\mathbb{Z}$ is Euclidean with respect to $\mathbb{Z} \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |z|$, any field K is Euclidean with respect to $K \setminus \{0\} \to \mathbb{N}_0\colon x \mapsto 0$, and $K[X]$ is Euclidean with respect to $K[X] \setminus \{0\} \to \mathbb{N}_0\colon f \mapsto \deg(f)$. All these fulfil $\delta(a) \leq \delta(ab)$ for all $0 \neq a, b \in R$, and $\delta(a) < \delta(ab)$ if additionally $b \notin R^*$.

This additional condition can always be fulfilled: Letting $\delta'\colon R \setminus \{0\} \to \mathbb{N}_0\colon a \mapsto \min\{\delta(ab) \in \mathbb{N}_0; 0 \neq b \in R\}$, we have $\delta'(a) \leq \delta'(ab)$ for all $0 \neq a, b \in R$, and δ' is a degree function: For $a \in R$ and $0 \neq b \in R$, letting $0 \neq c \in R$ such that $\delta'(b) = \delta(cb)$, there are $q, r \in R$ such that $a = qcb + r$ where $r = 0$ or $\delta'(r) \leq \delta(r) < \delta(cb) = \delta'(b)$.

(4.8) Theorem. Let R be Euclidean. Then R is a principal ideal domain.

Proof. Let $\{0\} \neq I \trianglelefteq R$, then using the degree function δ we have $\delta(I) := \{\delta(a) \in \mathbb{N}_0; 0 \neq a \in I\} \neq \emptyset$, thus there is $0 \neq b \in I$ such that $\delta(b) \in \delta(I)$ is minimal. For $a \in I$ let $q, r \in R$ such that $a = qb + r$ where $r = 0$ or $\delta(r) < \delta(b)$. Assume that $r \neq 0$, then $r = a - qb \in I$ contradicts the minimality of b. Hence we have $r = 0$, implying $b \mid a$ and $I = bR$. ♯

(4.9) Extended Euclidean algorithm. Let R be Euclidean with respect to the degree function $\delta\colon R\backslash\{0\} \to \mathbb{N}_0$, and let $a, b \in R$ such that $a \neq 0$. A greatest common divisor $r \in R$ and Bézout coefficients $s, t \in R$ such that $r = as + bt \in R$ are computed as follows; leaving out the computation of the $s_i, t_i \in R$ just yields a greatest common divisor:

- $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$
- $s_0 \leftarrow 1$, $t_0 \leftarrow 0$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$
- while $r_i \neq 0$ do
  - $[q_i, r_{i+1}] \leftarrow \mathsf{QuotRem}(r_{i-1}, r_i)$ # quotient and remainder
  # $q_i, r_{i+1} \in R$ such that $r_{i+1} = r_{i-1} - q_i r_i$ where $r_{i+1} = 0$ or $\delta(r_{i+1}) < \delta(r_i)$
  - $s_{i+1} \leftarrow s_{i-1} - q_i s_i$, $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
  - $i \leftarrow i + 1$
- $r \leftarrow r_{i-1}$
- $s \leftarrow s_{i-1}$, $t \leftarrow t_{i-1}$
- return $[r, s, t]$

Since $\delta(r_i) > \delta(r_{i+1}) \geq 0$ for $i \in \mathbb{N}$, there is $l \in \mathbb{N}$ such that $r_l \neq 0$ and $r_{l+1} = 0$, hence the algorithm terminates. We have $r_i = as_i + bt_i$ for all $i \in \{0, \ldots, l+1\}$, hence it remains to show that $r_l \in \gcd(a, b) = \gcd(r_0, r_1)$: Let $c \in \gcd(r_0, r_1)$. Then for all $i \in \{1, \ldots, l\}$ we by induction have $c \mid r_{i-1}, r_i$ and thus $c \mid r_{i-1} - q_i r_i = r_{i+1}$, hence in particular $c \mid r_l$. Conversely, since $r_{l+1} = 0$, for all $i \in \{l, l-1, \ldots, 1\}$ we by induction have $r_l \mid r_{i+1}, r_i$ and thus $r_l \mid q_i r_i + r_{i+1} = r_{i-1}$, hence in particular $r_l \mid r_0, r_1$, thus $r_l \mid c$. ♯

(4.10) Example. a) For $R := \mathbb{Z}$ and $a := 126$ and $b := 35$ the following shows that $d := 7 \in \gcd(a, b)$ and that $d = 2a - 7b$:

i	q_i	r_i	s_i	t_i
0		126	1	0
1	3	35	0	1
2	1	21	1	−3
3	1	14	−1	4
4	2	7	2	−7
5		0	−5	18

b) For $R := \mathbb{Q}[X]$ and $f := 3X^3 - 7X^2 + 5X - 1$ and $g := -6X^2 + 5X - 1$ the

following shows that $h := 3X - 1 \in \gcd(f, g)$ and that $h = 4f + (2X - 3)g$:

i	q_i	r_i	s_i	t_i
0		$3X^3 - 7X^2 + 5X - 1$	1	0
1	$-\frac{1}{2}X + \frac{3}{4}$	$-6X^2 + 5X - 1$	0	1
2	$-8X + 4$	$\frac{3}{4}X - \frac{1}{4}$	1	$\frac{1}{2}X - \frac{3}{4}$
3		0	$8X - 4$	$4X^2 - 8X + 4$

(4.11) Example. For $n \in \{-2, -1, 2, 3\}$ the ring $R := \mathbb{Z}[\sqrt{n}]$ is Euclidean with respect to the degree function $R \setminus \{0\} \to \mathbb{N}_0 \colon z \mapsto |N(z)|$, where $N \colon \mathcal{Q}(R) = \mathbb{Q}(\sqrt{n}) \to \mathbb{Q} \colon a + b\sqrt{n} \mapsto (a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - nb^2$ is the norm map; in particular we have $N(z) = 0$ if and only if $z = 0$, and $R^* = \{z \in R; |N(z)| = 1\}$.

Let $u := a + b\sqrt{n} \in R$ and $0 \neq v := c + d\sqrt{n} \in R$, where $a, b, c, d \in \mathbb{Z}$. Let $uv^{-1} = s + t\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ for some $s, t \in \mathbb{Q}$, let $x, y \in \mathbb{Z}$ such that $|s - x| \leq \frac{1}{2}$ and $|t - y| \leq \frac{1}{2}$, and let $q := x + y\sqrt{n} \in R$ and $r := u - qv \in R$. Hence we have $r = v(uv^{-1} - q) = v((s - x) + (t - y)\sqrt{n})$, and since $|(s - x)^2 - n(t - y)^2| \leq \frac{1}{4} + 2 \cdot \frac{1}{4} < 1$ for $|n| \leq 2$, and $-\frac{3}{4} \leq (s - x)^2 - 3(t - y)^2 \leq \frac{1}{4}$ for $n = 3$, we from N being a homomorphism of multiplicative monoids obtain $|N(r)| = |N(v)| \cdot |(s - x)^2 - n(t - y)^2| < |N(v)|$. ♯

(4.12) Theorem. Let $p \in \mathbb{N}$ be a prime such that $p \equiv 1 \pmod 4$. Then there are $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$.

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we have $\varphi(p) = |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$, and thus by Lagrange's Theorem we for all $0 \neq x \in \mathbb{Z}/p\mathbb{Z}$ have $x^{p-1} = 1 \in \mathbb{Z}/p\mathbb{Z}$, implying the **Euler-Fermat Theorem** $x^p = x \in \mathbb{Z}/p\mathbb{Z}$ for all $x \in \mathbb{Z}/p\mathbb{Z}$.

Let $R := \mathbb{Z}[\sqrt{-1}]$ and let $\overline{\ }\colon R \to R/pR$ be the natural homomorphism. Hence for $z = x + y\sqrt{-1} \in R$, where $x, y \in \mathbb{Z}$, we have $\overline{z}^p = \overline{(x + y\sqrt{-1})^p} = \overline{\sum_{k=0}^{p} \binom{p}{k} x^k (y\sqrt{-1})^{p-k}} \in R/pR$. Since $\binom{p}{k} \in p\mathbb{Z} \subseteq pR \trianglelefteq R$ for $k \in \{1, \ldots, p-1\}$, we have $\overline{z}^p = \overline{x}^p + \overline{y}^p \overline{\sqrt{-1}^p} \in R/pR$. Since from $p \equiv 1 \pmod 4$ we get $\sqrt{-1}^p = \sqrt{-1}$, and from $x^p \equiv x \pmod p$ we get $\overline{x}^p = \overline{x} \in R/pR$ and similarly $\overline{y}^p = \overline{y} \in R/pR$, we conclude $\overline{z^p} = \overline{x} + \overline{y}\overline{\sqrt{-1}} = \overline{z} \in R/pR$.

From $pR = \{x + y\sqrt{-1} \in R, x, y \in p\mathbb{Z}\}$ we get $|R/pR| = p^2$, hence $p \notin R^*$. Assume that $p \in R$ is irreducible, then R/pR is a field, hence $|(R/pR)^*| = p^2 - 1$, a contradiction. Thus $p \in R$ is reducible, hence there is an irreducible element $z = a + b\sqrt{-1} \mid p \in R$, where $a, b \in \mathbb{Z}$. Thus $1 \neq N(z) = a^2 + b^2 \in \mathbb{Z}$ is a proper divisor of $N(p) = p^2 \in \mathbb{Z}$, hence $a^2 + b^2 = p$. ♯

(4.13) Primitivity. a) Let R be factorial, and let $0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$. Then $c(f) \in \gcd(a_0, \ldots, a_n) \subseteq R \setminus \{0\}$ is called a **content** of f, and if $c(f) \in R^*$ then f is called **primitive**. In particular, if f is monic then it is primitive, thus if R is a field then all non-zero polynomials are primitive.

For all $a \in R$ we have $c(af) \sim ac(f) \in R$. Thus letting $a_i = a_i' c(f) \in R$ for suitable $a_i' \in R$ we have $\gcd(a_0', \ldots, a_n') = R^*$, and letting $f' := \sum_{i=0}^n a_i' X^i \in R[X]$ we have $f = c(f)f' \in R[X]$ where $f' \in R[X]$ is primitive. If $af' = bf'' \in R[X]$, where $0 \neq a, b \in R$ and $f', f'' \in R[X]$ are primitive, then $a \sim ac(f') \sim bc(f'') \sim b \in R$, and thus $f' \sim f'' \in R[X]$. Hence the **primitive part** $f' \in R[X]$ is uniquely determined up to taking associates; we have $\deg(f) = \deg(f')$ and if $f \in R[X]$ is not primitive then $f \in R[X]$ is reducible.

b) Let $K := \mathcal{Q}(R)$, and let $0 \neq f = \sum_{i=0}^n \frac{r_i}{s_i} \cdot X^i \in K[X]$, where $r_i, s_i \in R$ are coprime and $s_i \neq 0$, for all $i \in \{0, \ldots, n\}$. Letting $d(f) := \prod_{i=0}^n s_i \in R$ we have $\widetilde{f} := d(f)f = \sum_{i=0}^n (\prod_{j \neq i} s_j) \cdot r_i X^i \in R[X] \subseteq K[X]$. Let $c(f) := c(\widetilde{f}) \in R$ be a content of $\widetilde{f} \in R[X]$ and $f' \in R[X]$ be primitive such that $\widetilde{f} = c(f)f' \in R[X]$, then we have $f = \frac{c(f)}{d(f)} \cdot f' \in K[X]$. If $f = \frac{c}{d} \cdot f' = \frac{a}{b} \cdot f'' \in K[X]$, where $a, b, c, d \in R$ such that $b, d \neq 0$ and $f', f'' \in R[X]$ are primitive, then $cbf' = adf'' \in R[X]$, hence $cb \sim ad \in R$ and $f' \sim f'' \in R[X]$. Hence the **primitivisation** $f' \in R[X]$ is uniquely determined up to taking associates; we have $\deg(f) = \deg(f')$.

(4.14) Lemma: Gauß. Let R be factorial, and let $f, g \in R[X]$ be primitive. Then $fg \in R[X]$ is primitive as well.

Proof. Let $p \in R$ be a prime, hence $pR \lhd R$ is prime. Then $\{0\} \neq pR[X] = \{\sum_{i \geq 0} a_i X^i \in R[X]; p \mid a_i \text{ for all } i \geq 0\} \lhd R[X]$ is prime as well; the following proof is valid for arbitrary integral domains: Let $h = \sum_{i \geq 0} a_i X^i \in R[X] \setminus pR[X]$ and $\widetilde{h} = \sum_{i \geq 0} b_i X^i \in R[X] \setminus pR[X]$, and let $k, l \in \mathbb{N}_0$ be minimal such that $a_k \notin pR$ and $b_l \notin pR$. Hence the $(k+l)$-th coefficient of $h\widetilde{h} \in R[X]$ is given as $(\sum_{i=0}^{k-1} a_i b_{k+l-i}) + a_k b_l + (\sum_{i=0}^{l-1} a_{k+l-i} b_i) \in R$, where the bracketed terms are elements of pR, while $a_k b_l \notin pR$, thus $h\widetilde{h} \notin pR[X]$ as well.

Assume that $c(fg) \notin R^*$. Since R is factorial there is a prime $p \in R$ such that $p \mid c(fg)$, thus all coefficients of fg are elements of pR, hence $fg \in pR[X]$. Thus we may assume that $f \in pR[X]$, implying that $p \mid c(f) \in R$, a contradiction. ♯

(4.15) Theorem. Let R be factorial, let $K := \mathcal{Q}(R)$ and $f \in R[X] \setminus R$. Then f is irreducible in $R[X]$ if and only if f is primitive and irreducible in $K[X]$.

Proof. Let f be reducible in $R[X]$. We may assume that f is primitive, hence there are $g, h \in R[X] \setminus R$ such that $f = gh$. Thus $g, h \in K[X] \setminus K^*$, and hence f is reducible in $K[X]$.

Let conversely f be irreducible in $R[X]$, hence f is primitive, and assume that there are $g, h \in K[X] \setminus K^*$ such that $f = gh \in K[X]$. Hence there are $c(g), d(g), c(h), d(h) \in K$ such that $d(g), d(h) \neq 0$ and $g', h' \in R[X] \setminus R$ primitive such that $g = \frac{c(g)}{d(g)} \cdot g' \in K[X]$ and $h = \frac{c(h)}{d(h)} \cdot h' \in K[X]$. Thus we have $d(g)d(h)f = c(g)c(h)g'h' \in R[X]$, and since by Gauß's Lemma $g'h' \in R[X]$ is primitive we infer $d(g)d(h)c(f) \sim c(g)c(h) \in R$. Thus we have $d(g)d(h) \mid$

$c(g)c(h) \in R$, hence letting $c := \frac{c(g)c(h)}{d(g)d(h)} \in R$ we have $f = cg'h' \in R[X]$, implying that f is reducible in $R[X]$, a contradiction. ♯

(4.16) Theorem: Gauß. Let R be an integral domain. Then $R[X]$ is factorial if and only if R is.

Proof. We only have to show that $R[X]$ is factorial whenever R is. Hence let R be factorial, then any $0 \neq f \in R[X]$ is a product of irreducible elements: Let $K := \mathcal{Q}(R)$, and let $f = c \cdot \prod_{i=1}^{n} p_i \in K[X]$ be a factorisation in the factorial ring $K[X]$, where $c \in K^*$ and $n \in \mathbb{N}_0$. Hence we have $f = c' \cdot \prod_{i=1}^{n} p_i' \in R[X]$, where $c' \in R$ and the $p_i' \in R[X] \setminus R$ are primitive. Since $p_i' \sim p_i \in K[X]$ is irreducible in $K[X]$, we conclude that p_i' is irreducible in $R[X]$, and since R is factorial c' is a product of irreducible elements of R.

For uniqueness let $0 \neq f = c \cdot \prod_{i=1}^{n} p_i = d \cdot \prod_{j=1}^{m} q_j \in R[X]$, where $c, d \in R$ and the $p_i, q_j \in R[X] \setminus R$ are irreducible in $R[X]$, hence primitive. Thus $c, d \in K^*$ and the $p_i, q_j \in K[X]$ are irreducible in $K[X]$. Since $K[X]$ is factorial we have $n = m$, and we may assume $p_i \sim q_i \in K[X]$ for all $i \in \{1, \ldots, n\}$. Thus using the primitivisations $p_i', q_i' \in R[X]$ we infer $p_i \sim p_i' \sim q_i' \sim q_i \in R[X]$. Hence $c \sim d \in R$ as well, uniqueness following from R being factorial. ♯

(4.17) Theorem: Eisenstein. Let R be factorial, and let $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ be primitive such that $\deg(f) = n \in \mathbb{N}$. If there is a prime $p \in R$ such that $p \not| \, a_n$, and $p \mid a_i$ for all $i \in \{0, \ldots, n-1\}$, and $p^2 \not| \, a_0$, then f is irreducible.

Proof. Let $f = gh$ where $g = \sum_{i=0}^{k} b_i X^i \in R[X]$ and $h = \sum_{i=0}^{l} c_i X^i \in R[X]$ such that $\deg(g) = k$ and $\deg(h) = l$, hence $k + l = n$. Thus we have $p \mid a_0 = b_0 c_0$, hence we may assume that $p \mid b_0$ and thus $p \not| \, c_0$. We have $a_n = b_k c_l$ and thus $p \not| \, b_k$. Hence let $m \in \{1, \ldots, k\}$ be minimal such that $p \not| \, b_m$. Thus for $a_m = b_m c_0 + \sum_{i=1}^{m} b_{m-i} c_i$ we have $p \not| \, b_m c_0$, while $p \mid b_{m-i} c_i$ for $i \in \{1, \ldots, m\}$, hence $p \not| \, a_m$, implying $n = m \leq k = \deg(g) \leq n = \deg(f)$. Thus we have $\deg(h) = l = 0$, and since f is primitive we conclude $h \in R^* = R[X]^*$. ♯

(4.18) Irreducibility. Let R and S be integral domains, let $\varphi\colon R \to S$ be a homomorphism, and let $\varphi_X\colon R[X] \to S[X]\colon f \mapsto f^\varphi$ be the associated evaluation homomorphism. Let $f \in R[X] \setminus R$ be primitive such that $f^\varphi \in S[X]$ is irreducible and $\deg(f^\varphi) = \deg(f)$; in particular the degree condition holds if $\mathrm{lc}(f) \in R^*$. Then $f \in R[X]$ is irreducible: Assume that there are $g, h \in R[X]$ such that $f = gh \in R[X]$. Then we have $f^\varphi = g^\varphi h^\varphi \in S[X]$. Since $\deg(f) = \deg(f^\varphi) = \deg(g^\varphi) + \deg(h^\varphi) \leq \deg(g) + \deg(h) = \deg(f)$ we conclude that $\deg(g^\varphi) = \deg(g) \geq 1$ and $\deg(h^\varphi) = \deg(h) \geq 1$, a contradiction.

No assertion is made if $f^\varphi \in S[X]$ is reducible. Since $R \subseteq \mathcal{Q}(R)$ is a subring, the 'if' part of (4.15) is a particular case of the above observation. Another special case is given as follows: Let $a \in R^*$ and $b \in R^*$. Then the evaluation homomorphism $\varphi_{aY+b}\colon R[X] \to R[Y]\colon X \mapsto aY + b$ is an isomorphism with

inverse $\varphi_{a^{-1}(X-b)}\colon R[Y] \to R[X]\colon Y \mapsto a^{-1}(X-b)$, hence $f(X) \in R[X]$ is irreducible if and only if $f(aY+b) \in R[Y]$ is irreducible; $\varphi_g\colon R[X] \to R[Y]$ is injective for any $g \in R[Y]$, if φ_g is surjective then g is linear with $\mathrm{lc}(g) \in R^*$.

(4.19) Example. a) Let $k \in \mathbb{N}$, let $n \in \mathbb{Z} \setminus \{-1,0,1\}$ be squarefree, and let $f := X^k - n \in \mathbb{Z}[X]$. The Eisenstein Criterion for any prime $p \mid n$ implies the irreducibility of f in $\mathbb{Z}[X]$, hence in $\mathbb{Q}[X]$; in particular for $k, n \geq 2$ we have $\sqrt[k]{n} \in \mathbb{R} \setminus \mathbb{Q}$. For $k \geq 2$ and $p \mid n$, using the natural homomorphism $\overline{\ } = \nu_p\colon \mathbb{Z} \to \mathbb{F}_p$, the **reduced** polynomial $\overline{f} = X^k \in \mathbb{F}_p[X]$ is reducible.

Let $g := X^4 - 1 \in \mathbb{Z}[X]$. Since $\pm 1 \in \mathbb{Z}$ are roots of g, we have the factorisation $g = (X-1)(X+1)(X^2+1) \in \mathbb{Z}[X]$, where $h := X^2+1 \in \mathbb{Z}[X]$ is irreducible: Reducing modulo $p = 3$ the polynomial $\overline{h} = X^2 + 1 \in \mathbb{F}_3[X]$ has no root in $\mathbb{F}_3$, thus is irreducible in $\mathbb{F}_3[X]$.

b) Let $p \in \mathbb{N}$ be a prime, and let $\Phi_p := \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$ be the **p-th cyclotomic polynomial**. Hence we have $X^p - 1 = (X-1)\Phi_p \in \mathbb{Z}[X]$, where $\Phi_p \in \mathbb{Z}[X]$ is irreducible: Using the isomorphism $\varphi_{X+1}\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ we get $X \cdot \Phi_p(X+1) = (X+1)^p - 1 = -1 + \sum_{i=0}^{p} \binom{p}{i} X^i = X \cdot \sum_{i=0}^{p-1} \binom{p}{i+1} X^i$, implying $\Phi_p(X+1) = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i \in \mathbb{Z}[X]$. Since $\binom{p}{p} = 1$, and $p \mid \binom{p}{i+1}$ for all $i \in \{0, \ldots, p-2\}$, and $\binom{p}{1} = p$, the Eisenstein Criterion for the prime p implies the irreducibility of $\Phi_p(X+1) \in \mathbb{Z}[X]$.

5 Field extensions

(5.1) Field extensions. Let $K \subseteq L$ be a field extension; we also write L/K. Let $S \subseteq L$ be a subset, then $K \subseteq K(S) := \bigcap\{M \subseteq L \text{ field extension}; K \cup S \subseteq M\} \subseteq L$ is the smallest subfield of L containing $K \cup S$, being called the subfield obtained by **adjoining** S to K; if $S = \{s_1, \ldots, s_n\}$ is finite, we also write $K(S) = K(s_1, \ldots, s_n)$. The field extension L/K is called **simple**, if there is $a \in L$ such that $L = K(a)$, then $a \in L$ is called a **primitive element**.

The field L being a K-vector space, the K-dimension $[L\colon K] = \deg(L/K) := \dim_K(L) \in \mathbb{N} \dot\cup \{\infty\}$ is called the **degree** of L/K. If $[L\colon K] \in \mathbb{N}$ then L/K is called **finite**, otherwise **infinite**.

