Introductory algebra

Friedrich-Schiller-Universität Jena, SS 2016

Jürgen Müller

Contents

1 Groups

(1.1) Groups. a) A set G together with a **multiplication** $\cdot\colon G \times G \to G$ fulfilling the following conditions is called a **group**: **i)** We have **associativity** $(fg)h = f(gh)$ for all $f, g, h \in G$; **ii)** there is a **right neutral element** $1 \in G$ such that $g \cdot 1 = g$ for all $g \in G$; and **iii)** for any $g \in G$ there is a **right inverse** $g^{-1} \in G$ such that $g \cdot g^{-1} = 1$. If additionally $gh = hg$ holds for all $g, h \in G$, then G is called **commutative** or **abelian**.

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 abelian 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 $g^{n+1} := g^n g$, and $g^{-n} := (g^{-1})^n$; then by the statements to be shown below we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ and $g^{-n} = (g^n)^{-1}$, for all $m, n \in \mathbb{Z}$. If $g, h \in G$ **commute**, that is we have $gh = hg$, then we have $(gh)^n = g^n h^n = h^n g^n$ for all $n \in \mathbb{Z}$. If G is finite, then its cardinality is called the **order** of G.

b) We collect a few immediate consequences: In particular, we have $G \neq \emptyset$.

We show that the right neutral element is left neutral as well, and that right inverses are left inverses as well: To do so, we first observe that $gg = g$ if and only if $g = 1$: From $gg = g$ we get $g = g \cdot 1 = g(gg^{-1}) = (gg)g^{-1} = gg^{-1} = 1$, and for $g = 1$ we have $1 \cdot 1 = 1$; in particular $1^{-1} = 1$. Now, from $(g^{-1}g)(g^{-1}g) = g^{-1}(gg^{-1})g = (g^{-1} \cdot 1)g = g^{-1}g$ we infer $g^{-1}g = 1$, and we get $g = g \cdot 1 = g(g^{-1}g) = (gg^{-1})g = 1 \cdot g$.

From this we infer that the **neutral** element is uniquely defined: If $1' \in G$ also is a neutral element, then we have $1 = 1 \cdot 1' = 1'$. Moreover, **inverses** are uniquely defined: If $g' \in G$ also is an inverse of $g \in G$, then we have $g' = 1 \cdot g' = (g^{-1}g)g' = g^{-1}(gg') = g^{-1} \cdot 1 = g^{-1}$.

We show the **cancellation law**: For $f, g, h \in G$ we have $f = g$ if and only if $fh = gh$, which holds if and only if $hf = hg$: From $fh = gh$ we deduce $f = f \cdot 1 = f(hh^{-1}) = (fh)h^{-1}) = (gh)h^{-1} = g(hh^{-1}) = g \cdot 1 = g$, and from $hf = hg$ we deduce $f = 1 \cdot f = (h^{-1}h)f = h^{-1}(hf) = h^{-1}(hg) = (h^{-1}h)g = 1 \cdot g = g$.

c) A subset $\emptyset \neq H \subseteq G$ is called a **subgroup**, if whenever $g, h \in H$ then we have $gh^{-1} \in H$ as well. Then, assuming that $g, h \in H$, we first get $1 = gg^{-1} \in H$, and from this $g^{-1} = 1 \cdot g^{-1} \in H$, and $gh = g(h^{-1})^{-1} \in H$. Thus H is closed with respect to taking products and inverses, hence again is a group, and we write $H \leq G$; for example, we always have the **trivial subgroup** $\{1\}$ and G itself as subgroups of G.