E. g. we have $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, and since $\{1, \sqrt{-1}\} \subseteq \mathbb{C}$ is an $\mathbb{R}$-basis we have $[\mathbb{C}\colon \mathbb{R}] = 2$, while $\mathbb{R}/\mathbb{Q}$ is infinite. We have the field extension $K \subseteq K(X) = \mathcal{Q}(K[X])$, and since $K[X] \leq K(X)$ as K-vector spaces, where $\{X^i; i \in \mathbb{N}_0\} \subseteq K[X]$ is K-linearly independent, we conclude that $K(X)/K$ is infinite.

(5.2) Proposition. Let L/K be a field extension and let V be an L-vector space. Then we have $\dim_K(V) = [L\colon K] \cdot \dim_L(V)$; in particular if $\dim_K(V)$ is finite then $\dim_L(V) \mid \dim_K(V)$ and $[L\colon K] \mid \dim_K(V)$.

In particular, if $K \subseteq L \subseteq M$ is a field extension then $[M\colon K] = [M\colon L] \cdot [L\colon K]$, and if M/K is finite then $[M\colon L] \mid [M\colon K]$ and $[L\colon K] \mid [M\colon K]$.

Proof. We may assume that $V \neq \{0\}$. If either of $\dim_L(V)$ or $[L\colon K]$ is infinite, then $\dim_K(V)$ is infinite as well. Thus we may assume that both $m := \dim_L(V) \in \mathbb{N}$ and $n := [L\colon K] \in \mathbb{N}$. Let $\mathcal{A} := \{a_1, \ldots, a_n\} \subseteq L$ be a K-basis, and let $\mathcal{B} := \{b_1, \ldots, b_m\} \subseteq V$ be an L-basis. Then $\mathcal{C} := \{b_j a_i \in V; i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\} \subseteq V$ is a K-basis:

Any $v \in V$ can be written as $v = \sum_{j=1}^m b_j c_j$ where $c_j \in L$. For all $j \in \{1, \ldots, m\}$ we have $c_j = \sum_{i=1}^n a_i a_{ji}$ where $a_{ji} \in K$. Hence we have $v = \sum_{j=1}^m \sum_{i=1}^n b_j a_i a_{ji}$, thus $\mathcal{C} \subseteq V$ is a K-generating set. If $a_{ji} \in K$ such that $\sum_{j=1}^m \sum_{i=1}^n b_j a_i a_{ji} = 0$, then by the L-linear independence of $\mathcal{B}$ we have $\sum_{i=1}^n a_i a_{ji} = 0$ for all $j \in \{1, \ldots, m\}$, and thus by the K-linear independence of $\mathcal{A}$ we have $a_{ji} = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, m\}$, hence $\mathcal{C}$ is K-linearly independent. ♯

(5.3) Prime fields. Let K be a field. Then the **prime field** $P(K) := \bigcap\{M \subseteq K \text{ field extension}\} \subseteq K$ is the unique smallest subfield of K.

Let $\varphi_K\colon \mathbb{Z} \to K\colon n \mapsto n \cdot 1$ be the natural homomorphism. Since $\mathbb{Z}/\ker(\varphi_K) \cong \operatorname{im}(\varphi_K) \subseteq K$ is an integral domain, $p\mathbb{Z} := \ker(\varphi_K) \lhd \mathbb{Z}$ is prime, hence $p = 0$ or $p \in \mathbb{Z}$ is a prime. Then $\operatorname{char}(K) := p \geq 0$ is called the **characteristic** of K; e. g. we have $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$ and $\operatorname{char}(\mathbb{F}_p) = p$; thus any prime $p \in \mathbb{N}$ occurs as a characteristic of some field. Any finite field has prime characteristic, thus fields of characteristic 0 are infinite.

Let L/K be a field extension. Since $\operatorname{im}(\varphi_K) \subseteq P(K)$ as rings, we have $\operatorname{im}(\varphi_K) = \operatorname{im}(\varphi_L) \subseteq P(K) = P(L)$, hence $\operatorname{char}(K) = \operatorname{char}(L)$; e. g. we have $P(K) = P(K(X))$ and $\operatorname{char}(K) = \operatorname{char}(K(X))$, thus $\mathbb{F}_p(X)$ is an infinite field of characteristic p. If $\operatorname{char}(K) = p > 0$ then we have $\operatorname{im}(\varphi_K) \cong \mathbb{Z}/\ker(\varphi_K) = \mathbb{F}_p$, implying $P(K) \cong \mathbb{F}_p$. If $\operatorname{char}(K) = 0$ then we have $\varphi_K(\mathbb{Z} \setminus \{0\}) \subseteq P(K)^*$, hence there is a ring isomorphism $\mathbb{Q} = \mathcal{Q}(\mathbb{Z}) \cong \{\frac{\varphi_K(m)}{\varphi_K(n)} \in P(K); m, n \in \mathbb{Z}, n \neq 0\} \subseteq P(K)$, implying $P(K) \cong \mathbb{Q}$; e. g. we have $P(\mathbb{R}) = P(\mathbb{C}) = \mathbb{Q}$.

Let K be finite, thus $\operatorname{char}(K) = p > 0$ and $P(K) \cong \mathbb{F}_p$, then $K/\mathbb{F}_p$ is finite, hence $|K| = p^{[K\colon \mathbb{F}_p]}$; conversely, if $|K| = p^n$ for a prime $p \in \mathbb{N}$ and some $n \in \mathbb{N}$ then $\operatorname{char}(K) = p$. If L/K is finite, then $|L|$ is finite as well, hence L^* is cyclic, thus there is $a \in L^*$ such that $L = \{0, 1, a, \ldots, a^{|L|-2}\}$, implying that $L = K(a)$, thus L/K is simple.

(5.4) Algebraic extensions. Let L/K be a field extension. For $a \in L$ let $\varphi_a = \varphi_{L/K,a}\colon K[X] \to L\colon f \mapsto f(a)$ be the associated evaluation homomorphism. Hence $K[a] := \operatorname{im}(\varphi_a) = \{f(a) \in L; f \in K[X]\} \subseteq L$ is an integral domain, and $\ker(\varphi_a) := \{f \in K[X]; f(a) = 0\} \lhd K[X]$ is called the **order ideal** of a over K.

If $\ker(\varphi_a) = \{0\}$ then a is called **transcendental** over K; e. g. $X \in K(X)$ is transcendental over K. If $\ker(\varphi_a) \neq \{0\}$ then a is called **algebraic** over K, and there is a unique monic irreducible polynomial $\mu_a = \mu_{K,a} \in K[X]$ such that $\ker(\varphi_a) = \mu_a K[X] \lhd K[X]$, being called the **minimum polynomial** of a over K, and $\deg_K(a) := \deg(\mu_a) \in \mathbb{N}$ is called the **degree** of a over K. If a is

algebraic over K then a is algebraic over any intermediate field $K \subseteq M \subseteq L$, and L/K is called **algebraic** if any element of L is algebraic over K.

E. g. any $a \in K$ is algebraic over K, and since $\mu_a = X - a \in K[X]$ we have $\deg_K(a) = 1$; we have $K(a) = K$, thus $[K(a)\colon K] = 1$. For $n \in \mathbb{Z} \setminus \{0,1\}$ squarefree the polynomial $X^2 - n \in \mathbb{Q}[X]$ is irreducible, hence $\mu_{\sqrt{n}} = X^2 - n \in \mathbb{Q}[X]$ shows that $\deg_{\mathbb{Q}}(\sqrt{n}) = 2$; since $\{1, \sqrt{n}\}$ is a $\mathbb{Q}$-basis of the **quadratic number field** $\mathbb{Q}(\sqrt{n})$ we have $[\mathbb{Q}(\sqrt{n})\colon \mathbb{Q}] = 2$; a field $K \subseteq \mathbb{C}$ such that $K/\mathbb{Q}$ is finite is called a **number field**.

(5.5) Theorem. Let L/K be a field extension.
a) If $a \in L$ is transcendental over K, then we have $K(X) \cong K(a) \subseteq L$; in particular $K(a)/K$ is infinite. If $a \in L$ is algebraic over K, then we have $K[X]/\mu_a K[X] \cong K[a] = K(a) \subseteq L$, and letting $n := \deg_K(a) \in \mathbb{N}$ the set $\{1, a, \ldots, a^{n-1}\} \subseteq K(a)$ is a K-basis.
b) L/K is finite if and only if there are $a_1, \ldots, a_n \in L$ algebraic over K such that $L = K(a_1, \ldots, a_n)$; in particular, if L/K is finite then it is algebraic. If $K \subseteq M \subseteq L$ is an intermediate field, then L/K is algebraic if and only if both M/K and L/M are algebraic.

Proof. a) If $a \in L$ is transcendental over K, then we have the isomorphism $\varphi_a\colon K[X] \to K[a]\colon f \mapsto f(a)$. Since $\mathcal{Q}(K[a]) \subseteq L$ is the smallest subfield of L containing $K \cup \{a\}$, we have $\mathcal{Q}(K[a]) = K(a) \subseteq L$, and thus φ_a extends to an isomorphism $K(X) = \mathcal{Q}(K[X]) \to \mathcal{Q}(K[a]) = K(a)\colon \frac{f}{g} \mapsto f(a)g(a)^{-1}$. If $a \in L$ is algebraic over K, then since $\mu_a K[X] \lhd K[X]$ is maximal the isomorphism $K[X]/\mu_a K[X] \cong K[a]$ shows that $K[a] \subseteq L$ is a subfield, implying $K[a] = K(a)$. This isomorphism also provides a K-basis of $K[a]$:

For any $f \in K[X] \setminus K$, let $\overline{\ }\colon K[X] \to K[X]/fK[X] =: V$ denote the natural homomorphism. Since $K \cap fK[X] = \{0\}$ we have $K \subseteq V$, hence V is a K-vector space. Letting $n := \deg(f) \in \mathbb{N}$ the set $\{\overline{X}^0, \ldots, \overline{X}^{n-1}\} \subseteq V$ is a K-basis: Let $\sum_{i=0}^{n-1} a_i \overline{X}^i = 0 \in V$ where $a_i \in K$. Hence for $g := \sum_{i=0}^{n-1} a_i X^i \in K[X]$ we have $f \mid g$, implying $g = 0$, hence $a_i = 0$ for $i \in \{0, \ldots, n-1\}$, thus $\{\overline{X}^0, \ldots, \overline{X}^{n-1}\}$ is K-linearly independent. Let $g \in K[X]$, then there are $q, r \in K[X]$, where $r = 0$ or $\deg(r) < \deg(f) = n$, such that $g = qf + r \in K[X]$, hence $\overline{g} = \overline{qf + r} = \overline{r} \in V$, thus $\overline{g}$ is a K-linear combination of $\{\overline{X}^0, \ldots, \overline{X}^{n-1}\}$.

b) If L/K is finite, then for any $a \in L$ the degree $[K(a)\colon K] \leq [L\colon K]$ is finite, thus L/K is algebraic, and letting $\{a_1, \ldots, a_n\} \subseteq L$ be a K-basis we have $L = K(a_1, \ldots, a_n)$. Conversely, let $a_1, \ldots, a_n \in L$ be algebraic over K such that $L = K(a_1, \ldots, a_n)$, then for $i \in \{1, \ldots, n\}$ the element $a_i \in L$ is algebraic over $K(a_1, \ldots, a_{i-1})$, hence $K(a_1, \ldots, a_i)/K(a_1, \ldots, a_{i-1})$ is finite, and thus $[L\colon K] = \prod_{i=1}^{n} [K(a_1, \ldots, a_i)\colon K(a_1, \ldots, a_{i-1})]$ is finite as well.

Let M/K and L/M be algebraic, and for $a \in L$ let $\mu_a = \mu_{M,a} = \sum_{i=0}^{n} a_i X^i \in M[X]$ be the minimum polynomial of $a \in L$ over M. Since $a_i \in M$ is algebraic over K, the field extension $K \subseteq K(a_0, \ldots, a_n) =: M'$ is finite. From $\mu_a \in M'[X]$

we infer that $a \in L$ is algebraic over M', thus $M'(a)/M'$ is finite. Hence $M'(a)/K$ is finite, thus algebraic, hence $a \in L$ is algebraic over K. ♯

(5.6) Splitting fields. Let K be a field and let $f \in K[X] \setminus K$. A field extension L/K such that $f = \mathrm{lc}(f) \cdot \prod_{i=1}^{n}(X - a_i) \in L[X]$ **splits** and $K(a_1, \ldots, a_n) = L$ is called a **splitting field** for f over K. If M/K is a field extension such that $f = \mathrm{lc}(f) \cdot \prod_{i=1}^{n}(X - a_i) \in M[X]$ splits, then $L := K(a_1, \ldots, a_n) \subseteq M$ is the unique splitting field for f in M, and for any intermediate field $K \subseteq M' \subseteq M$ the field $M'(L)$ is a splitting field for f over M'.

Hence the $a_i \in L$ for $i \in \{1, \ldots, n\}$, where $n = \deg(f) \in \mathbb{N}$, are the roots of f in L, thus algebraic over K, and L/K is finite, minimal inasmuch that f does not split over any intermediate field $K \subseteq M \subset L$. We may assume that $\{a_1, \ldots, a_r\} \subseteq L$, for some $r \leq n$, are the pairwise distinct roots of f. Then we have the factorisation $f = \mathrm{lc}(f) \cdot \prod_{j=1}^{r}(X - a_j)^{m_j} \in L[X]$, where the $m_j \in \mathbb{N}$ are the associated multiplicities. If $m_j = 1$ then $a_j \in L$ is called a **simple** root, otherwise $a_j \in L$ is called a **multiple** root; since $n = \sum_{j=1}^{r} m_j$ the polynomial f has precisely n roots in L counting multiplicities.

(5.7) Theorem: Kronecker. Let K be a field and $f \in K[X]$ be irreducible.
a) There is a field extension L/K of degree $[L\colon K] = \deg(f)$ such that f has a root in L.
b) Let K' be a field, let $\varphi\colon K \to K'$ be an isomorphism, let L/K and L'/K' be field extensions, let $a \in L$ be a root of f, and let $a' \in L'$ be a root of $f^\varphi \in K'[X]$. There is a unique isomorphism $\widehat{\varphi}\colon K(a) \to K'(a')$ such that $\widehat{\varphi}|_K = \varphi$ and $a^{\widehat{\varphi}} = a'$.

Proof. a) Since $f \in K[X]$ is irreducible, $L := K[X]/fK[X]$ is an extension field of K such that $[L\colon K] = \deg(f)$. Letting $\overline{\ }\colon K[X] \to L$ be the natural homomorphism, for $\overline{X} \in L$ we have $f(\overline{X}) = \overline{f(X)} = 0 \in L$.
b) We have $\mu_a \sim f \in K[X]$, hence $\varphi_a\colon K[X] \to L$ induces an isomorphism $\overline{\varphi}_a\colon K[X]/fK[X] \cong K[a] = K(a) \subseteq L$. Since $\varphi\colon K[X] \to K'[X]$ is an isomorphism, $f^\varphi \in K'[X]$ is irreducible, and hence we have $\overline{\varphi}_{a'}\colon K'[X]/f^\varphi K'[X] \cong K'[a'] = K'(a') \subseteq L'$. Since φ induces an isomorphism $\overline{\varphi}\colon K[X]/fK[X] \to K'[X]/f^\varphi K'[X]$, the map $\widehat{\varphi} := (\overline{\varphi}_a)^{-1}\overline{\varphi}\overline{\varphi}_{a'}$ is as desired. ♯

(5.8) Corollary. Let K be a field and let $f \in K[X] \setminus K$.
a) Then there is a splitting field L for f such that $[L\colon K] \leq \deg(f)!$.
b) Let K' be a field, let $\varphi\colon K \to K'$ be an isomorphism, let L/K be a splitting field for f, let L'/K' be a splitting field for $f^\varphi \in K'[X]$. Then there is an isomorphism $\widehat{\varphi}\colon L \to L'$ such that $\widehat{\varphi}|_K = \varphi$; in particular, $\widehat{\varphi}$ induces a bijection between the roots of f in L and the roots of f^φ in L', respecting multiplicities.

Proof. a) We proceed by induction on $n := \deg(f) \in \mathbb{N}$, and assume that f is monic. If $n = 1$ then $f = X - a \in K[X]$, thus K is a splitting field

such that $[K\colon K] = 1$. Let $n \geq 2$, and let $g \in K[X]$ be irreducible such that $g \mid f$. Then there is a field extension M/K having an element $a_n \in M$ such that $g(a_n) = 0$ and $M = K(a_n)$, hence $[M\colon K] = \deg(g) \leq n$. Thus there is $f' \in M[X]$ such that $f = (X - a_n)f' \in M[X]$, and since $\deg(f') = n - 1$ there is a splitting field $L := M(a_1, \ldots, a_{n-1})$ for f' over M, where $f' = \prod_{i=1}^{n-1}(X - a_i) \in L[X]$, having degree $[L\colon M] \leq (n-1)!$. Hence we have $K(a_1, \ldots, a_n) = K(a_n)(a_1, \ldots, a_{n-1}) = M(a_1, \ldots, a_{n-1}) = L$, where $f = \prod_{i=1}^{n}(X - a_i) \in L[X]$, and $[L\colon K] = [L\colon M] \cdot [M\colon K] \leq (n-1)! \cdot n = n!$.

b) We proceed by induction on $d := [L\colon K] \in \mathbb{N}$. If $d = 1$ then we have $L = K$, thus there are $a_1, \ldots, a_n \in K$ such that $f = \mathrm{lc}(f) \cdot \prod_{i=1}^{n}(X - a_i) \in K[X]$. Hence $f^\varphi = \mathrm{lc}(f)^\varphi \cdot \prod_{i=1}^{n}(X - a_i^\varphi) \in K'[X]$, thus $L' = K'(a_1^\varphi, \ldots, a_n^\varphi) = K'$, and we let $\widehat{\varphi} = \varphi$. Let $d \geq 2$, and let $g \in K[X]$ be irreducible such that $g \mid f$, where we may assume that $\deg(g) \geq 2$. Then $g^\varphi \in K'[X]$ is irreducible such that $g^\varphi \mid f^\varphi$. Let $a \in L$ be a root of g, and let $a' \in L'$ be a root of g^φ, hence there is an isomorphism $\widetilde{\varphi}\colon K(a) \to K'(a')$ extending φ. Then $L/K(a)$ is a splitting field for f, and $L'/K'(a')$ is a splitting field for f^φ. Since $[L\colon K(a)] = \frac{[L\colon K]}{[K(a)\colon K]} = \frac{[L\colon K]}{\deg(g)} < [L\colon K] = d$, there is an isomorphism $\widehat{\varphi}\colon L \to L'$ extending $\widetilde{\varphi}$. ♯

(5.9) Example. a) Let $f := X^2 + 1 \in \mathbb{R}[X]$, hence f is irreducible. By the Kronecker construction $L := \mathbb{R}[Y]/(Y^2 + 1)\mathbb{R}[Y]$ contains the roots $\pm\overline{Y}$ of f, where $\overline{\ }\colon \mathbb{R}[Y] \to L$ is the natural homomorphism; hence L is a splitting field for $f = (X - \overline{Y})(X + \overline{Y}) \in L[X]$. Thus we have an isomorphism $L \to L\colon \overline{Y} \mapsto -\overline{Y}$ extending $\mathrm{id}_\mathbb{R}$. Since $X^2 + 1 = (X - \sqrt{-1})(X + \sqrt{-1}) \in \mathbb{C}[X]$ and $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$ there are isomorphisms $L \to \mathbb{C}\colon \overline{Y} \mapsto \sqrt{-1}$ and $L \to \mathbb{C}\colon \overline{Y} \mapsto -\sqrt{-1}$ extending $\mathrm{id}_\mathbb{R}$, as well as $\mathbb{C} \to \mathbb{C}\colon \sqrt{-1} \mapsto -\sqrt{-1}$, being called **complex conjugation**.

b) Let $f := X^3 - 2 \in \mathbb{Q}[X]$, hence f is irreducible. Letting $\rho := \sqrt[3]{2} \in \mathbb{R} \subseteq \mathbb{C}$ and $\zeta := \zeta_3 = \exp(\frac{2\pi\sqrt{-1}}{3}) = \frac{1+\sqrt{-3}}{2} \in \mathbb{C}$, we have $\zeta^3 = 1$, and thus the roots of f are $\rho \in \mathbb{R} \subseteq \mathbb{C}$ and $\rho\zeta^{\pm 1} \in \mathbb{C} \setminus \mathbb{R}$. Thus the Kronecker construction yields $\mathbb{Q}[X]/(X^3 - 2)\mathbb{Q}[X] \cong K_\epsilon := \mathbb{Q}(\rho\zeta^\epsilon) \subseteq \mathbb{C}$, where $\epsilon \in \{0, 1, -1\}$. We have $f = X^3 - \rho^3 = (X - \rho)(X^2 + \rho X + \rho^2) \in K_0[X]$, where $X^2 + \rho X + \rho^2 \in K_0[X]$ does not have a root in $K_0 \subseteq \mathbb{R}$, thus is irreducible. Hence K_0 is not a splitting field for f, and thus neither K_1 and K_{-1} is.

Applying the Kronecker construction again yields $K_0[X]/(X^2 + \rho X + \rho^2)K_0[X]$, which contains a root of $X^2 + \rho X + \rho^2$, and thus is a splitting field for f. We have $X^2 + \rho X + \rho^2 = (X - \rho\zeta)(X - \rho\zeta^{-1}) \in \mathbb{C}[X]$, hence we have $K_0[X]/(X^2 + \rho X + \rho^2)K_0[X] \cong L := K_0(\rho\zeta) = \mathbb{Q}(\rho, \rho\zeta) = \mathbb{Q}(\rho, \zeta) \subseteq \mathbb{C}$. Thus L is the splitting field for f in $\mathbb{C}$, and we have $[L\colon \mathbb{Q}] = [L\colon K_0] \cdot [K_0\colon \mathbb{Q}] = 2 \cdot 3 = 6 = \deg(f)!$.

(5.10) Theorem. A finite field extension L/K is **normal**, i. e. any irreducible polynomial in $K[X]$ having a root in L already splits in $L[X]$, if and only if L is a splitting field for some polynomial in $K[X] \setminus K$.

Proof. Let L/K be normal, let $\{a_1, \ldots, a_n\} \subseteq L$ be a K-basis, and let $\mu_i \in K[X]$ be the minimum polynomial of a_i over K. Then the irreducible polynomial $\mu_i \in K[X]$ has the root $a_i \in L$, thus $f := \prod_{i=1}^n \mu_i$ splits in $L[X]$. Since $L = K(a_1, \ldots, a_n)$ we conclude that L is a splitting field for f over K.

Let conversely L be a splitting field for $f \in K[X] \setminus K$, and let $g \in K[X]$ be irreducible having a root $a \in L$. Let M/L be a splitting field for g, and let $b \in M$ be a root of g. Hence there is an isomorphism $\varphi\colon K(a) \to K(b)$ such that $\varphi|_K = \mathrm{id}_K$. Since $L(a) = L$ is a splitting field for f over $K(a)$, and $L(b)$ is a splitting field for f over $K(b)$, there is an isomorphism $\widehat{\varphi}\colon L(a) \to L(b)$ extending φ. Since $\widehat{\varphi}|_K = \mathrm{id}_K$ is equivalent to $\widehat{\varphi}$ being K-linear, we have $[L\colon K] = [L(b)\colon K]$, thus $L = L(b)$ and $b \in L$, implying that g splits in $L[X]$. ♯

(5.11) Corollary. Let L/K be a finite field extension.
a) Then there is a normal finite field extension M/K such that $L \subseteq M$.
b) If L/K is normal, then L is normal over any intermediate field $K \subseteq M \subseteq L$.

(5.12) Derivatives. Let K be a field and let $f = \sum_{i \geq 0} a_i X^i \in K[X]$. Then the **derivative** of f is defined as $\frac{\partial f}{\partial X} := \sum_{i \geq 1} i a_i X^{i-1} \in K[X]$. Hence we have $\frac{\partial f}{\partial X} = 0$ or $\deg(\frac{\partial f}{\partial X}) < \deg(f)$, and if $K \subseteq L$ is a field extension then the derivative of $f \in K[X]$ and the derivative of $f \in L[X]$ coincide. The map $\frac{\partial}{\partial X}\colon K[X] \to K[X]$ is K-linear, and we have $\frac{\partial(fg)}{\partial X} = \frac{\partial f}{\partial X} \cdot g + f \cdot \frac{\partial g}{\partial X}$ for all $f, g \in K[X]$: We may assume that $f = X^i$ and $g = X^j$ where $i, j \in \mathbb{N}_0$, and since $\frac{\partial 1}{\partial X} = 0$ we may assume $i, j \geq 1$, then we have $\frac{\partial(X^{i+j})}{\partial X} = (i+j)X^{i+j-1} = iX^{i-1}X^j + jX^iX^{j-1} = \frac{\partial(X^i)}{\partial X} \cdot X^j + X^i \cdot \frac{\partial(X^j)}{\partial X}$.

For $f \in K[X] \setminus K$ let $\widetilde{f} \in \gcd(f, \frac{\partial f}{\partial X}) \subseteq K[X]$. Then the multiple roots of f in a splitting field L for f coincide with the roots of $\widetilde{f}$ in L: By the Euclidean algorithm we have $\widetilde{f} \in \gcd_{L[X]}(f, \frac{\partial f}{\partial X}) \subseteq L[X]$. For $a \in L$ we have $f = (X-a)^m g$, where $m \in \mathbb{N}_0$ and $g \in L[X]$ such that $g(a) \neq 0$. If a is a root of f, then $m \geq 1$, thus $\frac{\partial f}{\partial X} = m(X-a)^{m-1}g + (X-a)^m \frac{\partial g}{\partial X} = (X-a)^{m-1}(mg + (X-a)\frac{\partial g}{\partial X}) \in L[X]$. If a is a multiple root of f, hence $m \geq 2$, then $X - a \mid \widetilde{f} \in L[X]$, thus a is a root of $\widetilde{f}$. Conversely, if a is a root of $\widetilde{f}$, then it is a root of f, thus $m \geq 1$, and a root of $\frac{\partial f}{\partial X}$, hence a root of $\frac{\partial f}{\partial X} - (X-a)^m \frac{\partial g}{\partial X} = m(X-a)^{m-1}g$, which since $g(a) \neq 0$ implies $m \geq 2$.

Hence f has a multiple root in L if and only if we have $\widetilde{f} \notin K$. In particular, if f is irreducible then f has a multiple root in L if and only if $\frac{\partial f}{\partial X} = 0$: We have either $\widetilde{f} \in K$ or $\widetilde{f} \sim f \in K[X]$, where since $\frac{\partial f}{\partial X} = 0$ or $\deg(\frac{\partial f}{\partial X}) < \deg(f)$ the latter case occurs if and only if $\frac{\partial f}{\partial X} = 0$.

Thus for f irreducible, if $\mathrm{char}(K) = 0$ then f has only simple roots in L, while if $\mathrm{char}(K) = p > 0$ then f has a multiple root in L if and only if there is $g \in K[X]$ such that $f = g(X^p) \in K[X]$: If $f = \sum_{i \geq 0} a_i X^i$ such that $\frac{\partial f}{\partial X} = \sum_{i \geq 1} i a_i X^{i-1} = 0$, then we have $a_i = 0$ for all $p \not| \, i \in \mathbb{N}_0$, thus $f = \sum_{i \geq 0} a_{ip} X^{ip}$,

and if conversely $f = \sum_{i\geq 0} a_{ip} X^{ip}$ then we have $\frac{\partial f}{\partial X} = \sum_{i\geq 1} ipa_{ip} X^{ip-1} = 0$.

(5.13) Separability. Let K be a field. An irreducible polynomial $f \in K[X]$ is called **separable**, if it has only simple roots in a splitting field for f; otherwise f is called **inseparable**. A polynomial $f \in K[X] \setminus K$ is called **separable**, if all its irreducible divisors are separable; in particular a squarefree polynomial $f \in K[X] \setminus K$ is separable if and only if it has only simple roots in a splitting field for f. The field K is called **perfect** if all irreducible polynomials in $K[X]$ are separable.

Let L/K be a field extension. An element $a \in L$ is called **separable** over K, if $a \in L$ is algebraic over K and its minimum polynomial $\mu_a \in K[X]$ over K is separable, equivalently $a \in L$ is a simple root of μ_a. The field extension L/K is called **separable** if any element of L is separable over K. E. g. any algebraic extension of a perfect field is separable, if $\mathrm{char}(K) = 0$ then K is perfect, and if K is a finite field then K is perfect as well:

(5.14) Proposition. Let K be a field such that $\mathrm{char}(K) = p > 0$. Then the **Frobenius map** $\varphi_p \colon K \to K \colon a \mapsto a^p$ is a monomorphism, and K is perfect if and only if $\varphi_p \colon K \to K$ is surjective, i. e. if and only if φ_p is an isomorphism.

Proof. For $a, b \in K$ we have $(ab)^p = a^p b^p \in K$ and $1^p = 1 \in K$, and since $p \mid \binom{p}{i}$, for all $i \in \{1, \ldots, p-1\}$, we have $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p \in K$.

Let $\varphi_p \colon K \to K$ be surjective, and assume there is $f \in K[X]$ irreducible and inseparable. Then there is $g = \sum_{i\geq 0} a_i X^i \in K[X]$ such that $f = g(X^p) \in K[X]$. Let $b_i \in K$ such that $a_i = b_i^p$ for all $i \geq 0$. Hence the Frobenius map on $K(X)$ yields $f = g(X^p) = \sum_{i\geq 0} b_i^p X^{ip} = (\sum_{i\geq 0} b_i X^i)^p \in K[X]$, a contradiction.

Let $\varphi_p \colon K \to K$ be not surjective and let $a \in K \setminus \mathrm{im}(\varphi_p)$. Hence $f := X^p - a \in K[X]$ does not have a root in K. Let $g \in K[X]$ be an irreducible divisor of f, hence $d := \deg(g) > 1$, and let $b \in L$ be a root of g in a splitting field L for g. Thus we have $0 = f(b) = b^p - a \in L$, which yields $f = X^p - b^p = (X-b)^p \in L[X]$. Thus $g = (X-b)^d \in L[X]$ has a multiple root in L, hence g is inseparable. ♯

(5.15) Example. Let K be a field such that $\mathrm{char}(K) = p > 0$. Then $X \in K(X) \setminus \mathrm{im}(\varphi_p)$, hence $K(X)$ is not perfect: Assume there are $f = \sum_{i\geq 0} a_i X^i \in K[X]$ and $0 \neq g = \sum_{i\geq 0} b_i X^i \in K[X]$ such that $X = (\frac{f}{g})^p \in K(X)$, hence $\sum_{i\geq 0} a_i^p X^{ip} = f^p = g^p \cdot X = \sum_{i\geq 0} b_i^p X^{ip+1} \in K[X]$, a contradiction.

(5.16) Theorem: Finite fields. a) Let K be a finite field such that $|K| = p^n$, for a prime $p \in \mathbb{N}$ and $n \in \mathbb{N}$. Then K is a splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$. **b)** Let $p \in \mathbb{N}$ be a prime and $n \in \mathbb{N}$, and let K be a splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$. Then we have $|K| = p^n$.

Thus up to isomorphism there is a unique field of cardinality p^n, being called the associated **Galois field** $\mathrm{GF}(p^n) = \mathbb{F}_{p^n}$.

Proof. a) Since $|K^*| = p^n - 1$ we have $a^{p^n-1} = 1 \in K$ for all $a \in K^*$, and thus $a^{p^n} - a = 0 \in K$ for all $a \in K$. Hence $X^{p^n} - X = \prod_{a \in K}(X - a) \in K[X]$ splits, thus K is a splitting field for $X^{p^n} - X$.
b) Letting $f := X^{p^n} - X \in \mathbb{F}_p[X]$, its set of roots $M := \{a \in K; f(a) = 0 \in K\} = \{a \in K; a^{p^n} = a\} \subseteq K$ is a subfield: We have $0, 1 \in M$, and for $a, b \in M$ such that $b \neq 0$ we by iteration of the Frobenius map get $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$ and $(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1}$, thus $M \subseteq K$ is an additive subgroup and $M \setminus \{0\} \subseteq K^*$ is a multiplicative subgroup. Hence M is a splitting field for f, and thus $M = K$. Since $\frac{\partial f}{\partial X} = -1 \in \mathbb{F}_p[X]$ we have $\gcd(f, \frac{\partial f}{\partial X}) = \mathbb{F}_p^*$, thus f has only simple roots, hence $|K| = |M| = p^n$. ♯

(5.17) Theorem: Existence of primitive elements. Let L/K be a field extension, let $c_1, \ldots, c_n \in L$ be separable over K, and let $b \in L$ be algebraic over K. Then $K(b, c_1, \ldots, c_n)/K$ is a simple field extension. In particular, if L/K is finite and K is perfect then L/K is simple.

Proof. Letting $a := c_1$, it suffices to show that $K(a, b)/K$ is simple. Since $K(a, b)/K$ is finite, we are done if K is a finite field. Thus we may assume that K is infinite, and we may assume that $a \notin K$. Let $\mu_a \in K[X]$ and $\mu_b \in K[X]$ be the minimum polynomials of a and b over K, respectively. We may assume that μ_a and μ_b split in $L[X]$, hence we have $\mu_a = \prod_{i=1}^{n}(X - a_i) \in L[X]$, where $n \geq 2$, the a_i are pairwise distinct and $a = a_1$, and $\mu_b = \prod_{j=1}^{m}(X - b_j) \in L[X]$, where $b = b_1$. Let $d \in K \setminus \{\frac{b_j - b}{a - a_i} \in L; i \in \{2, \ldots, n\}, j \in \{1, \ldots, m\}\} \neq \emptyset$ and $c := ad + b \in K(a, b) \subseteq L$. Then we have $K(a, b) = K(c)$:

Let $f \in \gcd(\mu_a(X), \mu_b(c - dX)) \subseteq K(c)[X] \subseteq L[X]$ be monic. Since $\mu_a(a) = 0$ and $\mu_b(c - da) = \mu_b(b) = 0$ we have $X - a \mid f$. Since $f \mid \mu_a$, we conclude that f splits in $L[X]$, and its roots are amongst the a_i. Assume $\mu_b(c - da_i) = 0$ for some $i \in \{2, \ldots, n\}$, then for some $j \in \{1, \ldots, m\}$ we have $b_j = c - da_i = d(a - a_i) + b$, implying $d = \frac{b_j - b}{a - a_i}$, a contradiction. Thus $X - a_i \not| \mu_b(c - dX)$ for all $i \in \{2, \ldots, n\}$, hence $a \in L$ is the only root of f in L. Since $\mu_a \in K[X]$ is irreducible and separable, we have $f = X - a \in K(c)[X] \subseteq L[X]$. Thus we have $a \in K(c)$ and hence $b = c - ad \in K(c)$, implying $K(a, b) \subseteq K(c)$. ♯

6 Galois theory

(6.1) Galois groups. Let L/K be a field extension, and let $\mathrm{Aut}(L)$ be the group of automorphisms of L. The subgroup $\mathrm{Aut}(L/K) := \{\varphi \in \mathrm{Aut}(L); \varphi|_K = \mathrm{id}_K\} \leq \mathrm{Aut}(L)$ is called the **Galois group** of L over K, or the **group of K-automorphisms** of L.

Hence we have $\mathrm{Aut}(L/K) = \mathrm{Aut}(L) \cap \mathrm{Hom}_K(L, L)$. For any intermediate field $K \subseteq M \subseteq L$ we have $\mathrm{Aut}(L/M) \leq \mathrm{Aut}(L/K)$. We have $\mathrm{Aut}(L) = \mathrm{Aut}(L/P(L))$: Letting $\varphi_L \colon \mathbb{Z} \to L$ be the natural homomorphism, we have $P(L) = \mathcal{Q}(\mathrm{im}(\varphi_L)) \subseteq L$, and for $\varphi \in \mathrm{Aut}(L)$ we have $\varphi|_{\mathrm{im}(\varphi_L)} = \mathrm{id}_{\mathrm{im}(\varphi_L)}$, thus $\varphi|_{\mathcal{Q}(\mathrm{im}(\varphi_L))} = \mathrm{id}_{\mathcal{Q}(\mathrm{im}(\varphi_L))}$.

For $S \subseteq \mathrm{Aut}(L/K)$ let $\mathrm{Fix}_L(S) := \{a \in L; a^\varphi = a \text{ for all } \varphi \in S\}$ be the associated set of **fixed points**; we have $\mathrm{Fix}_L(S) = \mathrm{Fix}_L(\langle S\rangle)$. Hence we have $K \subseteq \mathrm{Fix}_L(S)$, and for $a, b \in \mathrm{Fix}_L(S)$ such that $b \neq 0$ we have $a - b \in \mathrm{Fix}_L(S)$ and $ab^{-1} \in \mathrm{Fix}_L(S)$, implying that $\mathrm{Fix}_L(S)$ is a field, being called the **fixed field** of S. The field extension L/K is called **Galois** if $\mathrm{Fix}_L(\mathrm{Aut}(L/K)) = K$.

(6.2) Proposition: Dedekind's Theorem. Let K be a field, let G be a monoid, and let $\varphi_1, \ldots, \varphi_n \colon G \to K^*$ be monoid homomorphisms. Then the set $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{Maps}(G, K)$ is K-linearly independent if and only if $\varphi_1, \ldots, \varphi_n$ are pairwise distinct; here $\mathrm{Maps}(G, K)$ is an K-vector space with respect to pointwise addition and scalar multiplication.

Proof. Letting $\varphi_1, \ldots, \varphi_n$ be pairwise distinct, we proceed by induction on $n \in \mathbb{N}$: Let $n = 1$, and let $\varphi_1 a_1 = 0$ for some $a_1 \in K$, then $1^{\varphi_1} = 1$ implies $a_1 = 1a_1 = 0$. Let $n \geq 2$, let $\sum_{i=1}^n \varphi_i a_i = 0$ where $a_i \in K$, and let $y \in G$ such that $y^{\varphi_1} \neq y^{\varphi_n}$. For all $x \in G$ we have $(\sum_{i=1}^n x^{\varphi_i} a_i) y^{\varphi_1} = 0$ and $\sum_{i=1}^n (xy)^{\varphi_i} a_i = \sum_{i=1}^n x^{\varphi_i} y^{\varphi_i} a_i = 0$, thus we have $\sum_{i=1}^n x^{\varphi_i}(y^{\varphi_1} - y^{\varphi_i}) a_i = 0$. Hence $\sum_{i=2}^n \varphi_i (y^{\varphi_1} - y^{\varphi_i}) a_i = 0$ by induction implies $(y^{\varphi_1} - y^{\varphi_i}) a_i = 0$ for $i \in \{2, \ldots, n\}$, thus $a_n = 0$, and by induction $a_i = 0$ for $i \in \{1, \ldots, n-1\}$. ♯

(6.3) Proposition. Let L/K and L'/K be finite field extensions. Then there are at most $[L\colon K]$ monomorphisms $\varphi \colon L \to L'$ such that $\varphi_K = \mathrm{id}_K$. In particular, we have $|\mathrm{Aut}(L/K)| \leq [L\colon K]$.

Proof. Let $\varphi_1, \ldots, \varphi_n \colon L \to L'$ be pairwise distinct monomorphisms such that $\varphi_i|_K = \mathrm{id}_K$. Then the maps $\varphi_i^* := \varphi_i|_{L^*} \colon L^* \to (L')^*$ are pairwise distinct, thus $\{\varphi_1^*, \ldots, \varphi_n^*\} \subseteq \mathrm{Maps}(L^*, L')$ is L'-linearly independent, hence $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{Maps}(L, L')$ is L'-linearly independent. Since $\mathrm{Hom}_K(L, L') \leq \mathrm{Maps}(L, L')$ as L'-vector spaces, the set $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{Hom}_K(L, L')$ is L'-linearly independent, hence $n \leq \dim_{L'}(\mathrm{Hom}_K(L, L'))$. Since $\mathrm{Hom}_K(L, L') \cong K^{[L'\colon K] \times [L\colon K]}$ as K-vector spaces we have $[L'\colon K] \cdot \dim_{L'}(\mathrm{Hom}_K(L, L')) = \dim_K(\mathrm{Hom}_K(L, L')) = [L'\colon K] \cdot [L\colon K]$, thus $\dim_{L'}(\mathrm{Hom}_K(L, L')) = [L\colon K]$. ♯

(6.4) Proposition: Artin's Theorem. Let L/K be a finite field extension, and let $H \leq \mathrm{Aut}(L/K)$. Then we have $[L\colon \mathrm{Fix}_L(H)] = |H|$.

Proof. Let $M := \mathrm{Fix}_L(H)$. From $\varphi|_M = \mathrm{id}_M$ for all $\varphi \in H$ we conclude $n := |H| \leq [L\colon M]$. Conversely, let $H = \{\varphi_1, \ldots, \varphi_n\}$ and $\mathrm{Tr}_H := \sum_{i=1}^n \varphi_i \in \mathrm{Maps}(L, L)$ be the associated **trace map**. Since $\{\varphi_1, \ldots, \varphi_n\} \subseteq \mathrm{Maps}(L, L)$ is L-linearly independent, we have $\mathrm{Tr}_H \neq 0$. For all $\varphi \in H$ and $a \in L$ we have $(\mathrm{Tr}_H(a))^\varphi = \sum_{i=1}^n a^{\varphi_i \varphi} = \sum_{i=1}^n a^{\varphi_i} = \mathrm{Tr}_H(a)$, thus we have $\mathrm{Tr}_H(a) \in M$.

Let $\{a_1, \ldots, a_{n+1}\} \subseteq L$ be any subset, and let $A := [a_j^{\varphi_i^{-1}}]_{ij} \in L^{n \times (n+1)}$. Hence the system of L-linear equations $A \cdot \mathcal{X}^{\mathrm{tr}} = 0 \in L^{n \times 1}$, where $\mathcal{X} = [X_1, \ldots, X_{n+1}]$, has a solution $0 \neq [x_1, \ldots, x_{n+1}] \in L^{n+1}$. Picking $k \in \{1, \ldots, n+1\}$ such that

$x_k \neq 0$, and replacing $[x_1, \ldots, x_{n+1}]$ by a non-zero scalar multiple if necessary, we may assume that $\mathrm{Tr}_H(x_k) \neq 0$. We thus have $\sum_{j=1}^{n+1} a_j^{\varphi_i^{-1}} x_j = 0$, hence $\sum_{j=1}^{n+1} a_j x_j^{\varphi_i} = 0$ for all $i \in \{1, \ldots, n\}$, implying $\sum_{j=1}^{n+1} a_j \mathrm{Tr}_H(x_j) = 0$. Since $\mathrm{Tr}_H(x_j) \in M$ for all $j \in \{1, \ldots, n+1\}$, and $\mathrm{Tr}_H(x_k) \neq 0$, this implies that $\{a_1, \ldots, a_{n+1}\} \subseteq L$ is M-linearly dependent, and hence $[L\colon M] \leq n$. ♯

(6.5) Theorem. For a finite field extension L/K the following are equivalent:
a) The field extension L/K is Galois, i. e. we have $\mathrm{Fix}_L(\mathrm{Aut}(L/K)) = K$.
b) We have $[L\colon K] = |\mathrm{Aut}(L/K)|$.
c) The field extension L/K is normal and separable.
d) The field L is a splitting field for a separable polynomial in $K[X] \setminus K$.

Proof. a)⇔b): Letting $M := \mathrm{Fix}_L(\mathrm{Aut}(L/K))$ we have $|\mathrm{Aut}(L/K)| = [L\colon M]$, and L/K is Galois if and only if $[L\colon M] = [L\colon K]$.

a)⇒c): Let $G := \mathrm{Aut}(L/K)$. For $a \in L$ let $a^G = \{a_1, \ldots, a_m\} \subseteq L$ be the associated G-orbit, where $a_1 := a$, and let $f_a := \prod_{i=1}^m (X - a_i) = \sum_{j=0}^m b_j X^j \in L[X]$. For $\varphi \in G$ we have $f_a^\varphi = \prod_{i=1}^m (X - a_i^\varphi) = \prod_{i=1}^m (X - a_i) = f_a$, hence $b_j^\varphi = b_j$, thus $b_j \in \mathrm{Fix}_L(\mathrm{Aut}(L/K)) = K$. Hence $f_a \in K[X]$ has a as a root, and since f_a has pairwise distinct roots a is separable over K, thus L/K is separable.

Let $\{a_1, \ldots, a_n\} \subseteq L$ be a K-basis, hence in particular $L = K(a_1, \ldots, a_n)$, and for all $j \in \{1, \ldots, n\}$ let $a_j^G = \{a_{j1}, \ldots, a_{jm_j}\} \subseteq L$ be the associated G-orbit and $f_j := \prod_{i=1}^{m_j} (X - a_{ji}) \in L[X]$. Hence we have $f_j \in K[X]$, and $f := \prod_{j=1}^n f_j$ splits in $L[X]$. Since $f(a_j) = 0$ we conclude that L is a splitting field for f.

c)⇒d): By normality let L/K be a splitting field for $f \in K[X] \setminus K$. Let $g \in K[X]$ be irreducible such that $g \mid f$, hence g splits in $L[X]$. Since g is the minimum polynomial of any of its roots in L, by separability g has only simple roots in L. Hence g is separable, and thus f is separable as well.

d)⇒a): Let L/K be a splitting field for the separable polynomial $f \in K[X] \setminus K$, which we may assume monic and squarefree, hence $f = \prod_{i=1}^n (X - a_i) \in L[X]$, where the $a_i \in L$ are pairwise distinct. We proceed by induction on $r := |\{i \in \{1, \ldots, n\}; a_i \notin K\}| \in \mathbb{N}_0$: If $r = 0$ then $K = L$ and thus $\mathrm{Fix}_L(\mathrm{Aut}(L/K)) = K$. Let $r \geq 1$, hence we may assume $a := a_1 \in L \setminus K$. Thus we have $K(a) \neq K$, and $L/K(a)$ is a splitting field for the separable polynomial $f \in K(a)[X]$. Thus by induction $L/K(a)$ is Galois, and since $\mathrm{Aut}(L/K(a)) \leq \mathrm{Aut}(L/K)$ we have $\mathrm{Fix}_L(\mathrm{Aut}(L/K)) \subseteq \mathrm{Fix}_L(\mathrm{Aut}(L/K(a))) = K(a)$.