(1.2) Symmetric groups. a) Let X be a set, and let $\mathcal{S}_X := \{\pi\colon X \to X; \pi \text{ bijective}\}$. Now the composition of maps is associative, that is we have $(f(gh))(x) = f(g(h(x))) = ((fg)h)(x)$ for all $x \in X$, in other words $(fg)h = f(gh)$ for all maps $f, g, h\colon X \to X$; we have $\mathrm{id}_X \in \mathcal{S}_X$, and for all $\pi, \rho \in \mathcal{S}_X$ we have $\pi\rho \in \mathcal{S}_X$ and $\pi^{-1} \in \mathcal{S}_X$, where the latter is the inverse map of π; and we have $\pi \cdot \mathrm{id}_X = \pi$ and $\pi\pi^{-1} = \mathrm{id}_X$. Hence we conclude that $\mathcal{S}_X$ is a group, being called the **symmetric group** on X. It is in general non-abelian, and its elements are called **permutations**.

b) For $n \in \mathbb{N}$ we write $\mathcal{S}_n := \mathcal{S}_{\{1,\ldots,n\}}$, where for $n = 0$ we let $\mathcal{S}_0 := \mathcal{S}_\emptyset$. Then we have $|\mathcal{S}_n| = n!$, where for $n \in \mathbb{N}$ we let $n! := n(n-1)\cdots 1$, and $0! := 1$, being called the associated **factorial**:

We proceed by induction on $n \in \mathbb{N}_0$, where for $n = 0$ there is a unique map $\emptyset \to \emptyset$, which is bijective. Hence letting $n \in \mathbb{N}$ we may assume that $X = \{1, \ldots, n\}$, and let $X' := X \setminus \{n\}$. Given a bijective map $\pi\colon X \to X$, we have $\pi(n) = y$ for some $y \in X$, and hence $\pi\colon X' \to X \setminus \{y\}$ is bijective as well. Since there are n possibilities to choose y, and we have $|X'| = n-1$, by induction there are $n \cdot (n-1)! = n!$ possibilities for π. $\sharp$

For example, for $n = 1$ there the unique permutation $\mathrm{id}_{\{1\}}\colon 1 \mapsto 1$. For $n = 2$ there are two permutations $\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$, where we write out the pairs $[i, \pi(i)]$ in 'downward notation'. For $n = 3$ there are six permutations:

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

Then composition of maps is given by concatenation; for example:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} \underline{1} & \underline{3} & \underline{2} \\ 2 & 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ \underline{1} & \underline{3} & \underline{2} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} \underline{2} & \underline{1} & \underline{3} \\ 3 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 \\ \underline{2} & \underline{1} & \underline{3} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

Inversion is given by swapping the rows, and subsequently standard notation is achieved by sorting the rows in parallel; for example:

$$\left(\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \right)^{-1} = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

c) Any permutation $\pi \in \mathcal{S}_n$ can be written as a product of **disjoint cycles**: We consider the **directed graph** with **vertex** set $\{1, \ldots, n\}$ having an **edge** $i \to j$ if $\pi(i) = j$. Since π is a map, from any vertex precisely one edge emanates, and since π is bijective, at any vertex precisely one edge ends. Hence the **connected components** of this graph are **directed circles**. This also shows that the cycle decomposition of π is unique up to reordering the factors, where the order of the factors does not matter. Moreover, **fixed points**, that is cycles of **length** 1, are typically left out; and inverses are given by reading cycles backwardly.

For example, we have $\mathcal{S}_1 = \{()\}$ and $\mathcal{S}_2 = \{(), (1,2)\}$; these groups are abelian. Next, we have $\mathcal{S}_3 = \{(1,2,3), (1,3), (2,3), (1,3,2), (), (1,2)\}$, where $(1,2,3)^{-1} = (1,3,2)$ and $(1,3,2)^{-1} = (1,2,3)$, while the other elements of $\mathcal{S}_3$ are their own inverses; from $(1,2,3) \cdot (1,2) = (1,3)$ and $(2,3) \cdot (1,2,3) = (1,3)$ we deduce that $\mathcal{S}_n$ is non-abelian whenever $n \geq 3$.

(1.3) Alternating groups. a) Let $n \in \mathbb{N}_0$, and for $\pi \in \mathcal{S}_n$ let $l(\pi) := |\{\{i,j\} \subseteq \{1,\ldots,n\}; i < j, \pi(i) > \pi(j)\}| \in \mathbb{N}_0$ be its **inversion number**. Moreover, let the **sign** map $\operatorname{sgn}\colon \mathcal{S}_n \to \mathbb{Q}$ be defined by $\operatorname{sgn}(\pi) := \prod_{1\leq i<j\leq n} \frac{\pi(j)-\pi(i)}{j-i}$.