Let $\mu_a \in K[X]$ be the minimum polynomial of a over K. Hence we have $\mu_a \mid f \in K[X]$, and thus we may assume that $\mu_a = \prod_{i=1}^m (X - a_i) \in L[X]$ where $m \leq n$. Hence for $i \in \{1, \ldots, m\}$ there are pairwise distinct isomorphisms $\psi_i\colon K(a) \to K(a_i)\colon a \mapsto a_i$ extending id_K, and thus there are isomorphisms $\varphi_i \in \mathrm{Aut}(L/K)$ extending ψ_i. Let $b = \sum_{j=0}^{m-1} b_j a^j \in \mathrm{Fix}_L(\mathrm{Aut}(L/K)) \subseteq K(a) \cong K[X]/\mu_a K[X]$, where $b_j \in K$. This yields $b = b^{\varphi_i} = \sum_{j=0}^{m-1} b_j (a^j)^{\varphi_i} = \sum_{j=0}^{m-1} b_j a_i^j$. Thus $g := -b + \sum_{j=0}^{m-1} b_j X^j \in K(a)[X]$ has $m > \deg(g)$ pairwise

distinct roots $\{a_1, \dots, a_m\} \subseteq L$, implying $g = 0$. Thus we have $b = b_0 \in K$, and hence $\mathrm{Fix}_L(\mathrm{Aut}(L/K)) = K$. ♯

(6.6) Corollary. a) Let L/K be a finite field extension, generated by separable elements. Then there is a finite Galois extension M/K such that $L \subseteq M$.
b) Let L/K be a field extension. Then the **separable closure** $L_s := \{a \in L; a \text{ separable over } K\}$ of K in L is a subfield of L.

(6.7) Theorem: Galois correspondence. Let L/K be a finite Galois extension, and let $G := \mathrm{Aut}(L/K)$. Then the following maps are mutually inverse inclusion-reversing bijections:

$$\mathcal{F}\colon \{H \leq G \text{ subgroup}\} \to \{K \subseteq M \subseteq L \text{ intermediate field}\}\colon H \mapsto \mathrm{Fix}_L(H)$$

$$\mathcal{G}\colon \{K \subseteq M \subseteq L \text{ intermediate field}\} \to \{H \leq G \text{ subgroup}\}\colon M \mapsto \mathrm{Aut}(L/M)$$

For all subgroups $H \leq G$ we have $[L\colon \mathcal{F}(H)] = |H|$, and for all intermediate fields $K \subseteq M \subseteq L$ we have $[M\colon K] = [G\colon \mathcal{G}(M)]$.

For an intermediate field $K \subseteq M \subseteq L$ the field extension M/K is Galois if and only if $M\varphi = M$ for all $\varphi \in G$, which holds if and only if $\mathrm{Aut}(L/M) \trianglelefteq G$; in this case we have $G/\mathrm{Aut}(L/M) \cong \mathrm{Aut}(M/K)$.

Proof. For $H \leq G$ we have $H \leq \mathrm{Aut}(L/\mathrm{Fix}_L(H)) = \mathcal{GF}(H)$, and for $K \subseteq M \subseteq L$ we have $M \subseteq \mathrm{Fix}_L(\mathrm{Aut}(L/M)) = \mathcal{FG}(M)$. Applying $\mathcal{F}$ to the first inequality yields $\mathcal{F}(H) \supseteq \mathcal{FGF}(H)$, and the second inequality for $M = \mathcal{F}(H)$ yields $\mathcal{F}(H) \subseteq \mathcal{FGF}(H)$, hence we have $\mathcal{F}(H) = \mathcal{FGF}(H)$. Thus we have $|H| = [L\colon \mathcal{F}(H)] = [L\colon \mathcal{FGF}(H)] = |\mathcal{GF}(H)|$, and since $H \leq \mathcal{GF}(H)$ this implies $H = \mathcal{GF}(H)$, thus $\mathcal{GF} = \mathrm{id}$; so far we only used that L/K is finite.

For any intermediate field $K \subseteq M \subseteq L$, the field extension L/M is a splitting field for some separable polynomial in $M[X] \setminus M$, hence is Galois. Thus we have $M = \mathrm{Fix}_L(\mathrm{Aut}(L/M)) = \mathcal{FG}(M)$, hence $\mathcal{FG} = \mathrm{id}$ as well. We have $|G| = [L\colon K] = [L\colon M] \cdot [M\colon K] = [L\colon \mathcal{FG}(M)] \cdot [M\colon K] = |\mathcal{G}(M)| \cdot [M\colon K]$, hence $[M\colon K] = \frac{|G|}{|\mathcal{G}(M)|} = [G\colon \mathcal{G}(M)]$.

We have $\mathcal{G}(M) \trianglelefteq G$ if and only if $\mathcal{G}(M)^\varphi = \mathcal{G}(M)$ for all $\varphi \in G$, which holds if and only if $\mathcal{F}(\mathcal{G}(M)^\varphi) = \mathcal{FG}(M) = M$. We have $\mathcal{F}(\mathcal{G}(M)^\varphi) = \{a \in L; a\varphi^{-1}\psi\varphi = a \text{ for all } \psi \in \mathcal{G}(M)\} = \{a \in L; a\varphi^{-1} \in \mathcal{FG}(M)\} = (\mathcal{FG}(M))\varphi = M\varphi$. Thus we have $\mathrm{Aut}(L/M) \trianglelefteq G$ if and only if $M\varphi = M$ for all $\varphi \in G$. The latter condition holds if and only if M/K is normal, which holds if and only if M/K is Galois:

By separability we have $M = K(a)$ for some primitive element $a \in L$. Let $M\varphi = M$ for all $\varphi \in G$, and let $f := \prod_{\varphi \in G}(X - a^\varphi) \in M[X]$. For $\psi \in G$ we have $f^\psi = \prod_{\varphi \in G}(X - a^{\varphi\psi}) = \prod_{\varphi \in G}(X - a^\varphi) = f$. Thus we have $f \in \mathrm{Fix}_L(G)[X] = K[X]$ such that $f(a) = 0$, splitting in $M[X]$, hence M/K is a splitting field for f, and thus M/K is normal.

Conversely let M/K be normal, then the minimum polynomial $\mu_a \in K[X]$ of a over K, having the root $a \in M$, splits in $M[X]$. Thus M contains all roots of μ_a in L. Since for $\varphi \in G$ we have $\mu_a(a^\varphi) = (\mu_a(a))^\varphi = 0$, we conclude $a^\varphi \in M$, and thus $M\varphi \subseteq M$, by K-linearity and M/K finite implying $M\varphi = M$.

If M/K is Galois, since $M\varphi = M$ for all $\varphi \in G$, we have the group homomorphism $\mathrm{res}^L_M \colon G \to \mathrm{Aut}(M/K) \colon \varphi \mapsto \varphi|_M$. Since L/M is a splitting field for some polynomial in $M[X] \setminus M$, any element of $\mathrm{Aut}(M/K)$ extends to an element of G, thus res^L_M is surjective. We have $\ker(\mathrm{res}^L_M) = \{\varphi \in G; \varphi|_M = \mathrm{id}_M\} = \mathrm{Aut}(L/M)$, and thus $G/\mathrm{Aut}(L/M) \cong \mathrm{Aut}(M/K)$. ♯

(6.8) Example. a) Since $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is a splitting field for $X^2 + 1 \in \mathbb{R}[X]$, the field extension $\mathbb{C}/\mathbb{R}$ is Galois, and we have $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_\mathbb{C}, \overline{\ }\} \cong C_2$, where $\overline{\ } \colon \mathbb{C} \to \mathbb{C} \colon \sqrt{-1} \to -\sqrt{-1}$ is complex conjugation.

b) Let $f := X^3 - 2 \in \mathbb{Q}[X]$, see (5.9), hence f is irreducible. Letting $\rho := \sqrt[3]{2} \in \mathbb{R} \subseteq \mathbb{C}$ and $\zeta := \zeta_3 := \exp(\frac{2\pi\sqrt{-1}}{3}) \in \mathbb{C}$, the roots of f in $\mathbb{C}$ are $\rho\zeta^\epsilon$, where $\epsilon \in \{0, 1, -1\}$. Thus $L := \mathbb{Q}(\zeta, \rho) \subseteq \mathbb{C}$ is the splitting field for f in $\mathbb{C}$, hence $L/\mathbb{Q}$ is Galois such that $[L \colon \mathbb{Q}] = 6$, see Table 3. Let $K_\epsilon := \mathbb{Q}(\rho\zeta^\epsilon)$, hence we have $[K_\epsilon \colon \mathbb{Q}] = 3$ and $K_\epsilon/\mathbb{Q}$ is not normal. Letting $M := \mathbb{Q}(\zeta)$, from $\mu_\zeta = X^2 + X + 1 \in \mathbb{Q}[X]$ we get $[M \colon \mathbb{Q}] = 2$, hence $M/\mathbb{Q}$ is normal.

Let $G := \mathrm{Aut}(L/\mathbb{Q})$, hence we have $|G| = 6$. We have $L = M(\rho)$, and since $[L \colon M] = 3$ we conclude that $f = X^3 - 2 \in M[X]$ is irreducible, thus there is $\tau \in \mathrm{Aut}(L/M)$ given by $\tau \colon \zeta \mapsto \zeta, \rho \mapsto \zeta\rho$. Hence $\tau \colon \rho \mapsto \zeta\rho \mapsto \zeta^{-1}\rho \mapsto \rho$ shows $|\tau| = 3$, thus $\mathrm{Aut}(L/M) = \langle\tau\rangle \cong C_3$ and $\mathrm{Fix}_L(\tau) = M$. We have $L = K_0(\zeta)$, and since $[L \colon K_0] = 2$ we conclude that $\mu_\zeta = X^2 + X + 1 \in K_0[X]$ is irreducible, thus there is $\sigma \in \mathrm{Aut}(L/K_0)$ given by $\sigma \colon \rho \mapsto \rho, \zeta \mapsto \zeta^{-1}$, hence $\mathrm{Aut}(L/K_0) = \langle\sigma\rangle \cong C_2$ and $\mathrm{Fix}_L(\sigma) = K_0$.

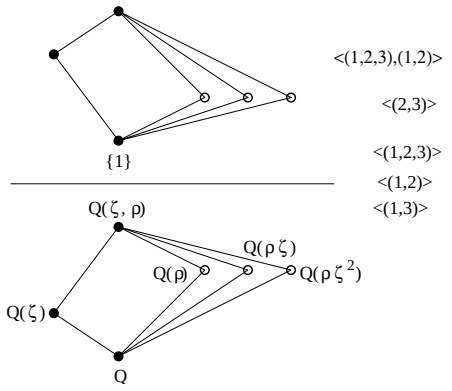
We have $\tau^\sigma \colon \zeta \mapsto \zeta, \rho \mapsto \zeta^{-1}\rho$, hence $\tau^\sigma = \tau^{-1}$, and thus $G \cong D_6 \cong \mathcal{S}_3$. The subgroup lattice of G shows that we have found all intermediate fields of $L/\mathbb{Q}$. Since $|\sigma\tau| = |\sigma\tau^{-1}| = 2$ we have $\mathrm{Fix}_L(\sigma\tau) = K_{-1}$ and $\mathrm{Fix}_L(\sigma\tau^{-1}) = K_1$.

c) Let $f := X^4 - 2 \in \mathbb{Q}[X]$, hence f is irreducible. Letting $\rho := \sqrt[4]{2} \in \mathbb{R} \subseteq \mathbb{C}$ and $\zeta := \zeta_4 = \sqrt{-1} \in \mathbb{C}$, we have $f = \prod_{k=0}^3 (X - \zeta^k\rho) \in \mathbb{C}[X]$. Thus $L := \mathbb{Q}(\zeta, \rho) \subseteq \mathbb{C}$ is the splitting field for f in $\mathbb{C}$, see Table 4.

Letting $K := \mathbb{Q}(\rho) \subseteq \mathbb{R}$, we have $[K \colon \mathbb{Q}] = 4$ and $f = (X-\rho)(X+\rho)(X^2+\rho^2) \in K[X]$, where $g := X^2 + \rho^2 \in K[X]$ is irreducible, hence $K/\mathbb{Q}$ is not normal. Since $g = (X - \zeta\rho)(X + \zeta\rho) \in L[X]$, we have $L = K(\zeta\rho)$, and thus $[L \colon K] = 2$, yielding $[L \colon \mathbb{Q}] = 8$. Similarly, letting $K' := \mathbb{Q}(\zeta\rho) \not\subseteq \mathbb{R}$, we have $[K' \colon \mathbb{Q}] = 4$ and $f = (X-\zeta\rho)(X+\zeta\rho)(X^2-\rho^2) \in K'[X]$, where hence $g' := X^2-\rho^2 \in K'[X]$ is irreducible, while $g' = (X - \rho)(X + \rho) \in L[X]$, hence $K'/\mathbb{Q}$ is not normal.

We have $\mathbb{Q}(\rho^2) = \mathbb{Q}(\zeta^2\rho^2) = \mathbb{Q}(\sqrt{2}) = K \cap K'$, where since $\mu_{\rho^2} = X^2-2 \in \mathbb{Q}[X]$ we have $[\mathbb{Q}(\rho^2) \colon \mathbb{Q}] = 2$, hence $\mathbb{Q}(\rho^2)/\mathbb{Q}$ is normal. Letting $M := \mathbb{Q}(\zeta)$, from $\mu_\zeta = X^2+1 \in \mathbb{Q}[X]$ we get $[M \colon \mathbb{Q}] = 2$, hence $M/\mathbb{Q}$ is normal. Since $\zeta \notin \mathbb{Q}(\rho^2)$ we have $[\mathbb{Q}(\zeta, \rho^2) \colon \mathbb{Q}] = 4$, and being a splitting field for $(X^2-2)(X^2+1) \in \mathbb{Q}[X]$

Table 3: Galois correspondence for $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$.



the field extension $\mathbb{Q}(\zeta, \rho^2)/\mathbb{Q}$ is normal. We have $\mathbb{Q}(\zeta\rho^2) = \mathbb{Q}(\sqrt{-2})$, where $\mu_{\zeta\rho^2} = X^2 + 2 \in \mathbb{Q}[X]$ implies $[\mathbb{Q}(\zeta\rho^2)\colon \mathbb{Q}] = 2$, hence $\mathbb{Q}(\zeta\rho^2)/\mathbb{Q}$ is normal.

Let $G := \mathrm{Aut}(L/\mathbb{Q})$, hence we have $|G| = 8$. We have $L = M(\rho)$, and since $[L\colon M] = 4$ we conclude that $f = X^4 - 2 \in M[X]$ is irreducible, thus there is $\tau \in \mathrm{Aut}(L/M)$ given by $\tau\colon \zeta \mapsto \zeta, \rho \mapsto \zeta\rho$. Hence $\tau\colon \rho \mapsto \zeta\rho \mapsto -\rho \mapsto \zeta^{-1}\rho \mapsto \rho$ shows $|\tau| = 4$ and thus $\mathrm{Aut}(L/M) = \langle\tau\rangle \cong C_4$. We have $\mathbb{Q}(\zeta, \rho^2) \subseteq \mathrm{Fix}_L(\tau^2)$, thus from $[L\colon \mathbb{Q}(\zeta, \rho^2)] = 2 = |\tau^2|$ we get $\mathrm{Fix}_L(\tau^2) = \mathbb{Q}(\zeta, \rho^2)$.

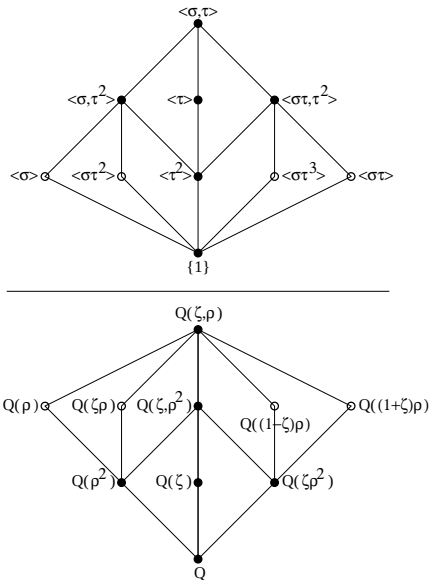
We have $L = K(\zeta)$, and since $[L\colon K] = 2$ we conclude that $\mu_\zeta = X^2 + 1 \in K[X]$ is irreducible, thus there is $\sigma \in \mathrm{Aut}(L/K)$ given by $\sigma\colon \rho \mapsto \rho, \zeta \mapsto -\zeta = \zeta^{-1}$, hence $\mathrm{Aut}(L/K) = \langle\sigma\rangle \cong C_2$. Since $\mathrm{Fix}_L(\tau) \cap \mathrm{Fix}_L(\sigma) = M \cap K = \mathbb{Q}$ and $L = \mathbb{Q}(M, K)$, we get $\langle\tau, \sigma\rangle = G$ and $\langle\tau\rangle \cap \langle\sigma\rangle = \{1\}$, respectively.

We have $\tau^\sigma\colon \zeta \mapsto \zeta, \rho \mapsto \zeta^{-1}\rho$, hence $\tau^\sigma = \tau^{-1}$. Thus we have $G \cong D_8$. From the subgroup lattice of G we determine all intermediate fields of $L/\mathbb{Q}$: We have $\mathrm{Fix}_L(\langle\sigma, \tau^2\rangle) = K \cap \mathbb{Q}(\zeta, \rho^2) = \mathbb{Q}(\rho^2)$ and $\mathrm{Fix}_L(\sigma\tau^2) = K'$, as well as $\mathrm{Fix}_L(\langle\sigma\tau, \tau^2\rangle) = \mathbb{Q}(\zeta\rho^2)$.

To find $\mathrm{Fix}_L(\sigma\tau)$ and $\mathrm{Fix}_L(\sigma\tau^3)$ we use the trace map $\mathrm{Tr}_{\langle\sigma\tau\rangle} = \mathrm{id} + \sigma\tau\colon L \to \mathrm{Fix}_L(\sigma\tau)$: We have $\mathrm{Tr}_{\langle\sigma\tau\rangle}(\zeta) = \zeta + \zeta^{-1} = 0$ as well as $\mathrm{Tr}_{\langle\sigma\tau\rangle}(\rho) = \rho + \zeta\rho = (1 + \zeta)\rho =: \omega$. Since $\omega^{\tau^2} = \zeta^2\omega \neq \omega$ we have $\omega \notin \mathbb{Q}(\zeta\rho^2)$, hence $\mathrm{Fix}_L(\sigma\tau) = \mathbb{Q}(\omega)$; since $\zeta_8 := \exp(\frac{2\pi\sqrt{-1}}{8}) = \frac{1}{\sqrt{2}} \cdot (1 + \zeta) \in \mathbb{C}$ we have $\omega = \zeta_8\rho^3 \in \mathbb{C}$, hence $\omega^4 = -8$, thus $\mu_\omega = X^4 + 8 \in \mathbb{Q}[X]$. Since $\sigma\tau^3 = (\sigma\tau)^\sigma$, we have $\mathrm{Fix}_L(\sigma\tau^3) = \mathrm{Fix}_L(\sigma\tau)^\sigma = \mathbb{Q}(\omega^\sigma) = \mathbb{Q}((1 - \zeta)\rho)$.

(6.9) Finite fields. Let $p \in \mathbb{N}$ be a prime and $n \in \mathbb{N}$. Since $\mathbb{F}_{p^n}$ is a splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$, the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, and we have $|\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n}\colon \mathbb{F}_p] = n$. Let the Frobenius automorphism $\varphi_p \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ have order $k \mid n$. Then $\varphi_p^k = \mathrm{id}_{\mathbb{F}_{p^n}}$ implies $a^{p^k} = a$ for

Table 4: Galois correspondence for $\mathbb{Q}(\zeta_4, \sqrt[4]{2})/\mathbb{Q}$.



$a \in \mathbb{F}_{p^n}$, hence all elements of $\mathbb{F}_{p^n}$ are roots of $X^{p^k} - X \in \mathbb{F}_p[X]$. Thus we have $p^k \geq p^n$, implying that $k = n$ and $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi_p \rangle \cong C_n$.

The Galois correspondence is given as follows: For any $d \in \mathbb{N}$ such that $d \mid n$ there is a unique subgroup $\langle \varphi_p^d \rangle \trianglelefteq \langle \varphi_p \rangle$ of index d. Hence for any such d there is a unique intermediate field $\mathbb{F}_p \subseteq M := \mathrm{Fix}_{\mathbb{F}_{p^n}}(\varphi_p^d) \subseteq \mathbb{F}_{p^n}$ such that $[M\colon \mathbb{F}_p] = d$, where from $|M| = p^d$ we infer $M \cong \mathbb{F}_{p^d}$. The field extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^d}$ is Galois such that $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) = \langle \varphi_p^d \rangle$, and the field extension $\mathbb{F}_{p^d}/\mathbb{F}_p$ is Galois such that $\langle \varphi_p|_{\mathbb{F}_{p^d}} \rangle = \mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)/\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) = \langle \varphi_p \rangle / \langle \varphi_p^d \rangle$.

(6.10) Cyclotomic fields. For $n \in \mathbb{N}$ let $\zeta_n := \exp(\frac{2\pi\sqrt{-1}}{n}) \in \mathbb{C}$. Then $\mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$ is called the n-th **cyclotomic field**; we have $\zeta_1 = 1$ and $\zeta_2 = -1$ and $\zeta_4 = \sqrt{-1}$, thus $\mathbb{Q} = \mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2)$, and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ is called the **Gaussian number field**.

The group $\langle \zeta_n \rangle \leq \mathbb{C}^*$ of n-th **roots of unity** has order n, its generators are called **primitive** n-th roots of unity. Thus we have $X^n - 1 = \prod_{k \in \mathbb{Z}/n\mathbb{Z}} (X - \zeta_n^k) \in \mathbb{C}[X]$. Running over the primitive roots yields the n-th **cyclotomic polynomial** $\Phi_n := \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta_n^k) \in \mathbb{C}[X]$, thus $\deg(\Phi_n) = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. Hence $X^n - 1 = \prod_{d \mid n} \Phi_d \in \mathbb{C}[X]$, by induction yielding $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ and $\Phi_n = \frac{X^n - 1}{\prod_{d \mid n, d \neq n} \Phi_d} \in \mathbb{Z}[X]$ for all $n \neq 1$. Then $\Phi_n \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ is irreducible:

Let $\Phi_n = fg \in \mathbb{Z}[X]$, where f, g are monic and f is irreducible, and let ζ be a primitive n-th root of unity such that $f(\zeta) = 0$. We show that for any $k \in (\mathbb{Z}/n\mathbb{Z})^*$ we have $f(\zeta^k) = 0$ as well, implying that $\Phi_n = f$; it suffices to show $f(\zeta^p) = 0$ for all primes $p \in \mathbb{N}$ such that $p \not| n$: Assume that $f(\zeta^p) \neq 0$, then $g(\zeta^p) = 0$ implies $\mu_\zeta = f \mid g(X^p) \in \mathbb{Z}[X]$, hence $g(X^p) = fh$ for some $h \in \mathbb{Z}[X]$. Using the natural homomorphism $\overline{\ }\colon \mathbb{Z} \to \mathbb{F}_p$, and that $\mathbb{F}_p$ is the prime field of characteristic p, this implies $\overline{fh} = \overline{g(X^p)} = \overline{g}^p \in \mathbb{F}_p[X]$, and hence $1 \notin \gcd(\overline{f}, \overline{g})$. From $X^n - 1 = \overline{fg} \cdot \prod_{d \mid n, d \neq n} \overline{\Phi_d} \in \mathbb{F}_p[X]$ we infer that $X^n - 1 \in \mathbb{F}_p[X]$ has a multiple root in a splitting field. Since $\frac{\partial(X^n-1)}{\partial X} = \overline{n}X^{n-1} \neq 0 \in \mathbb{F}_p[X]$, thus $1 \in \gcd(X^n - 1, \overline{n}X^{n-1})$, this is a contradiction. ♯

We thus have $\mu_{\zeta_n} = \Phi_n$, hence $[\mathbb{Q}(\zeta_n)\colon \mathbb{Q}] = \varphi(n)$. Since Φ_n splits in $\mathbb{Q}(\zeta_n)[X]$, we conclude that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$ is the splitting field for Φ_n in $\mathbb{C}$, hence $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois. Thus we have $|\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, and for any $k \in (\mathbb{Z}/n\mathbb{Z})^*$ there is an automorphism $\varphi_k\colon \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)\colon \zeta_n \mapsto \zeta_n^k$ extending $\mathrm{id}_\mathbb{Q}$; in particular φ_{-1} is the restriction of complex conjugation to $\mathbb{Q}(\zeta_n)$. Hence $(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\colon k \mapsto \varphi_k$ is an isomorphism.

7 Applications

(7.1) Construction with ruler and compass. We consider the Euclidean plane $\mathbb{R}^2$, and assume the points $[0, 0], [1, 0] \in \mathbb{R}^2$ to be given. To construct new points, we draw lines through two distinct points already constructed, or circles around points already constructed whose radii are the distances of points already constructed, and take the finite non-empty line-line, line-circle and circle-circle intersections as new points.

Let $\mathcal{M} \subseteq \mathbb{R}$ be the set of all coordinates of all points which can be thus constructed in a finite number of steps; instead, only the first or only the second coordinates may be considered. We have $0, 1 \in \mathcal{M}$, and for $a, b \in \mathcal{M}$ such that $b \neq 0$ we have $a - b \in \mathcal{M}$ and $ab^{-1} \in \mathcal{M}$, hence $\mathcal{M} \subseteq \mathbb{C}$ is a field. For $0 \leq a \in \mathcal{M}$ we have $\sqrt{a} \in \mathcal{M}$ as well, hence any quadratic polynomial $X^2 + pX + q = (X + \frac{p}{2})^2 - ((\frac{p}{2})^2 - q) \in \mathcal{M}[X]$ such that $(\frac{p}{2})^2 - q \geq 0$ splits.

Let $a \in \mathbb{R}$. Then we have $a \in \mathcal{M}$ if and only if there are fields $\mathbb{Q} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n \subseteq \mathbb{R}$, where $n \in \mathbb{N}_0$, such that $[M_i\colon M_{i-1}] = 2$ for $i \in \{1, \ldots, n\}$ and $a \in M_n$: If the M_i are as above, we by induction on $i \in \mathbb{N}_0$ have $M_i \subseteq \mathcal{M}$, where $M_0 = \mathbb{Q} \subseteq \mathcal{M}$: For $i \geq 1$ there is $b \in M_i$ such that $M_i = M_{i-1}(b)$, having minimum polynomial $\mu_b = X^2 + pX + q \in M_{i-1}[X]$ such that $(\frac{p}{2})^2 - q > 0$. Thus we have $M_i = M_{i-1}(\sqrt{(\frac{p}{2})^2 - q}) \subseteq \mathcal{M}$. Conversely, if $M \subseteq \mathcal{M}$ is a subfield, lines and circles are given by equations $aX + bY = c$ and $(X - s)^2 + (Y - t)^2 = r^2$, where $a, b, c, r, s, t \in M$. If any two of these intersect in a finite non-empty set, the intersection consists of one or two points, whose coordinates are roots of polynomials over M of degree at most 2; for circle-circle intersections we by translation, dilatation and rotation may assume that the circles are given as the unit circle $X^2 + Y^2 = 1$ and $(X - s)^2 + Y^2 = r^2$, where $s \neq 0$, implying

$(x-s)^2 - x^2 = r^2 - 1$ and thus $x = \frac{s^2-r^2+1}{2s} \in M$ and $y^2 = 1 - x^2$.

This allows to show the insolubility of various problems from classical geometry: Given a unit cube in the Euclidean space $\mathbb{R}^3$, **Deli's problem** is to construct a cube having volume 2, hence to construct $\sqrt[3]{2}$, but $X^3 - 2 \in \mathbb{Q}[X]$ being irreducible we have $[\mathbb{Q}(\sqrt[3]{2})\colon \mathbb{Q}] = 3$, thus $\sqrt[3]{2} \notin \mathcal{M}$. Given a unit circle, the **squaring problem** is to construct a square having area π, to construct $\sqrt{\pi}$, but π being transcendental over $\mathbb{Q}$ we have $\pi \notin \mathcal{M}$, see (7.4).

Given a constructible angle $0 \leq \beta \leq \pi$, i. e. $\cos(\beta) \in \mathcal{M}$, the **trisection problem** is to construct $\frac{\beta}{3}$, i. e. to construct $\cos(\frac{\beta}{3}) \in \mathbb{R}$. But there is $0 \leq \alpha \leq \frac{\pi}{3}$ such that $\cos(3\alpha) \in \mathcal{M}$ and $\cos(\alpha) \notin \mathcal{M}$: From $\exp(3\alpha\sqrt{-1}) = \exp(\alpha\sqrt{-1})^3$, taking real and imaginary parts and using $\sin(\alpha)^2 + \cos(\alpha)^2 = 1$ yields $\cos(3\alpha) = \cos(\alpha)^3 - 3\sin(\alpha)^2\cos(\alpha) = 4\cos(\alpha)^3 - 3\cos(\alpha)$. Letting $\alpha := \frac{\pi}{9}$, hence $\cos(3\alpha) = \frac{1}{2}$, shows that $a := \cos(\frac{\pi}{9})$ is a root of $f := 4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X]$. Since $f(\frac{X+1}{2}) = \frac{1}{2}(X^3 + 3X^2 - 3) \in \mathbb{Q}[X]$, the Eisenstein Criterion for $p = 3$ shows that f is irreducible. Hence we have $[\mathbb{Q}(a)\colon \mathbb{Q}] = 3$, thus $a \notin \mathcal{M}$.

A **regular n-gon**, for $n \in \mathbb{N}$, is constructible if and only if $\varphi(n)$ is a 2-power: A regular n-gon is constructible if and only if $a := \cos(\frac{2\pi}{n}) \in \mathcal{M}$, equivalently $b := \sin(\frac{2\pi}{n}) \in \mathcal{M}$. If $a \in \mathcal{M}$, then $[\mathbb{Q}(a)/\mathbb{Q}]$ is a 2-power, and since $a^2 + b^2 = 1$ and $\zeta_n = a + b\sqrt{-1}$ we conclude that $[\mathbb{Q}(a,b)/\mathbb{Q}]$ and $\varphi(n) = [\mathbb{Q}(\zeta_n)/\mathbb{Q}]$ are 2-powers. Conversely, if $[\mathbb{Q}(\zeta_n)/\mathbb{Q}]$ is a 2-power, let $M := \mathrm{Fix}_{\mathbb{Q}(\zeta_n)}(\varphi_{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ be the **real subfield** of the Galois extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$; since $\mathrm{Aut}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian, $M/\mathbb{Q}$ is Galois. Since $[M\colon \mathbb{Q}]$ is a 2-power this implies that there are fields $\mathbb{Q} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$, where $k \in \mathbb{N}_0$, such that $[M_i\colon M_{i-1}] = 2$ for $i \in \{1, \ldots, k\}$. Since $a = \frac{1}{2}(\zeta_n + \zeta_n^{\varphi_{-1}}) \in M$ we conclude $a \in \mathcal{M}$.

We determine $\varphi(n)$: Let $m \in \mathbb{N}$ be coprime to n. Then for the natural homomorphism $\nu\colon \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, where the right hand side is a ring with respect to **componentwise** addition and multiplication, we have $\ker(\nu) = m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \trianglelefteq \mathbb{Z}$, and since $|\mathbb{Z}/mn\mathbb{Z}| = mn = |(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})|$ the induced map $\mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ is an isomorphism. Hence we have $(\mathbb{Z}/mn\mathbb{Z})^* \cong ((\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}))^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ as groups, and thus $\varphi(mn) = \varphi(m)\varphi(n)$, i. e. φ is a **number theoretic function**. This reduces us to the case p^e where $p \in \mathbb{N}$ is a prime and $e \in \mathbb{N}$: We have $(\mathbb{Z}/p^e\mathbb{Z}) \setminus (\mathbb{Z}/p^e\mathbb{Z})^* = \{\overline{x} \in \mathbb{Z}/p^e\mathbb{Z}; x \in \mathbb{Z}_{p^e}, p \mid x\} = \{\overline{xp} \in \mathbb{Z}/p^e\mathbb{Z}; x \in \mathbb{Z}_{p^{e-1}}\}$, hence $\varphi(p^e) = p^e - p^{e-1} = (p-1)p^{e-1}$.

Thus $\varphi(n)$ is a 2-power if and only if for $p^e \mid n$, where $p \in \mathbb{N}$ is a prime and $e \in \mathbb{N}$, the number $\varphi(p^e) = (p-1)p^{e-1}$ is a 2-power, which holds if and only if for any such prime power we have $p = 2$, or $e = 1$ and $p = 2^m + 1$ is a **Fermat prime** for some $m \in \mathbb{N}$.

If $p = 2^m + 1$ is a Fermat prime, for some $m = kl \in \mathbb{N}$ where $k, l \in \mathbb{N}$ such that l is odd, then $X^{kl} + 1 = (X^k + 1) \cdot \sum_{i=1}^{l} (-1)^{i-1} X^{k(l-i)} \in \mathbb{Z}[X]$ implies that $2^k + 1 \mid 2^m + 1$, hence $k = m$ and $l = 1$. Thus p is of the form $F_k = 2^{2^k} + 1$ for some $k \in \mathbb{N}_0$, where $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ are

the only known Fermat primes; it is not known whether this list is complete, not even whether there are only finitely many Fermat primes.

(7.2) Theorem: Wedderburn [1905]. Any finite skewfield is a field.

Proof. Let K be a finite skewfield. For $a \in K$ let $C_K(a) := \{b \in K; ab = ba\}$ be the associated **centraliser**, and let $Z(K) := \bigcap_{a \in K} C_K(a)$ be the **centre** of K. The $C_K(a)$ are subskewfields, and $Z(K)$ is a subfield of K, thus K and $C_K(a)$ are $Z(K)$-vector spaces. Let $n := \dim_{Z(K)}(K) \in \mathbb{N}$ and $n_a := \dim_{Z(K)}(C_K(a)) \in \mathbb{N}$, letting $q := |Z(K)| \geq 2$ we get $|K| = q^n$ and $|C_K(a)| = q^{n_a}$.

From $C_K(a)^* \leq K^*$ we get $q^{n_a} - 1 \mid q^n - 1$, which implies $n_a \mid n$: For $m \in \mathbb{N}$ let $k \in \mathbb{Z}$ and $l \in \{0, \ldots, m-1\}$ such that $n = km + l$; hence we have $\gcd(n, m) = \gcd(m, l) \subseteq \mathbb{Z}$. Then $X^n - 1 = (X^m - 1) \cdot \sum_{i=1}^{k} X^{m(k-i)+l} + (X^l - 1) \in \mathbb{Z}[X]$ implies $\gcd(q^n - 1, q^m - 1) = \gcd(q^m - 1, q^l - 1) \subseteq \mathbb{Z}$ and thus $\gcd(q^n - 1, q^m - 1) = q^d - 1$, where $0 < d \in \gcd(n, m)$.

Writing K^* as the disjoint union of its conjugacy classes, where $\mathcal{T} \subseteq K^*$ is a set of representatives, we from $Z(K)^* = \{a \in \mathcal{T}; n_a = n\}$ get $|K^*| = |Z(K)^*| + \sum_{a \in \mathcal{T}, n_a < n} \frac{|K^*|}{|C_K(a)^*|}$, hence $q^n - 1 = q - 1 + \sum_{a \in \mathcal{T}, n_a < n} \frac{q^n - 1}{q^{n_a} - 1}$. Since $(X^m - 1)\Phi_n \mid (X^n - 1) \in \mathbb{Z}[X]$ for $n \neq m \mid n$, we infer $\Phi_n(q) \mid (q^n - 1) - \sum_{a \in \mathcal{T}, n_a < n} \frac{q^n - 1}{q^{n_a} - 1} = q - 1 \in \mathbb{Z}$, hence $|\Phi_n(q)| \leq q - 1$. For $n \geq 2$ and $k \in (\mathbb{Z}/n\mathbb{Z})^*$ we by the triangle inequality have $|q - \zeta_n^k| > q - 1 \geq 1$, implying $|\Phi_n(q)| = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} |q - \zeta_n^k| > (q-1)^{\varphi(n)} \geq q - 1$, a contradiction. Hence we have $n = 1$, thus $K = Z(K)$ is commutative. ♯

(7.3) Theorem: Fundamental Theorem of Algebra [Gauß, 1801]. Let $L/\mathbb{C}$ be an algebraic field extension. Then we have $L = \mathbb{C}$.

Proof: Artin. We may assume that $L/\mathbb{C}$ is finite. Hence $L/\mathbb{R}$ is finite as well, and since $L/\mathbb{R}$ is separable we may assume that $L/\mathbb{R}$ is Galois. Let $G := \mathrm{Aut}(L/\mathbb{R})$, for $S \in \mathrm{Syl}_2(G)$ let $\mathbb{R} \subseteq K := \mathrm{Fix}_L(S) \subseteq L$, and let $a \in K$ such that $K = \mathbb{R}(a)$, having minimum polynomial $\mu_a \in \mathbb{R}[X]$. Since $\deg(\mu_a) = [K\colon \mathbb{R}] = \frac{|G|}{|S|}$ is odd, by the **mean value theorem** we conclude that μ_a has a root in $\mathbb{R}$, thus $\deg(\mu_a) = 1$. Hence we have $G = S$, thus G is a 2-group.

Hence $L/\mathbb{C}$ is Galois such that $H := \mathrm{Aut}(L/\mathbb{C}) < G$ is a 2-group. Assume that $|H| > 1$, then H has a normal subgroup of index 2, and replacing L by the associated fixed field, we may assume that $[L\colon \mathbb{C}] = 2$. Thus there is $b \in L$ such that $L = \mathbb{C}(b)$, having minimum polynomial $\mu_b = X^2 + pX + q = (X + \frac{p}{2})^2 - ((\frac{p}{2})^2 - q) \in \mathbb{C}[X]$. Since any element $r \exp(\alpha\sqrt{-1}) \in \mathbb{C}$, where $r \in \mathbb{R}_{\geq 0}$ and $\alpha \in \mathbb{R}$, has the square roots $\pm\sqrt{r} \exp(\frac{\alpha\sqrt{-1}}{2}) \in \mathbb{C}$, we deduce that μ_b splits, a contradiction. Thus we have $|H| = 1$ and hence $L = \mathbb{C}$. ♯

(7.4) Algebraic closure. Let L/K be a field extension. Then $\overline{K} := \{a \in L; a \text{ algebraic over } K\} \subseteq L$ is a subfield, called the **algebraic closure** of K in L: Let $a, b \in \overline{K}$ such that $b \neq 0$, then since $K(a,b)/K$ is finite and thus algebraic we have $a - b, ab^{-1} \in K(a,b) \subseteq \overline{K}$. Thus $\overline{K}/K$ is algebraic, and we have $\overline{K} = \overline{\overline{K}} \subseteq L$. If $K = \overline{K} \subseteq L$, then K is called **algebraically closed** in L.

If K is algebraically closed in any field extension L/K, then K is called **algebraically closed**; e. g. $\mathbb{C}$ is algebraically closed. A field K is algebraically closed if and only if any $f \in K[X] \setminus K$ splits; in particular algebraically closed fields are perfect: Let K be algebraically closed, and let $f \in K[X]$ be irreducible, then $L := K[X]/fK[X]$ is algebraic over K, thus $\deg(f) = [L\colon K] = 1$. Conversely, let the property on polynomials be fulfilled, let L/K be a field extension and let $a \in L$ be algebraic over K, then the minimum polynomial $\mu_a \in K[X]$ of a over K is irreducible, thus $\deg(\mu_a) = 1$, hence $a \in K$.

If L/K is algebraic such that L is algebraically closed, then L is called an **algebraic closure** of K; e. g. $\mathbb{C}/\mathbb{R}$ is an algebraic closure. An algebraic field extension L/K is an algebraic closure if and only if any $f \in K[X] \setminus K$ splits in $L[X]$: Let the property on polynomials be fulfilled, let M/L be a field extension, and let $a \in M$ be algebraic over L, then a is also algebraic over K, and the minimum polynomial $\mu_a \in K[X]$ of a over K splits in $L[X]$, hence $a \in L$.

If L/K is a field extension such that L is algebraically closed, then the algebraic closure $\overline{K} \subseteq L$ of K in L is an algebraic closure of K: Any $f \in K[X] \setminus K$ splits in $L[X]$, and all roots of f in L are algebraic over K, hence f splits in $\overline{K}[X]$.

Thus to show the existence of algebraic closures in general, it suffices to show the existence of an algebraically closed field extension: Let $\mathcal{Y} = \{Y_f; f \in K[X] \setminus K\}$ be commuting indeterminates. Then we have $I := \langle f(Y_f); f \in K[X] \setminus K\rangle \lhd K[\mathcal{Y}]$: Assume that there are $f_1, \ldots, f_n \in K[X] \setminus K$ and $g_1, \ldots, g_n \in K[\mathcal{Y}]$ such that $\sum_{i=1}^n f_i(Y_{f_i})g_i = 1 \in K[\mathcal{Y}]$. Let $Y_{f_{n+1}}, \ldots, Y_{f_m}$, for some $m \geq n$, be the further indeterminates occurring in the g_i, let M/K be a field extension such that f_i has a root $a_i \in M$ for $i \in \{1, \ldots, n\}$, and let $a_i := 0$ for $i \in \{n+1, \ldots, n\}$. The evaluation map $K[Y_{f_1}, \ldots, Y_{f_m}] \to M\colon Y_{f_i} \mapsto a_i$ yields $1 = \sum_{i=1}^n f_i(a_i)g_i(a_1, \ldots, a_m) = 0 \in M$, a contradiction. Hence let $J \lhd K[\mathcal{Y}]$ be maximal such that $I \subseteq J$, and $L_1 := K[\mathcal{Y}]/J$. Then L_1/K is a field extension such that any polynomial in $K[X] \setminus K$ has a root in L_1. By induction there are field extensions $K =: L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$, such that for $i \in \mathbb{N}_0$ any polynomial in $L_i[X] \setminus L_i$ has a root in L_{i+1}. Then $L := \bigcup_{i\in\mathbb{N}} L_i$ is a field extension such that any polynomial in $L[X] \setminus L$ has a root in L, hence L is algebraically closed.

We show uniqueness of algebraic closures: Let L/K and L'/K be algebraic closures. Then the set Φ of all isomorphisms $\varphi\colon M \to M'$ extending id_K, for some $K \subseteq M \subseteq L$ and $K \subseteq M' \subseteq L'$, is partially ordered by letting $(\varphi\colon M \to M') \leq (\psi\colon N \to N')$ if $M \subseteq N$ and $\psi_M = \varphi$. If $\Psi := \{\psi_i\colon M_i \to M_i'; i \in \mathbb{N}\} \subseteq \Phi$ is totally ordered, then $N := \bigcup_{i\in\mathbb{N}} M_i$ and $N' := \bigcup_{i\in\mathbb{N}} M_i'$ are fields, and there is an isomorphism $\psi\colon N \to N'$ such that $\psi|_{M_i} = \psi_i$ for all $i \in \mathbb{N}$, hence ψ is an upper bound for Ψ in Φ. Thus by Zorn's Lemma there

is a maximal element $\varphi\colon M \to M'$ in Φ. Let $a \in L$, and let $\mu_a \in M[X]$ be its minimum polynomial over M. Since $\mu_a^\varphi \in M'[X]$ splits in $L'[X]$, there is $a' \in L'$ and an isomorphism $M(a) \to M'(a')$ extending φ. By the maximality of φ we have $a \in M$, implying $M = L$. Let $b \in L'$, and let $\mu_b \in M'[X]$ be its minimum polynomial over M'. Since $M' = M^\varphi = L^\varphi$ is algebraically closed, μ_b splits, thus $b \in M'$, implying $M' = L'$.

E. g. the algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ of $\mathbb{Q}$ in $\mathbb{C}$, being called the **field of algebraic numbers**, is algebraically closed. Since $\mathbb{Q}$ is countable, $\mathbb{Q}[X]$ is countable as well, thus $\overline{\mathbb{Q}}$ also is countable. Since $\mathbb{C}$ is not countable, we have $\overline{\mathbb{Q}} \neq \mathbb{C}$, thus $\mathbb{C}$ contains more than countably many **transcendental numbers** [Cantor, 1874]. There are criteria to decide whether a given complex number is algebraic or transcendental [Liouville, 1844; Thue-Siegel-Roth, 1955]. These have been used to specify a particular transcendental number in the first place, while still it is not too easy to decide this for a given number. E. g. the **Euler number** $e := \sum_{n=0}^\infty \frac{1}{n!} \in \mathbb{R} \subseteq \mathbb{C}$ and $\pi := 2 \cdot \min\{x \in \mathbb{R}_{\geq 0}; \cos(x) = 0\} \in \mathbb{R} \subseteq \mathbb{C}$ are transcendental [Hermite, 1873; Lindemann, 1882].