Since π induces a bijection on the set of all 2-element subsets of $\{1,\ldots,n\}$, with $\{i,j\}$ also $\{\pi(i),\pi(j)\}$ runs through these subsets. Thus this implies $\prod_{1\leq i<j\leq n} |\pi(j)-\pi(i)| = \prod_{1\leq i<j\leq n}(j-i)$, which equals $\prod_{k\in\{1,\ldots,n-1\}}(n-k)!$. Hence we actually have $\operatorname{sgn}\colon \mathcal{S}_n \to \{\pm 1\}\colon \pi \mapsto (-1)^{l(\pi)}$.

For example, we have $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$, for all $\pi \in \mathcal{S}_n$, as well as $\operatorname{sgn}(()) = 1$ and $\operatorname{sgn}((1,2)) = -1$; in particular, we infer $\operatorname{im}(\operatorname{sgn}) = \{\pm 1\}$ for $n \geq 2$. Moreover, for $\pi, \rho \in \mathcal{S}_n$ we have **multiplicativity** $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\cdot\operatorname{sgn}(\rho)$:

We have $\operatorname{sgn}(\pi\rho) = \prod_{1\leq i<j\leq n} \frac{\pi\rho(j)-\pi\rho(i)}{j-i} = \prod_{1\leq i<j\leq n}(\frac{\pi\rho(j)-\pi\rho(i)}{\rho(j)-\rho(i)} \cdot \frac{\rho(j)-\rho(i)}{j-i}) = (\prod_{1\leq i<j\leq n} \frac{\pi(\rho(j))-\pi(\rho(i))}{\rho(j)-\rho(i)})\cdot(\prod_{1\leq i<j\leq n} \frac{\rho(j)-\rho(i)}{j-i})$. Since $\{\rho(i),\rho(j)\}$ runs through the 2-element subsets of $\{1,\ldots,n\}$ if $\{i,j\}$ does so, from this we get $\operatorname{sgn}(\pi\rho) = (\prod_{1\leq i<j\leq n} \frac{\pi(j)-\pi(i)}{j-i}) \cdot (\prod_{1\leq i<j\leq n} \frac{\rho(j)-\rho(i)}{j-i}) = \operatorname{sgn}(\pi)\cdot\operatorname{sgn}(\rho)$. ♯

b) To compute $\operatorname{sgn}(\pi)$ we may also proceed as follows: Writing $\pi \in \mathcal{S}_n$ as a product of $r \in \mathbb{N}_0$ disjoint cycles, we get $\operatorname{sgn}(\pi) = (-1)^{n-r}$: By multiplicativity, it suffices to show that for the k-cycle $\delta_k := (1,\ldots,k) \in \mathcal{S}_k$, where $k \geq 2$, we have $\operatorname{sgn}(\delta_k) = (-1)^{k-1}$: Indeed, writing $\delta_k = \begin{bmatrix} 1 & 2 & \ldots & k-1 & k \\ 2 & 3 & \ldots & k & 1 \end{bmatrix}$ yields $l(\delta_k) = k-1$; alternatively, we have $\delta_k = (1,k)(1,k-1)\cdots(1,3)(1,2) \in \mathcal{S}_k$, which is a product of $k-1$ **transpositions**, where $l((1,2)) = 1$.

Note that this also shows that any permutation can be written as a product of transpositions, but where in general this representation is not unique, not even the number of transpositions is: $(1,2,3) = (1,3)(1,2) = (1,2)(2,3) = (1,2)(1,3)(2,3)(1,2) \in \mathcal{S}_3$.

c) The elements of $\mathcal{A}_n := \operatorname{sgn}^{-1}(\{1\}) = \{\pi \in \mathcal{S}_n; \operatorname{sgn}(\pi) = 1\}$ and of $\mathcal{S}_n \setminus \mathcal{A}_n = \{\pi \in \mathcal{S}_n; \operatorname{sgn}(\pi) = -1\}$ are called **even** and **odd** permutations, respectively. Hence by the properties collected above we conclude that $\mathcal{A}_n \leq \mathcal{S}_n$ is a subgroup, being called the associated **alternating group**; note that $\mathcal{A}_0 = \mathcal{S}_0 \cong \{1\}$ and $\mathcal{A}_1 = \mathcal{S}_1 \cong \{1\}$, while $\mathcal{A}_n < \mathcal{S}_n$ for $n \geq 2$.

(1.4) Cosets. a) Let $H \leq G$. Then, given $g \in G$, let the associated **(left) coset** of H in G be defined as the subset $gH := \{gh \in G; h \in H\} \subseteq G$. Hence, by the cancellation law, we conclude that the surjective map $H \to gH\colon h \mapsto gh$ is injective as well, that is bijective, in particular saying that $|gH| = |H|$.

Let $G/H := \{gH \subseteq G; g \in G\}$ be the set of cosets of H in G. Then two distinct cosets are disjoint: Let $g, g' \in G$ such that $x \in gH \cap g'H$, then we have $x = gy = g'y'$ for some $y, y' \in H$, implying that $gh = g'y'y^{-1}h \in g'H$ for all $h \in H$, that is $gH \subseteq g'H$, and by symmetry $gH = g'H$. Thus, since $g \in gH$ for any $g \in G$, we infer that the cosets of H in G disjointly cover all of G.

A subset $\mathcal{T} \subseteq G$ such that $\mathcal{T} \to G/H\colon t \mapsto tH$ is a bijection, is called a **(left)**

transversal of H in G; note that giving a transversal $\mathcal{T}$ amounts to pick a **representative** out of each coset, hence transversals exist by the Axiom of Choice. Thus we have $G = \coprod_{t\in\mathcal{T}} tH$, and the cardinality $[G\colon H] := |G/H| = |\mathcal{T}|$ is called the **index** of H in G.

Let now G be a finite group; then all cardinalities occurring above are finite. Thus we have $|G| = \sum_{t\in\mathcal{T}} |gH| = \sum_{t\in\mathcal{T}} |H| = |\mathcal{T}| \cdot |H|$, implying **Lagrange's Theorem** saying that $[G\colon H] = \frac{|G|}{|H|}$; in particular we have $|H| \mid |G|$. Thus, in order to search for subgroups of G, we need only consider subsets of G of cardinality dividing the cardinality of G.

For example, for $n \geq 2$, using the multiplicativity of the sign map, for any $\pi \in \mathcal{S}_n$ we get either $\mathrm{sgn}(\pi) = 1$ or $\mathrm{sgn}((1,2)\cdot\pi) = 1$, thus $\mathcal{S}_n = \mathcal{A}_n \,\dot\cup\, (1,2)\cdot\mathcal{A}_n$. Hence $\{(), (1,2)\}$ is a left transversal of $\mathcal{A}_n$ in $\mathcal{S}_n$, and we conclude $|\mathcal{A}_n| = \frac{1}{2}\cdot|\mathcal{S}_n| = \frac{n!}{2}$.

b) Similarly, given $g \in G$, the set $Hg := \{hg \in G; h \in H\} \subseteq G$ is called the associated **right coset**, where again $H \to Hg\colon h \mapsto hg$ is bijective. Let $H\backslash G$ be the set of right cosets of H in G, and a set of representatives of the latter is called a **right transversal** of H in G. If $\mathcal{T} \subseteq G$ is a left transversal of H in G, then from $G = \coprod_{t\in\mathcal{T}} tH$ by inversion we get $G = \coprod_{t\in\mathcal{T}} Ht^{-1}$, hence $\mathcal{T}^{-1} := \{t^{-1} \in G; t \in \mathcal{T}\}$ is a right transversal of H in G. Thus the index $[G\colon H]$ is independent of whether right or left cosets are considered. But in general left and right cosets do not coincide, and left transversals are not right transversals, leading to the following notion:

$H \leq G$ is called **normal**, if $gH \subseteq Hg$ for all $g \in G$; in this case we write $H \trianglelefteq G$. In this case, inversion yields $Hg^{-1} \subseteq g^{-1}H$, and since this holds for all $g \in G$ we infer $gH = Hg$, saying that indeed left and right cosets coincide; equivalently we have $gHg^{-1} = H$, that is H equals its **conjugate** ${}^gH := gHg^{-1}$.