(7.5) Kummer extensions. Let $n \in \mathbb{N}$, let K be a field such that $\mathrm{char}(K) \not| \, n$ and $X^n - 1 \in P(K)[X]$ splits in $K[X]$. Since $\frac{\partial(X^n-1)}{\partial X} = nX^{n-1} \neq 0$, the polynomial $X^n - 1 \in P(K)[X]$ has n pairwise distinct roots in K, called **n-th roots of unity**. The latter form a cyclic subgroup of K^* of order n. Let $\zeta \in K$ be a **primitive** root of unity, i. e. having order n, then all primitive roots of unity in K are given as $\{\zeta^k \in K; k \in (\mathbb{Z}/n\mathbb{Z})^*\}$, and for the n-th cyclotomic polynomial we have $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta^k) \in K[X]$.

If $p := \mathrm{char}(K) > 0$, then from $X^{p^a n} - 1 = (X^n - 1)^{p^a} \in P(K)[X]$ we conclude that $X^{p^a n} - 1$ also splits in $K[X]$, hence $p^a n$-th roots of unity and n-th roots of unity in K coincide, and there are no primitive $p^a n$-th roots of unity for $a \geq 1$.

Let $0 \neq a \in K$ and $f := X^n - a \in K[X]$, called the associated **pure equation**. Since $\frac{\partial(X^n-a)}{\partial X} = nX^{n-1} \neq 0$ the polynomial f has pairwise distinct roots in any extension field, thus is separable. Letting L/K be a field extension such that $b \in L$ is a root of f, its roots in L are $\{b\zeta^k \in L; k \in \mathbb{Z}/n\mathbb{Z}\}$, hence the **Kummer extension** $K(b)/K$ is a splitting field for f, thus is Galois.

For $\varphi \in \mathrm{Aut}(K(b)/K)$ we have $f(b^\varphi) = f(b)^\varphi = 0$, hence $b^\varphi = b\zeta^{k_\varphi}$ for some $k_\varphi \in \mathbb{Z}/n\mathbb{Z}$. The map $\mathrm{Aut}(K(b)/K) \to \mathbb{Z}/n\mathbb{Z}\colon \varphi \mapsto k_\varphi$ is an injective group homomorphism: For $\psi \in \mathrm{Aut}(K(b)/K)$ we since $\zeta \in K$ have $b^{\varphi\psi} = (b\zeta^{k_\varphi})^\psi = b\zeta^{k_\varphi k_\psi}$, hence $k_{\varphi\psi} = k_\varphi k_\psi$; and if $k_\varphi = 0$ then $b^\varphi = b$ implies $\varphi = \mathrm{id}_{K(b)}$. Hence $\mathrm{Aut}(K(b)/K)$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, in particular is cyclic. Since $K(b)/K$ is Galois, if f is irreducible then we have $\mathrm{Aut}(K(b)/K) \cong \mathbb{Z}/n\mathbb{Z}$.

Conversely, let L/K be a Galois extension such that $\mathrm{Aut}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, and let $\varphi \in \mathrm{Aut}(L/K)$ be a generator. Hence $\{\varphi^k \in \mathrm{Hom}_K(L,L); k \in \mathbb{Z}/n\mathbb{Z}\}$ is K-linearly independent, and thus for the **Lagrange resolvent** we have $0 \neq \rho := \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \varphi^k \zeta^k \in \mathrm{Hom}_K(L,L)$. Letting $c \in L$ such that $0 \neq b := c^\rho \in L$, we have $b^\varphi = c^{\rho\varphi} = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} (c^{\varphi^k} \zeta^k)^\varphi = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} c^{\varphi^{k+1}} \zeta^k = \zeta^{-1} \cdot \sum_{k \in \mathbb{Z}/n\mathbb{Z}} c^{\varphi^k} \zeta^k =$

$b\zeta^{-1}$, implying $(b^n)^\varphi = (\zeta^{-1}b)^n = b^n$, thus $a := b^n \in \mathrm{Fix}_L(\varphi) = K$, hence b is a root of $f := X^n - a \in K[X]$. Let $\mu_b \in K[X]$ be the minimum polynomial of b over K, hence $\mu_b \mid f$. For $k \in \mathbb{Z}/n\mathbb{Z}$ we have $\mu_b(b\zeta^{-k}) = \mu_b(b^{\varphi^k}) = \mu_b(b)^{\varphi^k} = 0$, hence $\{b\zeta^k \in L; k \in \mathbb{Z}/n\mathbb{Z}\}$ are roots of μ_b, and since $b \neq 0$ these are pairwise distinct. Hence we have $\deg(\mu_b) \geq n = \deg(f)$, thus $f = \mu_b$ is irreducible. Since $[K(b)\colon K] = n = [L\colon K]$ we have $L = K(b)$, hence L/K is a Kummer extension.

(7.6) Radical extensions. A field extension L/K is called a **radical extension**, if there are intermediate fields $K = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L$, where $m \in \mathbb{N}$, such that there are $0 \neq a_i \in K_i$ and $n_i \geq 2$ and roots $b_i \in K_{i+1}$ of $X^{n_i} - a_i \in K_i[X]$ such that $K_{i+1} = K_i(b_i)$, for all $i \in \{1, \ldots, m-1\}$; radical extensions are finite, and Kummer extensions are radical extensions.

If L/K is a separable radical extension then the n_i can be chosen such that $\mathrm{char}(K) \nmid n_i$, for all $i \in \{1, \ldots, m-1\}$: By choosing intermediate fields appropriately we may assume that $K_{i+1} \neq K_i$ and that n_i is a prime, hence assuming $n_i = \mathrm{char}(K)$ implies $X^{n_i} - a_i = X^{n_i} - b_i^{n_i} = (X - b_i)^{n_i}$, contradicting the separability of K_{i+1}/K_i. If L/K is a radical extension such that $\mathrm{char}(K) \nmid n_i$ for $i \in \{1, \ldots, m-1\}$, then there is a Galois radical extension M/K such that $L \subseteq M$; in particular L/K is separable:

We proceed by induction on $[L\colon K]$, where we may assume that $[L\colon K] \geq 2$: Letting $K = K_1 \subseteq K_2 \subseteq \cdots \subseteq L' := K_{m-1} \subseteq K_m = L$ be intermediate fields as above, we have $m \geq 2$ and we may assume that $L' \neq L$, hence $[L'\colon K] < [L\colon K]$; let $n := n_{m-1}$ and $a := a_{m-1} \in L'$ and $b := b_{m-1} \in L$. By induction there is a Galois radical extension M'/K such that $L' \subseteq M'$. Let M/M' be a splitting field for $f := \prod_{\varphi \in \mathrm{Aut}(M'/K)}(X^n - a^\varphi) \in M'[X]$; since $b \in L$ is a root of f we may assume that $L = L'(b) \subseteq M$. Since $\mathrm{char}(K) \nmid n$ we have $\frac{\partial(X^n - a^\varphi)}{\partial X} = nX^{n-1} \neq 0$, thus f is separable, and its shape implies that M/M' is a Galois radical extension. Since M'/K is a radical extension, M/K also is a radical extension. Since for all $\psi \in \mathrm{Aut}(M'/K)$ we have $f^\psi = \prod_{\varphi \in \mathrm{Aut}(M'/K)}(X^n - a^{\varphi\psi}) = f \in M'[X]$, we infer $f \in \mathrm{Fix}_{M'}(\mathrm{Aut}(M'/K))[X] = K[X]$. Since M/M' is a splitting field for the separable polynomial $f \in K[X] \setminus K$, and M'/K is a splitting field for some separable polynomial $g \in K[X] \setminus K$, we conclude that M/K is a splitting field for the separable polynomial $fg \in K[X] \setminus K$, hence is Galois. ♯

(7.7) Soluble groups. Let G be a finite group. A chain of subgroups $\{1\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 = G$ such that $G_{i+1} \trianglelefteq G_i$ for $i \in \{1, \ldots, m-1\}$ is called a **subnormal series**, the groups G_i/G_{i+1} are called the associated **sections**. If G has a subnormal series with abelian sections, then G is called **soluble**; in this case, since any non-trivial abelian group has a normal subgroup of prime order, G has a subnormal series with cyclic sections of prime order.

If G is soluble, then so is any subgroup $H \leq G$ and quotient group G/N, where $N \trianglelefteq G$: The chain of subgroups $\{1\} = H \cap G_m \leq H \cap G_{m-1} \leq \cdots \leq H \cap G_1 = H$ is a subnormal series with abelian sections $(H \cap G_i)/(H \cap G_{i+1}) \cong$

$(H \cap G_i)G_{i+1}/G_{i+1} \leq G_i/G_{i+1}$; the chain of subgroups $\{1\} = G_mN/N \leq G_{m-1}N/N \leq \cdots \leq G_1N/N = G/N$ is a subnormal series whose sections $(G_iN/N)/(G_{i+1}N/N)$ are epimorphic images of the abelian groups G_i/G_{i+1}.

E. g. any abelian group is soluble; the symmetric groups $\mathcal{S}_3$ and $\mathcal{S}_4$ are soluble, with subnormal series $\{1\} < \mathcal{A}_3 < \mathcal{S}_3$ and $\{1\} < V_4 < \mathcal{A}_4 < \mathcal{S}_4$, respectively, having abelian sections; for $n \geq 3$ the dihedral groups D_{2n} are soluble, with subnormal series $\{1\} < T_n < D_{2n}$ having abelian sections, see (2.9).

For $n \geq 5$ the symmetric group $\mathcal{S}_n$ is not soluble: Assume that $\{1\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 = \mathcal{S}_n$ is a subnormal series having abelian sections. Then for $i \in \{1, \ldots, m\}$ we successively conclude that G_i contains every 3-cycle, which holds for $i = 1$, and thus since $G_m = \{1\}$ is a contradiction: Letting $a, b, c, d, e \in \{1, \ldots, n\}$ be pairwise distinct, using the natural homomorphism $\overline{\ }\colon G_i \to G_i/G_{i+1}$ to the abelian group G_i/G_{i+1}, the **commutator** formula $(a,b,c)^{-1}(c,d,e)^{-1}(a,b,c)(c,d,e) = (a,c,d) \in \mathcal{S}_n$ shows that $\overline{(a,c,d)} = \overline{(a,b,c)}^{-1}\overline{(c,d,e)}^{-1}\overline{(a,b,c)(c,d,e)} = \overline{1} \in G_i/G_{i+1}$, hence $(a,c,d) \in G_{i+1}$.

(7.8) Theorem. Let L/K be Galois extension.
a) If L/K is a radical extension, then $\mathrm{Aut}(L/K)$ is soluble.
b) If $\mathrm{Aut}(L/K)$ is soluble where $\mathrm{char}(K) \nmid [L\colon K]$, then letting $n \in \mathbb{N}$ be the product of the distinct prime divisors of $[L\colon K]$ and M/L be a splitting field for $X^n - 1 \in \mathbb{Q}[X]$, the field extension M/K is a Galois radical extension.

Proof. a) Let $K = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L$ be intermediate fields, such that there are $0 \neq a_i \in K_i$ and $n_i \geq 2$ and roots $b_i \in K_{i+1}$ of $X^{n_i} - a_i \in K_i[X]$ such that $K_{i+1} = K_i(b_i)$; since L/K is separable we may assume $\mathrm{char}(K) \nmid n_i$ for all $i \in \{1, \ldots, m-1\}$. Let $0 < n \in \mathrm{lcm}\{n_1, \ldots, n_{m-1}\}$, hence we have $\mathrm{char}(K) \nmid n$. Let M/L be a splitting field for $X^n - 1 \in \mathbb{Q}[X]$, let $\zeta \in M$ be a primitive n-th root of unity, and letting $K_i' := K_i(\zeta)$ for $i \in \{1, \ldots, m\}$ we have $K \subseteq K(\zeta) = K_1' \subseteq K_2' \subseteq \cdots \subseteq K_m' = L(\zeta) = M$.

$K(\zeta)/K$ is a splitting field for the separable polynomial $\Phi_n \in K[X]$, hence is Galois. Since for $\varphi \in \mathrm{Aut}(K(\zeta)/K)$ we have $\Phi_n(\zeta^\varphi) = \Phi_n(\zeta)^\varphi = 0$, there is $k_\varphi \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\zeta^\varphi = \zeta^{k_\varphi}$. The map $\mathrm{Aut}(K(\zeta)/K) \to (\mathbb{Z}/n\mathbb{Z})^*\colon \varphi \mapsto k_\varphi$ is an injective group homomorphism, hence $\mathrm{Aut}(K(\zeta)/K)$ is abelian. Since $K_{i+1}' = K_i'(b_i)$ for $i \in \{1, \ldots, m-1\}$, and $X^{n_i} - 1 = \prod_{k \in \mathbb{Z}/n_i\mathbb{Z}}(X - (\zeta^{\frac{n}{n_i}})^k) \in K_i'[X]$ splits, K_{i+1}'/K_i' is a Kummer extension and $\mathrm{Aut}(K_{i+1}'/K_i')$ is cyclic.

Since L/K is a splitting field for some separable polynomial $g \in K[X] \setminus K$, we conclude that $L(\zeta)/K$ is a splitting field for $\Phi_n g \in K[X]$, hence is Galois. We have $\{1\} = \mathrm{Aut}(K_m'/K_m') \leq \mathrm{Aut}(K_m'/K_{m-1}') \leq \cdots \leq \mathrm{Aut}(K_m'/K_1') \leq \mathrm{Aut}(K_m'/K)$, where $\mathrm{Aut}(K_m'/K_{i+1}') \trianglelefteq \mathrm{Aut}(K_m'/K_i')$ for $i \in \{1, \ldots, m-1\}$, and $\mathrm{Aut}(K_m'/K_1') \trianglelefteq \mathrm{Aut}(K_m'/K)$. Since we have $\mathrm{Aut}(K_m'/K)/\mathrm{Aut}(K_m'/K_1') \cong \mathrm{Aut}(K(\zeta)/K)$ and $\mathrm{Aut}(K_m'/K_i')/\mathrm{Aut}(K_m'/K_{i+1}') \cong \mathrm{Aut}(K_{i+1}'/K_i')$, this is a subnormal series with abelian sections, hence $\mathrm{Aut}(L(\zeta)/K)$ is soluble. We have

$\mathrm{Aut}(L(\zeta)/L) \trianglelefteq \mathrm{Aut}(L(\zeta)/K)$ and $\mathrm{Aut}(L(\zeta)/K)/\mathrm{Aut}(L(\zeta)/L) \cong \mathrm{Aut}(L/K)$, hence $\mathrm{Aut}(L/K)$ is soluble.

b) Let $\{1\} = G_m \leq G_{m-1} \leq \cdots \leq G_1 := \mathrm{Aut}(L/K)$ be a subnormal series with cyclic sections of prime order. Letting $K_i := \mathrm{Fix}_L(G_i)$ for $i \in \{1, \ldots, m\}$, we have $K = K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L$. Since $G_{i+1} \trianglelefteq G_i$ for $i \in \{1, \ldots, m-1\}$, the field extension K_{i+1}/K_i is Galois such that $\mathrm{Aut}(K_{i+1}/K_i) \cong \mathrm{Aut}(K_m/K_i)/\mathrm{Aut}(K_m/K_{i+1}) \cong G_i/G_{i+1} \cong \mathbb{Z}/p_i\mathbb{Z}$ is cyclic of prime order.

Hence we have $n \in \mathrm{lcm}\{p_1, \ldots, p_{m-1}\}$, and let $\zeta \in M$ be a primitive n-th root of unity. Letting $K_i' := K_i(\zeta)$ for $i \in \{1, \ldots, m\}$ yields $K \subseteq K(\zeta) = K_1' \subseteq K_2' \subseteq \cdots \subseteq K_m' = L(\zeta) = M$, where since L/K is Galois, $L(\zeta)/K$ is Galois. Since K_{i+1}/K_i is Galois, K_{i+1}'/K_i and K_{i+1}'/K_i' are Galois for $i \in \{1, \ldots, m-1\}$, and we have the restriction map $\mathrm{res}_{K_{i+1}}^{K_{i+1}'}\colon \mathrm{Aut}(K_{i+1}'/K_i) \to \mathrm{Aut}(K_{i+1}/K_i)$. If $\varphi \in \mathrm{Aut}(K_{i+1}'/K_i') \leq \mathrm{Aut}(K_{i+1}'/K_i)$ such that $\varphi \in \ker(\mathrm{res}_{K_{i+1}}^{K_{i+1}'})$, then $a^\varphi = a$ for all $a \in K_i' \cup K_{i+1}$ implies $\varphi = \mathrm{id}_{K_{i+1}'}$. Hence $\mathrm{res}_{K_{i+1}}^{K_{i+1}'}\colon \mathrm{Aut}(K_{i+1}'/K_i') \to \mathrm{Aut}(K_{i+1}/K_i)$ is injective, thus $\mathrm{Aut}(K_{i+1}'/K_i') \cong \mathbb{Z}/n_i\mathbb{Z}$, where $n_i \mid p_i$. Hence $X^{n_i} - 1 = \prod_{k \in \mathbb{Z}/n_i\mathbb{Z}}(X - (\zeta^{\frac{n}{n_i}})^k) \in K_i'[X]$ splits, thus K_{i+1}'/K_i' is a Kummer extension. Since $K(\zeta)/K$ is a radical extension, $L(\zeta)/K$ is as well. ♯

(7.9) Corollary. Let L/K be a splitting field for $f \in K[X] \setminus K$ separable.
a) If f is **solvable by radicals**, i. e. there is a separable radical extension M/K such that f splits in $M[X]$, then $\mathrm{Aut}(L/K)$ is soluble.
b) If $\mathrm{char}(K) \nmid [L\colon K]$ and $\mathrm{Aut}(L/K)$ is soluble then f is solvable by radicals.

Proof. a) There is a Galois radical extension M/K such that f splits in $M[X]$, where $\mathrm{Aut}(M/K)$ is soluble. There is a splitting field L/K for f such that $L \subseteq M$, hence $\mathrm{Aut}(L/K) \cong \mathrm{Aut}(M/K)/\mathrm{Aut}(M/L)$ is soluble.
b) There is a Galois radical extension M/K such that $L \subseteq M$. ♯

(7.10) Symmetric polynomials. a) Let K be a field, let $n \in \mathbb{N}$, and let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be commuting indeterminates. Then $f := \prod_{j=1}^n (X - X_j) = X^n + \sum_{k=1}^n (-1)^k S_{n,k} X^{n-k} \in K(\mathcal{X})[X]$, where the **elementary symmetric polynomials** are $S_{n,k} := \sum_{1 \leq i_1 < i_2 < \cdots i_k \leq n} \prod_{j=1}^k X_{i_j} \in K[\mathcal{X}]$; we have $S_{n,1} = X_1 + \cdots + X_n$ and $S_{n,n} = X_1 \cdot \cdots \cdot X_n$. Letting $\mathcal{S} := \{S_{n,1}, \ldots, S_{n,n}\}$ we conclude that $K(\mathcal{X})/K(\mathcal{S})$ is a splitting field for f, hence $[K(\mathcal{X})\colon K(\mathcal{S})] \leq \deg(f)! = n!$.

For $\pi \in \mathcal{S}_n$ the evaluation map $\pi\colon K[\mathcal{X}] \to K[\mathcal{X}]\colon X_i \mapsto X_{i\pi}$ is a ring automorphism, hence extends uniquely to a field automorphism of $K(\mathcal{X})$. Hence $\mathcal{S}_n$ acts on $K(\mathcal{X})$, yielding an injective action homomorphism $\mathcal{S}_n \to \mathrm{Aut}(K(\mathcal{X}))$. For $\pi \in \mathcal{S}_n$ we have $f^\pi = \prod_{j=1}^n (X - X_j^\pi) = \prod_{j=1}^n (X - X_j) = f \in K(\mathcal{X})[X]$, thus $S_{n,k}^\pi = S_{n,k}$ for all $k \in \{1, \ldots, n\}$, hence $K(\mathcal{S}) \subseteq M := \mathrm{Fix}_{K(\mathcal{X})}(\mathcal{S}_n)$. Since $K(\mathcal{X})/K(\mathcal{S})$ is finite, $K(\mathcal{X})/M$ is Galois such that $\mathrm{Aut}(K(\mathcal{X})/M) \cong \mathcal{S}_n$, and from $[K(\mathcal{X})\colon M] = |\mathcal{S}_n| = n!$ we conclude $M = K(\mathcal{S})$.

For $G \leq \mathcal{S}_n$ we have $G \cong \mathrm{Aut}(K(\mathcal{X})/\mathrm{Fix}_{K(\mathcal{X})}(G)) \leq \mathrm{Aut}(K(\mathcal{X})/K(\mathcal{S})) \cong \mathcal{S}_n$. Since any finite group is isomorphic to a subgroup of some symmetric group, any finite group can be realised as a Galois group of a suitable Galois extension.

b) The set $\mathcal{S}$ is **algebraically independent** over K, i. e. if $\mathcal{Z} := \{Z_1, \ldots, Z_n\}$ are commuting indeterminates, the evaluation map $K[\mathcal{Z}] \to K[\mathcal{X}]\colon Z_k \mapsto S_{n,k}$ is injective: Let $\mathcal{Y} := \{Y_1, \ldots, Y_n\}$ be commuting indeterminates and $g := X^n + \sum_{k=1}^n (-1)^k Y_k X^{n-k} \in K(\mathcal{Y})[X]$ be the **general polynomial** of degree n. Let $L/K(\mathcal{Y})$ be a splitting field for g, hence we have $g = \prod_{j=1}^n (X - y_j) \in L[X]$, and the evaluation map $K[\mathcal{X}] \to L\colon X_j \mapsto y_j$ implies $Y_k = S_{n,k}(y_1, \ldots, y_n)$ for $k \in \{1, \ldots, n\}$. Thus for $h \in K[\mathcal{Z}]$ such that $h(S_{n,1}, \ldots, S_{n,n}) = 0 \in K[\mathcal{X}]$ we get $0 = h(S_{n,1}(y_1, \ldots, y_n), \ldots, S_{n,n}(y_1, \ldots, y_n)) = h(Y_1, \ldots, Y_n) \in L$, and since $\mathcal{Y}$ is algebraically independent over K we infer $h = 0$.

Since $\mathcal{S}$ is algebraically independent, the evaluation map $K[\mathcal{Y}] \to K[\mathcal{S}]\colon Y_k \mapsto S_{n,k}$ is a ring isomorphism, which hence extends uniquely to a field isomorphism $K(\mathcal{Y}) \to K(\mathcal{S})$, and thus to a ring isomorphism $K(\mathcal{Y})[X] \to K(\mathcal{S})[X]$ such that $g = X^n + \sum_{k=1}^n (-1)^k Y_k X^{n-k} \mapsto X^n + \sum_{k=1}^n (-1)^k S_{n,k} X^{n-k} = f$. Hence this extends to an isomorphism $\varphi\colon L \to K(\mathcal{X})$ of the respective splitting fields, inducing a bijection between the roots $\{y_1, \ldots, y_n\}$ of g in L and $\{X_1, \ldots, X_n\}$ of f in $K(\mathcal{X})$, and implying that $\mathrm{Aut}(K(\mathcal{X})/K(\mathcal{S})) \to \mathrm{Aut}(L/K(\mathcal{Y}))\colon \pi \mapsto \varphi\pi\varphi^{-1}$ is a group isomorphism. Hence we have $\mathrm{Aut}(L/K(\mathcal{Y})) \cong \mathcal{S}_n$, where the action of $\mathcal{S}_n$ is given by permutations of $\{y_1, \ldots, y_n\}$.

Hence we have **Abel's Theorem**: For $n \geq 5$ the general polynomial of degree n is not solvable by radicals. If $n = 2$ and $\mathrm{char}(K) \neq 2$, or $n \in \{3, 4\}$ and $\mathrm{char}(K) \notin \{2, 3\}$, the general polynomial of degree n is solvable by radicals.

(7.11) Cardano's Formula. a) Let K be a field such that $\mathrm{char}(K) \neq 2$, and let $g := X^2 + PX + Q \in M[X]$, where $M := K(P, Q)$. From $g = (X - X_1)(X - X_2) \in K(\mathcal{X})[X]$, where $\mathcal{X} := \{X_1, X_2\}$, we get $P = -(X_1 + X_2)$ and $Q = X_1 X_2$. We have $\mathrm{Aut}(K(\mathcal{X})/M) \cong \mathcal{S}_2 = \langle (1,2) \rangle$, thus the Lagrange resolvent associated to $(1,2)$ maps X_1 to the **discriminant** $\Delta := X_1 - X_2$. Hence we have $\Delta^2 \in M$ and thus $K(\mathcal{X}) = M(X_1) = M(\Delta)$. We get $\Delta^2 = (X_1 - X_2)^2 = P^2 - 4Q$, and thus $X_i = -\frac{1}{2}(P + (-1)^i \Delta) = -\frac{P}{2} + (-1)^{i-1} \sqrt{\frac{P^2}{4} - Q}$ for $i \in \{1, 2\}$.

b) Let K be a field such that $\mathrm{char}(K) \notin \{2, 3\}$ and $X^3 - 1 = (X - 1)(X^2 + X + 1) \in K[X]$ splits, and let $\zeta \in K$ be a primitive 3-rd root of unity; hence we have $1 + \zeta + \zeta^2 = 0$. Let $g := X^3 + PX^2 + QX + R \in M[X]$, where $M := K(P, Q, R)$. From $g = (X - X_1)(X - X_2)(X - X_3) \in K(\mathcal{X})[X]$, where $\mathcal{X} := \{X_1, X_2, X_3\}$, we get $P = -(X_1 + X_2 + X_3)$ and $Q = X_1X_2 + X_1X_3 + X_2X_3$ and $R = X_1X_2X_3$. We have $\mathrm{Aut}(K(\mathcal{X})/M) \cong \mathcal{S}_3$, with subnormal series $\{1\} < \mathcal{A}_3 = \langle (1,2,3) \rangle < \mathcal{S}_3 = \langle (1,2,3), (1,2) \rangle$ having cyclic sections of order 2 and 3, respectively.

Let $\Delta := (X_1 - X_2)(X_1 - X_3)(X_2 - X_3) = X_1^2X_2 - X_1^2X_3 - X_1X_2^2 + X_1X_3^2 + X_2^2X_3 - X_2X_3^2$ be the **discriminant**. From $\Delta^{(1,2,3)} = \Delta$ and $\Delta^{(1,2)} = -\Delta$ we infer $\mathrm{Fix}_{K(\mathcal{X})}((1,2,3)) = M(\Delta)$, where $[M(\Delta)\colon M] = 2$. The Lagrange resolvent associated to $\mathcal{S}_3/\mathcal{A}_3 = \langle \overline{(1,2)} \rangle$ maps Δ to 2Δ, and we get $\Delta^2 =$

$-4P^3R + P^2Q^2 + 18PQR - 4Q^3 - 27R^2 \in M$.

The Lagrange resolvents associated to $\mathcal{A}_3 = \langle(1,2,3)\rangle = \langle(1,3,2)\rangle$ map X_1 to $\Theta := X_1 + \zeta X_2 + \zeta^2 X_3$ and $\widetilde{\Theta} := X_1 + \zeta^2 X_2 + \zeta X_3$, respectively, hence we have $\Theta^3, \widetilde{\Theta}^3 \in M(\Delta)$ and $K(\mathcal{X}) = M(\Delta, X_1) = M(\Delta, \Theta) = M(\Delta, \widetilde{\Theta})$. We get $\Theta^+ := \Theta^3 + \widetilde{\Theta}^3 = -2P^3 + 9PQ - 27R$ and $\Theta^- := \Theta^3 - \widetilde{\Theta}^3 = 3(\zeta - \zeta^2)\Delta = 3\sqrt{-3}\Delta$, hence $\Theta^3 = \frac{1}{2}(\Theta^+ + \Theta^-)$ and $\widetilde{\Theta}^3 = \frac{1}{2}(\Theta^+ - \Theta^-)$. This yields $X_i = \frac{1}{3}(-P + \zeta^{-i+1}\Theta + \zeta^{i-1}\widetilde{\Theta})$ for $i \in \{1, \ldots, 3\}$.

For simplification we let $X' := X + \frac{P}{3}$. This yields $g = (X' - \frac{P}{3})^3 + P(X' - \frac{P}{3})^2 + Q(X' - \frac{P}{3}) + R = X'^3 + Q'X' + R'$, where $Q' := Q - \frac{P^2}{3}$ and $R' := R - \frac{PQ}{3} + \frac{2P^3}{27}$. Hence we have $\Delta^2 = -4Q'^3 - 27R'^2$, and $\Theta^+ = -27R'$ and $\Theta^- = 3\sqrt{-3}\Delta$, yielding $\Theta^3 = -\frac{27}{2}R' + \frac{3}{2}\sqrt{-3}\Delta$ and $\widetilde{\Theta}^3 = -\frac{27}{2}R' - \frac{3}{2}\sqrt{-3}\Delta$, and thus

$$X_i = -\frac{P}{3} + \zeta^{-i+1} \cdot \sqrt[3]{-\frac{R'}{2} + \sqrt{\frac{Q'^3}{27} + \frac{R'^2}{4}}} + \zeta^{i-1} \cdot \sqrt[3]{-\frac{R'}{2} - \sqrt{\frac{Q'^3}{27} + \frac{R'^2}{4}}}.$$

8 Exercises (in German)

(8.1) Aufgabe: Gruppenaxiome.
Es seien G eine Menge und $\cdot\colon G \times G \to G$ eine assoziative Verknüpfung auf G. Außerdem gebe es ein **rechts-neutrales** Element $1 \in G$ mit $g \cdot 1 = g$ für alle $g \in G$, und zu jedem Element $g \in G$ gebe es ein **rechts-inverses** Element $h \in G$ mit $gh = 1$. Man zeige: G ist eine Gruppe.

(8.2) Aufgabe: Rechnen in Gruppen.
Es sei G eine Gruppe.
a) Man bestimme alle Elemente $g \in G$ mit $g^2 = g$.
b) Für alle $f, g, h \in G$ zeige man die folgenden **Kürzungsregeln**: Es ist $fh = gh$ genau dann, wenn $f = g$ ist, und dies gilt genau dann, wenn $hf = hg$ ist.
c) Man zeige: G ist genau dann abelsch, wenn $g^2h^2 = (gh)^2$ für alle $g, h \in G$.

(8.3) Aufgabe: Komplexprodukt.
Es sei G eine Gruppe. Für Teilmengen $A, B \subseteq G$ sei $A^{-1} := \{a^{-1} \in G; a \in A\}$ und das **Komplexprodukt** $AB := \{ab \in G; a \in A, b \in B\}$.
a) Man zeige: Eine Teilmenge $\emptyset \neq U \subseteq G$ ist genau dann eine Untergruppe, wenn $UU^{-1} \subseteq U$ gilt.
b) Man zeige: Eine endliche Teilmenge $\emptyset \neq U \subseteq G$ ist genau dann eine Untergruppe, wenn $UU \subseteq U$ gilt.
c) Für Untergruppen $U, V \leq G$ zeige man: Es ist UV genau dann eine Untergruppe, wenn $VU \subseteq UV$ gilt. Was folgt daraus für abelsche Gruppen?

(8.4) Aufgabe: Matrixgruppen.
Man zeige: $\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{R}^{2\times 2}; a^2 + b^2 \neq 0 \right\}$ ist eine Untergruppe von $\mathrm{GL}_2(\mathbb{R})$, die isomorph zur Einheitengruppe $\mathbb{C}^*$ ist.

(8.5) Aufgabe: Symmetrische Gruppen.
Für endliche Mengen $X, Y \neq \emptyset$ zeige man: Die symmetrischen Gruppen $\mathcal{S}_X$ und $\mathcal{S}_Y$ sind genau dann isomorph, wenn $|X| = |Y|$ gilt.

(8.6) Aufgabe: Index.
Es seien G eine Gruppe und $U, V \leq G$. Man zeige:
a) Sind $|U|$ und $|V|$ endlich mit $\mathrm{ggT}(|U|, |V|) = 1$, so gilt $U \cap V = \{1\}$.
b) Sind $U \leq V \leq G$ mit $[G\colon U]$ endlich, so sind auch $[G\colon V]$ und $[V\colon U]$ endlich, und es gilt $[G\colon U] = [G\colon V] \cdot [V\colon U]$.
c) Es gilt der **Satz von Poincaré**: Sind $[G\colon U]$ und $[G\colon V]$ endlich, so ist $[G\colon (U \cap V)]$ endlich, und es gilt $[G\colon (U \cap V)] \leq [G\colon U] \cdot [G\colon V]$. Unter welcher hinreichenden Bedingung gilt Gleichheit?

(8.7) Aufgabe: Vereinigung von Untergruppen.
Es seien G eine endliche Gruppe und $U < G$. Man zeige: Es ist $\bigcup_{g \in G} U^g \neq G$.

(8.8) Aufgabe: Tetraedergruppe.
a) Man bestimme die Symmetriegruppe eines regulären Tetraeders im Euklidischen Raum $\mathbb{R}^3$ als Gruppe von Permutationen seiner 4 Ecken. Wieviele Drehungen und Spiegelungen gibt es? Man zeige, daß die Menge der Drehungen eine Untergruppe bildet. Zu welchen bekannten Gruppen sind die volle Symmetriegruppe und die Drehgruppe isomorph?
b) Man bestimme die Anzahl der verschiedenen Färbungen der 4 Ecken eines regulären Tetraeders mit bis zu 4 Farben, bezüglich der vollen Symmetriegruppe und der Drehgruppe. Wie kann man das Ergebnis geometrisch interpretieren?

(8.9) Aufgabe: Lineare Gruppen.
Es sei K ein Körper mit $q \in \mathbb{N}$ Elementen. Für $n \in \mathbb{N}$ bestimme man die Ordnungen der linearen Gruppen $\mathrm{GL}_n(K)$ und $\mathrm{SL}_n(K)$.

(8.10) Aufgabe: Elementordnungen.
Es sei G eine endliche Gruppe. Dann heißt $\exp(G) := \mathrm{kgV}\{|g|; g \in G\} \in \mathbb{N}$ der **Exponent** von G. Man zeige:
a) Für alle $g, h \in G$ gilt $|g^{-1}| = |g|$ sowie $|gh| = |hg|$ und $|g^h| = |g|$.
b) Sind $g, h \in G$ mit $gh = hg$, so gilt genau dann $|gh| = |g| \cdot |h|$, wenn $\mathrm{ggT}(|g|, |h|) = 1$ ist. Was gilt im Falle $gh \neq hg$?
c) Ist G abelsch, so ist $\exp(G) = \max\{|g|; g \in G\}$. Gilt dies auch allgemein?
d) Ist $\exp(G) \leq 2$, so ist G abelsch.

(8.11) Aufgabe: Untergruppenverbände.
Man bestimme die Untergruppen, Normalteiler und Zentren der folgenden Gruppen, und zeichne jeweils das Hasse-Diagramm des Untergruppenverbandes:
a) Zyklische Gruppen C_n für $n \leq 12$,
b) Kleinsche Vierergruppe V_4,
c) Diedergruppen D_8, D_{10} und D_{12},
d) alternierende Gruppe $\mathcal{A}_4$.

(8.12) Aufgabe: Quaternionengruppe.
Es seien $A, B \in GL_2(\mathbb{C})$ gegeben durch

$$A := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{und} \quad B := \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},$$

sowie $Q_8 := \langle A, B \rangle \leq GL_2(\mathbb{C})$ die **Quaternionengruppe**. Man bestimme die Gruppenordnung, die Untergruppen, Normalteiler und das Zentrum von Q_8, zeichne das Hasse-Diagramm des Untergruppenverbandes, und gebe einen Monomorphismus $Q_8 \to \mathcal{S}_8$ an.

(8.13) Aufgabe: Symmetrische Gruppen.
Es seien $n \in \mathbb{N}$ und $\mathcal{S}_n$ die zugehörige symmetrische Gruppe. Ist $\pi \in \mathcal{S}_n$ ein Produkt von $r \in \mathbb{N}$ disjunkten Zykeln der Längen $n_1 \geq n_2 \geq \cdots \geq n_r > 0$, so heißt die nicht-aufsteigende Folge $[n_1, \ldots, n_r]$ der **Zykeltyp** von π.

a) Für $\pi \in \mathcal{S}_n$ zeige man $(1, \ldots, n)^\pi = (1\pi, \ldots, n\pi) \in \mathcal{S}_n$. Daraus folgere man: Elemente $\pi, \pi' \in \mathcal{S}_n$ sind genau dann konjugiert, wenn sie den gleichen Zykeltyp besitzen. Man bestimme die Konjugiertenklassen in $\mathcal{S}_n$ für $n \in \{3, 4, 5\}$.
b) Man gebe eine Transversale für $\mathrm{Stab}_{\mathcal{S}_n}(n)$ in $\mathcal{S}_n$ an. Zu welcher bekannten Gruppe ist $\mathrm{Stab}_{\mathcal{S}_n}(n)$ isomorph? Daraus folgere man: Es gilt $\mathcal{S}_n = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle = \langle (1,2), (1,2,\ldots,n) \rangle$.

(8.14) Aufgabe: Frattini-Argument.
Es seien $p \in \mathbb{N}$ prim und G eine endliche Gruppe.
a) Es seien $P \in \mathrm{Syl}_p(G)$ und $N_G(P) \leq U \leq G$. Man zeige: Es ist $N_G(U) = U$.
b) Es seien $N \trianglelefteq G$ und $P \in \mathrm{Syl}_p(N)$. Man zeige: Es ist $N_G(P)N = G$.

(8.15) Aufgabe: Gruppenordnungen mit wenigen Primteilern.
Es seien $p \neq q \in \mathbb{N}$ prim und G eine endliche Gruppe. Man zeige:
a) Ist $|G| = pq$ mit $p < q$, so hat G eine normale q-Sylow-Gruppe; ist zudem $q \not\equiv 1 \pmod{p}$, so ist G zyklisch. Gilt dies auch im Falle $q \equiv 1 \pmod{p}$?
b) Ist $|G| = 2p$, so ist $G \cong C_{2p}$ oder $G \cong D_{2p}$.
c) Ist $|G| = p^2q$, so hat G einen nicht-trivialen echten Normalteiler.
d) Ist $|G| = 8k$, wobei $k \leq 8$, so hat G einen nicht-trivialen echten Normalteiler.

(8.16) Aufgabe: Zentrum.
Es seien $p \in \mathbb{N}$ prim und G eine Gruppe.
a) Man zeige: Ist $G/Z(G)$ zyklisch, so ist G abelsch.
b) Man bestimme alle Gruppen G der Ordnung $|G| = p^2$.
c) Man zeige: Ist $|G| = p^3$, so ist G abelsch oder $|Z(G)| = p$.

(8.17) Aufgabe: Gruppen kleiner Ordnung.
Man bestimme bis auf Isomorphie
a) die nicht-abelschen Gruppen G der Ordnung $|G| = 8$,
b) die Gruppen G der Ordnung $|G| = 12$,
c) die Gruppen G der Ordnung $|G| = 21$.

(8.18) Aufgabe: Zyklische Gruppen.
Es sei $n \in \mathbb{N}$. Man zeige: Es ist $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(8.19) Aufgabe: Satz von Wilson.
Es sei $p \in \mathbb{N}$ prim. Man zeige man: Es gilt $(p-1)! \equiv -1 \pmod{p}$.

(8.20) Aufgabe: Quaternionen-Schiefkörper.
Für $u, v \in \mathbb{C}$ sei $Q_{u,v} := \begin{bmatrix} u & v \\ -\overline{v} & \overline{u} \end{bmatrix} \in \mathbb{C}^{2\times 2}$, wobei $\overline{\ }: \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation bezeichne.
a) Man zeige: $\mathbb{H} := \{Q_{u,v} \in \mathbb{C}^{2\times 2}; u, v \in \mathbb{C}\}$ ist ein Teilring von $\mathbb{C}^{2\times 2}$ und ein nicht-kommutativer Schiefkörper; $\mathbb{H}$ heißt der Schiefkörper der **Hamilton-Quaternionen**. Für $[0,0] \neq [u,v] \in \mathbb{C}^2$ gilt $Q_{u,v}^{-1} = \frac{1}{|u|^2+|v|^2} \cdot Q_{\overline{u},-v}$.

b) Es seien $I := Q_{\sqrt{-1},0}$ und $J := Q_{0,1}$ sowie $K := Q_{0,\sqrt{-1}}$ die **Pauli-Matrizen**. Man zeige: Jedes Element $Q \in \mathbb{H}$ hat eine eindeutige Darstellung der Form $Q = aE_2 + bI + cJ + dK \in \mathbb{H}$, wobei $a, b, c, d \in \mathbb{R}$, und es gilt $I^2 = J^2 = K^2 = -1$ und $IJ = -JI = K$ sowie $JK = -KJ = I$ und $KI = -IK = J$.
c) Man zeige: $Z := \{aE_2 + bI + cJ + dK \in \mathbb{H}; a, b, c, d \in \mathbb{Z}\}$ ist ein Teilring von $\mathbb{H}$. Zu welcher bekannten Gruppe ist die Einheitengruppe Z^* isomorph?

(8.21) Aufgabe: Matrixringe.
Es seien K ein Körper und $n \in \mathbb{N}$. Man zeige: Der Ring $K^{n\times n}$ ist einfach, aber kein Schiefkörper, und jedes von 0 verschiedene Element ist entweder eine Einheit oder ein Nullteiler.

(8.22) Aufgabe: Integritätsringe.
Man zeige: In einem endlichen kommutativen Ring ist jedes von 0 verschiedene Element entweder eine Einheit oder ein Nullteiler. Ein endlicher Integritätsring ist ein Körper.

(8.23) Aufgabe: Teilbarkeit.
Es seien R ein Integritätsring und $K := \mathcal{Q}(R)$ sein Quotientenkörper.
a) Man zeige: Sind $p \in R$ prim und $a \in R$, so gilt entweder $p \mid a$ oder $1 \in \mathrm{ggT}(a, p)$. Sind $p, q \in R$ prim, so gilt entweder $p \sim q$ oder $1 \in \mathrm{ggT}(p, q)$.
b) Man gebe eine formale Definition von **kleinsten gemeinsamen Vielfachen** zweier Elemente vom R an, und formuliere eine Eindeutigkeitsaussage. Man zeige: Ist R faktoriell, so gibt es kleinste gemeinsame Vielfache. Wie kann man eines berechnen? Wie kann man eines in Hauptidealringen berechnen?
c) Es sei R faktoriell. Man zeige: Sind $0 \neq a, b \in R$ teilerfremd und $c \in R$, so gilt $a \mid bc$ genau dann, wenn $a \mid c$, und aus $a \mid c$ und $b \mid c$ folgt $ab \mid c$. Ist $c \in K$, so gibt es bis auf Assoziiertheit eindeutig bestimmte teilerfremde Elemente $a \in R$ und $0 \neq b \in R$ mit $c = \frac{a}{b} \in K$.

(8.24) Aufgabe: Quadratische Ringe.
Für $n \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei sei $R := \mathbb{Z}[\sqrt{n}] := \{x + y\sqrt{n} \in \mathbb{C}; x, y \in \mathbb{Z}\}$.
a) Man bestimme R^* für $n < 0$, und zeige, daß $\mathbb{Z}[\sqrt{3}]^*$ unendlich ist.
b) Man faktorisiere 2, 3 und 5 in $\mathbb{Z}[\sqrt{-1}]$.
c) Man bestimme alle Teiler von 21 in $\mathbb{Z}[\sqrt{-5}]$.
d) Man zeige: $\langle 3, 2+\sqrt{-5}\rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}]$ und $\langle 3, 2-\sqrt{-5}\rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}]$ sind Primideale, und es gilt $\langle 3, 2 + \sqrt{-5}\rangle\langle 3, 2 - \sqrt{-5}\rangle = \langle 3\rangle \trianglelefteq \mathbb{Z}[\sqrt{-5}]$.

(8.25) Aufgabe: Größte gemeinsame Teiler.
a) Man bestimme jeweils einen größten gemeinsamen Teiler von $a, b \in R$ und zugehörige Bézout-Koeffizienten:
i) $R := \mathbb{Z}$, $a := 1256$, $b := 14372$.
ii) $R := \mathbb{Z}[\sqrt{-1}]$, $a := 2 + \sqrt{-1}$, $b := 2 - \sqrt{-1}$.
iii) $R := \mathbb{Z}[\sqrt{-1}]$, $a := 5 + 3 \cdot \sqrt{-1}$, $b := 13 + 8 \cdot \sqrt{-1}$.
iv) $R := \mathbb{Q}[X]$, $a := X^5 + X^4 - X^3 - 3X^2 - 3X - 1$, $b := X^4 - 2X^3 - X^2 - 2X - 1$.

v) $R := \mathbb{Q}[X]$, $a := X^3 - 6X^2 + X + 4$, $b := X^5 - 6X + 1$.

b) Für $a, b \in \mathbb{N}_0$ sei $\mathrm{ggT}_+(a,b) \in \mathbb{N}_0$ der **nichtnegative** größte gemeinsame Teiler. Für $k, m, n \in \mathbb{N}$ zeige man: Es gilt $\mathrm{ggT}_+(k^m - 1, k^n - 1) = k^{\mathrm{ggT}_+(m,n)} - 1$.