For example, we have $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$; and any subgroup of an abelian group is normal. Moreover, any subgroup of index 2 is normal: We have $G = H \,\dot\cup\, Hg = H \,\dot\cup\, gH$, for any $g \in G \setminus H$. In particular, for $n \geq 2$ we have $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$. But $H := \{(), (1,2)\} \leq G := \mathcal{S}_3$, being of index 3, is not normal: We have $\mathcal{S}_3 = \{(), (1,2)\} \,\dot\cup\, \{(1,2,3), (1,3)\} \,\dot\cup\, \{(1,3,2), (2,3)\}$ as left cosets, while we get $\mathcal{S}_3 = \{(), (1,2)\} \,\dot\cup\, \{(1,2,3), (2,3)\} \,\dot\cup\, \{(1,3,2), (1,3)\}$ as right cosets; a left transversal is $\{(), (1,2,3), (2,3)\}$, which is not a right transversal.

(1.5) Generating sets. a) Let G be a group, and let $\{U_i \leq G; i \in \mathcal{I}\}$ where $\mathcal{I}$ is an index set. Then the set-theoretic intersection $\bigcap_{i\in\mathcal{I}} U_i \leq G$ is a subgroup; if $\mathcal{I} = \emptyset$ the latter is defined to be G. Moreover, if $U_i \trianglelefteq G$ for all $i \in \mathcal{I}$, then $\bigcap_{i\in\mathcal{I}} U_i \trianglelefteq G$ is normal as well. But in general $\bigcup_{i\in\mathcal{I}} U_i \subseteq G$ is not a subgroup, hence the set-theoretic union has to be replaced suitably:

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

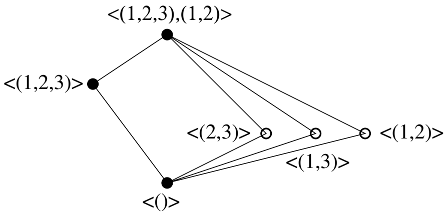
b) A subgroup $H \leq G$ is called **cyclic**, if there is $g \in H$ such that $H = \langle g \rangle$. For $g \in G$ we have $\langle g \rangle = \{g^i \in G; i \in \mathbb{Z}\}$; in particular cyclic groups are abelian.

If $\langle g \rangle$ is finite, then the cardinality $|g| := |\langle g \rangle| \in \mathbb{N}$ is called the **order** of g. We have the following description of $|g|$: Letting $i < j \in \mathbb{Z}$ such that $g^i = g^j$, we have $g^{j-i} = 1$. Hence there is $n \in \mathbb{N}$ minimal such that $g^n = 1$. Then for any $m \in \mathbb{Z}$ by quotient and remainder we get $m = kn + i$, where $k \in \mathbb{Z}$ and $i \in \{0, \ldots, n-1\}$, thus $g^m = (g^n)^k \cdot g^i = g^i$; in particular we have $g^m = 1$ if and only if $i = 0$, that is $n \mid m$. Hence we have $\langle g \rangle = \{g^i \in G; i \in \{0, \ldots, n-1\}\}$, where, since for $i < j \in \mathbb{Z}$ such that $g^i = g^j$ we have $n \mid j - i$, we conclude that $\langle g \rangle$ has precisely n elements, that is $|g|$ is the smallest $n \in \mathbb{N}$ such that $g^n = 1$.

Hence if G is finite, then by Lagrange's Theorem we have $|g| \mid |G|$, implying **Euler's Theorem** $g^{|G|} = 1$. In particular, if $|G|$ is a prime then G is cyclic.

Here is an infinite example: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is a cyclic additive group, and for any $n \in \mathbb{N}$ we have the cyclic subgroup $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle \trianglelefteq \mathbb{Z}$, the set $\mathbb{Z}_n := \{0, \ldots, n-1\} \subseteq \mathbb{Z}$ being a transversal: For $m \in \mathbb{Z}$ we have $m = kn + i$, where $k \in \mathbb{Z}$ and $i \in \{0, \ldots, n-1\}$, thus $m + n\mathbb{Z} = i + n\mathbb{Z}$; and if $i + n\mathbb{Z} = j + n\mathbb{Z}$, where $i < j \in \mathbb{Z}$, then $n \mid j - i$ implies that $j \geq i + n$.

c) As for non-cyclic groups, for example, for the symmetric group $\mathcal{S}_3$ we have $\mathcal{S}_3 = \langle (1,2,3), (1,2) \rangle$, where any non-cyclic subgroup coincides with $\mathcal{S}_3$, thus the only non-trivial proper subgroups are the normal cyclic subgroup $\langle (1,2,3) \rangle = \langle (1,3,2) \rangle$ of order 3, which coincides with the alternating group $\mathcal{A}_3$, and the non-normal cyclic subgroups $\langle (1,2) \rangle$, $\langle (1,3) \rangle$ and $\langle (2,3) \rangle$ of order 2; indeed for $\pi := (1,2,3)$ we get $\pi \cdot (1,2) \cdot \pi^{-1} = (2,3)$ and $\pi \cdot (2,3) \cdot \pi^{-1} = (1,3)$. The **lattice of subgroups** is depicted as a **Hasse diagram** as follows:



The other way around, given a group and a set of its elements, we might ask for the subgroup they generate; for example, we might just specify a few permutations in some symmetric group:

(1.6) Example: Perfect shuffles. We consider a deck of $n \in \mathbb{N}$ of cards.

a) The **Riffle shuffles** are given as follows: Assume that n is even, divide the deck into its top and bottom halves of the same size, and then interleave the halves perfectly. Then the top card of either the top or the bottom half ends up at the top of the final deck, where these cases are called the **out-shuffle** and the **in-shuffle**, respectively. Recording the position of the various cards before and after the shuffling yields permutations $\omega_n, \iota_n \in \mathcal{S}_n$. For example:

$$\begin{aligned} \omega_8 &= \begin{bmatrix} 1 & 5 & 2 & 6 & 3 & 7 & 4 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} &= (2,3,5)(4,7,6) \\ \iota_8 &= \begin{bmatrix} 5 & 1 & 6 & 2 & 7 & 3 & 8 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} &= (1,2,4,8,7,5)(3,6) \end{aligned}$$

Iterating the shuffling corresponds to multiplying the associated permutations: For example, for $n = 8$ performing an in-shuffle followed by an out-shuffle yields $\omega_8\iota_8 = (2,3,5)(4,7,6) \cdot (1,2,4,8,7,5)(3,6) = (1,3,4,8,6,5)(2,7)$, while the other way around we get $\iota_8\omega_8 = (1,2,4,8,7,5)(3,6) \cdot (2,3,5)(4,7,6) = (1,2,6,8,7,3)(4,5)$. This translates back into decks of cards as follows:

$$\begin{aligned} \omega_8\iota_8 &= (1,3,4,8,6,5)(2,7) &= \begin{bmatrix} 5 & 7 & 1 & 3 & 6 & 8 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} \\ \iota_8\omega_8 &= (1,2,6,8,7,3)(4,5) &= \begin{bmatrix} 3 & 1 & 7 & 5 & 4 & 2 & 8 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} \end{aligned}$$