(8.26) Aufgabe: Polynomringe.
a) Man zeige: Das Ideal $\langle 2, X \rangle \trianglelefteq \mathbb{Z}[X]$ ist kein Hauptideal.
b) Man zeige: Für einen kommutativen Ring R sind äquivalent:
i) Der Polynomring $R[X]$ ist ein Euklidischer Ring.
ii) Der Polynomring $R[X]$ ist ein Hauptidealring.
iii) Der Ring R ist ein Körper.

(8.27) Aufgabe: Multivariate Polynome.
Es seien R ein kommutativer Ring und $n \in \mathbb{N}$. Man zeige:
a) Für $\pi \in \mathcal{S}_n$ gilt $R[X_{1\pi}, \ldots, X_{n\pi}] \cong R[X_1, \ldots, X_n]$, und für $n \geq 2$ gilt $R[X_1, \ldots, X_n] \cong R[X_1, \ldots, X_{n-1}][X_n]$.
b) Ist R faktoriell, so ist $R[X_1, \ldots, X_n]$ ebenfalls faktoriell.
c) Für $n \geq 2$ ist $X_1^2 + X_2^2 + \cdots + X_n^2 - 1 \in \mathbb{Z}[X_1, \ldots, X_n]$ irreduzibel.

(8.28) Aufgabe: Lagrange-Interpolation.
Es seien K ein unendlicher Körper, $n \in \mathbb{N}$, sowie $a_1, \ldots, a_n \in K$ paarweise verschieden, $b_1, \ldots, b_n \in K$ und $f := \sum_{i=1}^{n} (b_i \cdot \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}) \in K[X]$. Man zeige: Es ist $f \in K[X]$ das eindeutig bestimmte **Interpolationspolynom** mit $f(a_i) = b_i$ für $i \in \{1, \ldots, n\}$, wobei $f = 0$ oder $\mathrm{Grad}(f) < n$.

(8.29) Aufgabe: Irreduzibilität.
Man zeige: Das Polynom $X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$ ist irreduzibel in $\mathbb{Q}[X]$, aber reduzibel in $\mathbb{F}_p[X]$ für alle $p \in \mathbb{N}$ prim.

Hinweis. Für $p \neq 2$ ist $\mathbb{F}_p^{*2} := \{x^2 \in \mathbb{F}_p^*; x \in \mathbb{F}_p^*\} \leq \mathbb{F}_p^*$ eine Untergruppe vom Index 2. Daraus folgere man für $p > 3$, daß $\{2, 3, 6\} \cap \mathbb{F}_p^{*2} \neq \emptyset$ gilt.

(8.30) Aufgabe: Kronecker-Faktorisierung in $\mathbb{Z}[X]$.
Es sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ primitiv mit $\mathrm{Grad}(f) = n \in \mathbb{N}$.
a) Es sei $g = \sum_{i=0}^{m} b_i X^i \in \mathbb{Z}[X]$ primitiv mit $\mathrm{Grad}(g) = m \in \mathbb{N}$. Man zeige: Es gilt $g \mid f \in \mathbb{Z}[X]$ genau dann, wenn $g \mid f \in \mathbb{Q}[X]$ gilt. In diesem Falle ist $b_m \mid a_n \in \mathbb{Z}$ und $b_0 \mid a_0 \in \mathbb{Z}$, sowie $g(a) \mid f(a) \in \mathbb{Z}$ für alle $a \in \mathbb{Z}$.
b) Wie kann man alle linearen Teiler von f bestimmen? Wie kann man mittels Lagrange-Interpolation, siehe (8.28), alle Teiler des Grades m bestimmen? Wieso reicht es aus, $m \in \{2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ zu betrachten?
c) Man faktorisiere $X^5 + 2X^4 + 5X^3 + 6X^2 + 5X + 6 \in \mathbb{Z}[X]$.

(8.31) Aufgabe: Faktorisierung in $\mathbb{Z}[X]$.
Man faktorisiere die folgenden Polynome in $\mathbb{Z}[X]$:

a) X^3+39X^2-4X+8 **b)** $X^4+11X^3+34X^2+46X+232$ **c)** X^4+1
d) X^4-10X^2+1 **e)** $12X^4-4X^3+6X^2+X-1$ **f)** X^4-X^2+1
g) $X^5-2X^4+6X+10$ **h)** $X^7+21X^5+35X^2+34X-8$ **i)** X^9-1
j) $18X^9+3X^8-15X^7+66X^6+12X^5-60X^4+48X^3+12X^2-60X-24$

(8.32) Aufgabe: Körpererweiterungen.
Es seien L/K eine Körpererweiterung und $a, b \in L$. Man zeige:
a) Ist $[L\colon K] \in \mathbb{N}$ prim, so ist $a \in L$ genau dann primitiv, wenn $a \notin K$ ist.
b) Sind die Grade $[K(a)\colon K]$ und $[K(b)\colon K]$ endlich und teilerfremd, so gilt $[K(a,b)\colon K] = [K(a)\colon K] \cdot [K(b)\colon K]$.
c) Ist b transzendent über K und algebraisch über $K(a)$, so ist a transzendent über K und algebraisch über $K(b)$.
d) Ist $a \neq 0$, so ist a genau dann algebraisch über K, wenn $a^{-1} \in K[a] \subseteq L$ ist. Die Körpererweiterung L/K ist genau dann algebraisch, wenn jeder Teilring $K \subseteq R \subseteq L$ ein Körper ist.

(8.33) Aufgabe: Transzendente Körpererweiterungen.
Es sei K ein Körper. Man zeige:
a) Ist $f \in K(X)$ algebraisch über K, so ist $f \in K$.
b) Für $n \geq 2$ ist $K(X^n) \subset K(X)$ und $K(X^n) \cong K(X)$.
c) Die Körpererweiterung $K(X)/K$ besitzt unendlich viele Zwischenkörper.

(8.34) Aufgabe: Algebraische Körpererweiterungen.
Es sei $K := \mathbb{Q}(\{\sqrt[n]{2}; n \in \mathbb{N}\}) \subseteq \mathbb{C}$. Man zeige: Es ist $K/\mathbb{Q}$ eine unendliche algebraische Körpererweiterung.

(8.35) Aufgabe: Kubische Zahlkörper.
Es sei $a \in \mathbb{C}$ eine Nullstelle von $f := X^3 - 6X^2 + 9X + 3 \in \mathbb{Q}[X]$. Man zeige: Es ist $\{1, a, a^2\} \subseteq \mathbb{Q}(a)$ eine $\mathbb{Q}$-Basis. Man schreibe die Elemente a^5 und $3a^4 - 2a^3 + 1$ und $(a+2)^{-1}$ von $\mathbb{Q}(a)$ als $\mathbb{Q}$-Linearkombinationen in $\{1, a, a^2\}$.

(8.36) Aufgabe: Biquadratische Zahlkörper.
Es sei $K := \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{C}$. Man zeige:
a) Es ist $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \subseteq K$ ist eine $\mathbb{Q}$-Basis. Für $0 \neq a = a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} \in K$, wobei $a_1, \ldots, a_4 \in \mathbb{Q}$, gebe man $a^{-1} \in K$ als $\mathbb{Q}$-Linearkombination in $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ an.
b) Es ist $\sqrt{2} + \sqrt{3} \in K$ ein primitives Element von $K/\mathbb{Q}$. Man gebe das zugehörige Minimalpolynom an.

(8.37) Aufgabe: Algebraische Zahlkörper.
Es seien $p \neq q \in \mathbb{N}$ prim und $K := \mathbb{Q}(\sqrt{p}, \sqrt[3]{q}) \subseteq \mathbb{C}$. Man zeige: Es ist $[K\colon \mathbb{Q}] = 6$. Man bestimme die Minimalpolynome von $\sqrt{p}$ und $\sqrt[3]{q}$ sowie von $\sqrt{p} \cdot \sqrt[3]{q}$ und $\sqrt{p} + \sqrt[3]{q}$ über $\mathbb{Q}$. Welche dieser Elemente sind primitiv für $K/\mathbb{Q}$?

(8.38) Aufgabe: Grad von Zerfällungskörpern.
Es seien K ein Körper, $f \in K[X] \setminus K$ und L/K ein Zerfällungskörper für f. Man zeige: Es gilt $[L\colon K] \mid \mathrm{Grad}(f)!$.

(8.39) Aufgabe: Zerfällungskörper.
Man bestimme die jeweiligen Zerfällungskörper $K \subseteq \mathbb{C}$ für die folgenden Polynome in $\mathbb{Q}[X]$ und die Körpergrade $[K\colon \mathbb{Q}]$:
a) X^4+1 **b)** X^4-2 **c)** X^4-2X^2+2 **d)** X^5-1 **e)** X^6+1

(8.40) Aufgabe: Nullstellenvielfachheiten.
Es seien K ein Körper, $f \in K[X] \setminus K$ und L/K ein Zerfällungskörper für f.
a) Es seien $\mathrm{char}(K) = 0$ und $\widetilde{f} \in \mathrm{ggT}(f, \frac{\partial f}{\partial X}) \in K[X]$. Man zeige: Das Polynom $\frac{f}{\widetilde{f}} \in K[X]$ hat als Nullstellen in L genau die Nullstellen von f, und diese sind alle einfach. Welche Bedeutung hat dies für das Faktorisierungsproblem?
b) Es seien $\mathrm{char}(K) = p > 0$ und $f \in K[X]$ irreduzibel. Man zeige: Alle Nullstellen von f in L haben die gleiche Vielfachheit.
c) Es seien $n \in \mathbb{N}$ und $f := X^n - 1 \in K[X]$. Man gebe ein hinreichendes und notwendiges Kriterium an n dafür an, daß f in L nur einfache Nullstellen hat.

(8.41) Aufgabe: Separabilität.
Es seien L/K eine algebraische Körpererweiterung mit $\mathrm{char}(K) = p > 0$, und $a \in L$. Man zeige:
a) Es ist genau dann $a \in L$ separabel über K, wenn $K(a) = K(a^p)$ gilt.
b) Es gibt $n \in \mathbb{N}_0$, so daß $a^{p^n} \in L$ separabel über K ist.
c) Ist L/K endlich mit $p \not| [L\colon K]$, so ist L/K separabel.

(8.42) Aufgabe: Perfekte Körper.
Es sei L/K eine algebraische Körpererweiterung. Man zeige:
a) Ist K perfekt, so ist auch L perfekt.
b) Ist L perfekt und L/K separabel, so ist auch K perfekt.

(8.43) Aufgabe: Existenz primitiver Elemente.
Es seien L/K eine Körpererweiterung mit $\mathrm{char}(K) = p > 0$, sowie $a, b \in L$ mit $a^p, b^p \in K$ und $[K(a,b)\colon K] = p^2$. Man gebe ein Beispiel für diese Situation an, und zeige, daß $K(a,b)/K$ kein primitives Element besitzt.

(8.44) Aufgabe: Endliche Körper.
Es seien $p \in \mathbb{N}$ prim und $n \in \mathbb{N}$.
a) Es sei $\widehat{\ }\colon \mathbb{F}_{p^n}[X] \to \mathrm{Abb}(\mathbb{F}_{p^n}, \mathbb{F}_{p^n})$ der Homomorphismus, der jedes Polynom auf die zugehörige Polynomabbildung abbildet. Man bestimme $\mathrm{Kern}(\widehat{\ })$.
b) Für $f \in \mathbb{F}_p[X]$ irreduzibel zeige man: Es gilt genau dann $f \mid X^{p^n} - X$, wenn $\mathrm{Grad}(f) \mid n$ gilt.

(8.45) Aufgabe: Positive Charakteristik.
Es sei K ein Körper mit $\mathrm{char}(K) = p > 0$ und Frobenius-Abbildung φ_p.
a) Man zeige: Das Polynom $f := X^p - X - a \in K[X]$ ist separabel, und f ist genau dann irreduzibel, wenn f keine Nullstelle in K hat. Hat f eine Nullstelle in K, so zerfällt f bereits. Für welche $a \in \mathbb{F}_p$ ist $f \in \mathbb{F}_p[X]$ irreduzibel?
b) Man zeige: Das Polynom $g := X^p - a \in K[X]$ ist genau dann irreduzibel, wenn g keine Nullstelle in K hat. Sind L/K eine Körpererweiterung und $b \in L$ eine Nullstelle von g, so ist genau dann $K(b) \neq K(b^p)$, wenn $[K(b)\colon K(b^p)] = p$.
c) Es sei $a \in K \setminus \mathrm{Bild}(\varphi_p)$. Für $n \in \mathbb{N}$ zeige man: $X^{p^n} - a \in K[X]$ ist irreduzibel.

(8.46) Aufgabe: Charakteristik 2.
Man zeige: $X^{2^n} + X + 1 \in \mathbb{F}_2[X]$ ist genau dann irreduzibel, wenn $n \leq 2$ ist.

(8.47) Aufgabe: Spurabbildung.
Es seien L/K eine endliche Galois-Erweiterung mit $\mathrm{char}(K) = 0$, sowie $H \leq \mathrm{Aut}(L/K)$ und $M := \mathrm{Fix}_L(H)$. Man zeige:
a) Die Spurabbildung $\mathrm{Tr}_H\colon L \to M$ ist M-linear und surjektiv.
b) Ist $\{a_1, \ldots, a_n\} \subseteq L$ eine K-Basis, so gilt $M = K(\mathrm{Tr}_H(a_1), \ldots, \mathrm{Tr}_H(a_n))$.

(8.48) Aufgabe: Galois-Korrespondenz.
Für die folgenden Körper $K \subseteq \mathbb{C}$ untersuche man, zu welcher bekannten Gruppe $\mathrm{Aut}(K/\mathbb{Q})$ isomorph ist, bestimme alle Zwischenkörper von $K/\mathbb{Q}$ und jeweils ein primitives Element, und gebe die Galois-Korrespondenz explizit an:
a) K Zerfällungskörper von $X^4 - 2 \in \mathbb{Q}[X]$
b) $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$

(8.49) Aufgabe: Galois-Gruppen von Polynomen.
Es seien K ein Körper, $f \in K[X] \setminus K$ und L/K ein Zerfällungskörper für f.
a) Man zeige: $\mathrm{Aut}(L/K)$ operiert auf der Menge $\mathcal{Z}$ der Nullstellen von f in L, und via dieser Operation ist $\mathrm{Aut}(L/K)$ isomorph zu einer Untergruppe von $\mathcal{S}_{\mathcal{Z}}$. Ist f irreduzibel, so operiert $\mathrm{Aut}(L/K)$ transitiv auf $\mathcal{Z}$.
b) Es seien K ein perfekter Körper, f irreduzibel und $\mathrm{Aut}(L/K)$ abelsch. Man zeige: Es gilt $|\mathrm{Aut}(L/K)| = \mathrm{Grad}(f)$.
c) Es sei $f \in \mathbb{Q}[X]$ irreduzibel mit $\mathrm{Grad}(f) \in \mathbb{N}$ prim, und f besitze genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$. Man zeige: Es ist $\mathrm{Aut}(L/\mathbb{Q}) \cong \mathcal{S}_{\mathrm{Grad}(f)}$.
d) Es sei $f := X^5 - kX + 1 \in \mathbb{Q}[X]$ mit $3 \leq k \in \mathbb{N}$. Man zeige: $\mathrm{Aut}(L/\mathbb{Q}) \cong \mathcal{S}_5$.

(8.50) Aufgabe: Kreisteilungspolynome.
a) Für $n, m \in \mathbb{N}$ zeige man $X^{\mathrm{ggT}_+(n,m)} - 1 \in \mathrm{gcd}(X^n - 1, X^m - 1) \subseteq \mathbb{Z}[X]$.
b) Man zeige: Es gilt $X^{\varphi(n)}\Phi_n(\frac{1}{X}) = \Phi_n(X) \in \mathbb{Q}(X)$.
c) Es sei $p \in \mathbb{N}$ prim. Man zeige: Ist $n \neq 1$ ungerade, so gilt $\Phi_{2n}(X) = \Phi_n(-X)$; ist $p \mid n$, so gilt $\Phi_{pn}(X) = \Phi_n(X^p)$; ist $p \nmid n$, so gilt $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$. Man gebe $\Phi_{p^n} \in \mathbb{Z}[X]$ explizit an.
d) Man berechne $\Phi_n \in \mathbb{Z}[X]$ für $n \in \{1, \ldots, 30\}$.

(8.51) Aufgabe: Gaußsche Summen.
Es seien $p \in \mathbb{N}$ prim und $\zeta_p := \exp(\frac{2\pi\sqrt{-1}}{p}) \in \mathbb{C}$.
a) Man zeige: Es ist $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong C_{p-1}$ zyklisch.
b) Es seien $p \geq 5$ prim und $\varphi \in \mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ ein Erzeuger, sowie $a_p := \sum_{i \in \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}} \zeta_p^{\varphi^{2i}} \in \mathbb{Q}(\zeta_p)$ und $\widetilde{a}_p := a_p^{\varphi} \in \mathbb{Q}(\zeta_p)$. Für die zugehörigen Minimalpolynome zeige man: Es gilt $\mu_{a_p} = \mu_{\widetilde{a}_p} = X^2 + X + \frac{1}{4}(1 + (-1)^{\frac{p+1}{2}} p) \in \mathbb{Q}[X]$.
c) Man zeige: Es ist $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} \cdot p}) \subseteq \mathbb{Q}(\zeta_p)$.

(8.52) Aufgabe: Kreisteilungskörper.
Für $n \in \mathbb{N}$ seien $\zeta_n := \exp(\frac{2\pi\sqrt{-1}}{n}) \in \mathbb{C}$ und $\rho_n := \zeta_n + \zeta_n^{-1} \in \mathbb{C}$.
a) Man zeige: Es gilt $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\rho_n)$. Man bestimme $[\mathbb{Q}(\rho_n) \colon \mathbb{Q}]$.
b) Man bestimme die Minimalpolynome von ρ_5 und ρ_7 über $\mathbb{Q}$. Wie kann man damit das reguläre 5-Eck konstruieren?

(8.53) Aufgabe: Winkeldreiteilung.
Für $n \in \mathbb{N}$ sei der Winkel $\alpha := \frac{2\pi}{n}$ gegeben. Man zeige: Ist $3 \nmid n$, so kann α mit Zirkel und Lineal in drei gleiche Teile geteilt werden.

(8.54) Aufgabe: Konstruktion mit Zirkel und Lineal.
In der Euklidischen Ebene $\mathbb{R}^2$ sei die Parabel $\mathcal{T}$ mit der Gleichung $Y = X^2 + X$ gegeben. Zulässige Konstruktionen seien die üblichen Konstruktionen mit Zirkel und Lineal und das Schneiden von konstruierbaren Geraden und Kreisen mit $\mathcal{T}$. Man zeige: Ist $\sqrt[n]{2} \in \mathbb{R}$ mit diesen Mitteln konstruierbar, so ist $n = 2^a 3^b$, wobei $a, b \in \mathbb{N}$. Man gebe eine Konstruktion für $\sqrt[3]{2} \in \mathbb{R}$ explizit an.

(8.55) Aufgabe: Algebraischer Abschluß.
Es seien L/K eine Körpererweiterung mit L algebraisch abgeschlossen, und $\overline{K} \subseteq L$ der algebraische Abschluß von K in L. Man zeige: L ist unendlich, und ist K endlich, so sind alle Elemente von $(\overline{K})^*$ Einheitswurzeln.

(8.56) Aufgabe: Kummer-Erweiterungen.
a) Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper für das Polynom $X^3 - 10 \in \mathbb{Q}[X]$. Für $K \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{-3})\}$ zeige man $K \subseteq L$ und bestimme $\mathrm{Aut}(L/K)$.
b) Es sei $L \subseteq \mathbb{C}$ der Zerfällungskörper für das Polynom $X^4 - 5 \in \mathbb{Q}[X]$. Für $K \in \{\mathbb{Q}, \mathbb{Q}(\sqrt{5}, \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-1})\}$ zeige man $K \subseteq L$ und bestimme $\mathrm{Aut}(L/K)$.
c) Es seien Y eine Unbestimmte über $\mathbb{C}$ und $M/\mathbb{C}(Y)$ ein Zerfällungskörper für $X^n - Y \in \mathbb{C}(Y)[X]$, wobei $n \in \mathbb{N}$. Man bestimme $\mathrm{Aut}(M/\mathbb{C}(Y))$.
d) Es seien Y eine Unbestimmte über $\mathbb{F}_2$ und $M/\mathbb{F}_2(Y)$ ein Zerfällungskörper für $X^2 + Y \in \mathbb{F}_2(Y)[X]$. Man bestimme $\mathrm{Aut}(M/\mathbb{F}_2(Y))$. Ist $M/\mathbb{F}_2(Y)$ Galoissch?

(8.57) Aufgabe: Radikalerweiterungen.
Für $n \leq 10$ seien $\zeta_n := \exp(\frac{2\pi\sqrt{-1}}{n}) \in \mathbb{C}$ und $K_n := \mathbb{Q}(\zeta_n)$. Man untersuche, zu welcher bekannten Gruppe $\mathrm{Aut}(K_n/\mathbb{Q})$ isomorph ist, bestimme alle

Zwischenkörper und jeweils ein primitives Element, und gebe die Galois-Korrespondenz explizit an. Welche Zwischenkörper sind Radikalerweiterungen von $\mathbb{Q}$?

(8.58) Aufgabe: Auflösbarkeit durch Radikale.
Es seien Y eine Unbestimmte über $\mathbb{F}_2$, und $L/\mathbb{F}_2(Y)$ ein Zerfällungskörper für $f := X^2 + X + Y \in \mathbb{F}_2(Y)[X]$. Man zeige: f ist separabel, $\mathrm{Aut}(L/\mathbb{F}_2(Y))$ ist auflösbar, aber f ist über $\mathbb{F}_2(Y)$ nicht durch Radikale lösbar.

9 References

[1] B. Huppert: Endliche Gruppen I, Nachdruck, Die Grundlehren der Mathematischen Wissenschaften 134, Springer, 1983.

[2] N. Jacobson: Basic algebra I, second edition, Freeman, 1985.

[3] N. Jacobson: Basic algebra II, second edition, Freeman, 1989.

[4] S. Lang: Algebra, revised third edition, Graduate Texts in Mathematics 211, Springer, 2002.

[5] K. Meyberg: Algebra, Teil 1, 2. Aufl., Hanser, 1980.

[6] K. Meyberg: Algebra, Teil 2, 1. Aufl., Hanser, 1976.

[7] K. Meyberg, P. Vachenauer: Aufgaben und Lösungen zur Algebra, Hanser, 1978.

[8] B. van der Waerden: Algebra I, based in part on lectures by E. Artin and E. Noether, translated from the seventh German edition, Springer, 1991.

[9] B. van der Waerden: Algebra II, based in part on lectures by E. Artin and E. Noether, translated from the fifth German edition, Springer, 1991.