Considering the Riffle shuffle group $\mathcal{R}_n := \langle \omega_n, \iota_n \rangle \leq \mathcal{S}_n$, for $n \geq 2$ even, we experimentally find the following pattern: $\mathcal{R}_n$ is transitive, but small compared to $\mathcal{S}_n$, where for $m \notin \{6,12\} \,\dot\cup\, \{2^k; k \geq 0\}$ we get $|\mathcal{R}_{2m}| = 2^{m-1} \cdot \frac{m!}{2}$ whenever $m \equiv 0 \pmod 4$, and $|\mathcal{R}_{2m}| = 2^m \cdot \frac{m!}{2}$ whenever $m \equiv 1 \pmod 4$, and $|\mathcal{R}_{2m}| = 2^m \cdot m!$ whenever $m \equiv 2 \pmod 4$, and $|\mathcal{R}_{2m}| = 2^{m-1} \cdot m!$ whenever $m \equiv 3 \pmod 4$, while for $k \geq 1$ we find $|\mathcal{R}_{2^k}| = 2^k \cdot k$, and $|\mathcal{R}_{12}| = 2^6 \cdot 120$ and $|\mathcal{R}_{24}| = 2^{11} \cdot 95040$; note that this indicates a close relationship between $\mathcal{R}_{2m}$ and the Mongean shuffle groups $\mathcal{M}_m$ discussed now:

b) The **Mongean shuffles** are given as follows: Start with the topmost card, and then put every other card on the top and on the bottom. Then the last card ends up at the top or the bottom, yielding permutations $\mu_n, \mu'_n \in \mathcal{S}_n$. For example, for $n = 8$ we get:

$$\begin{aligned} \mu_8 &= \begin{bmatrix} 8 & 6 & 4 & 2 & 1 & 3 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} &= (1,5,7,8)(2,4,3,6) \\ \mu'_8 &= \begin{bmatrix} 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} &= (1,4,6,7)(2,5) \end{aligned}$$

Considering the Mongean shuffle group $\mathcal{M}_n := \langle \mu_n, \mu'_n \rangle \leq \mathcal{S}_n$, for $n \geq 2$, we experimentally find the following pattern: If $n \notin \{6,12\} \,\dot\cup\, \{2^k; k \geq 3\}$, then $\mathcal{M}_n = \mathcal{S}_n$ whenever $n \equiv \{2,3\} \pmod 4$, and $\mathcal{M}_n = \mathcal{A}_n$ whenever $n \equiv \{0,1\} \pmod 4$, while for $k \geq 3$ we find $|\mathcal{M}_{2^k}| = 2^k \cdot (k+1)$, and we get $|\mathcal{M}_6| = 120 = \frac{6!}{6}$ and $|\mathcal{M}_{12}| = 95040 = \frac{12!}{5040}$.

(1.7) Homomorphisms. a) Let G and H be groups. Then $\varphi\colon G \to H$ is called a **(group) homomorphism**, if $\varphi(gg') = \varphi(g)\varphi(g')$ for all $g, g' \in G$. Then $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ yields $\varphi(1) = 1$, and for $g \in G$ we have $1 = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, hence $\varphi(g^{-1}) = \varphi(g)^{-1}$, thus $\varphi(g^n) = \varphi(g)^n$ for $n \in \mathbb{Z}$.

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**.

b) By the properties collected above, for any $U \leq G$ we have $\varphi(U) \leq H$, in particular $\mathrm{im}(\varphi) \leq G$; for any $V \leq H$ we have $\varphi^{-1}(V) \leq G$. Moreover, if $U \trianglelefteq G$ then from $\varphi(g)\varphi(U)\varphi(g)^{-1} = \varphi(gUg^{-1}) = \varphi(U)$, for all $g \in G$, we infer that $\varphi(U) \trianglelefteq \mathrm{im}(\varphi)$; and if $V \trianglelefteq \mathrm{im}(\varphi)$ then from $\varphi(g\varphi^{-1}(V)g^{-1}) = \varphi(g)V\varphi(g)^{-1} = V$, for all $g \in G$, we infer that $\varphi^{-1}(V) \trianglelefteq G$; in particular the **kernel** $\ker(\varphi) := \varphi^{-1}(\{1\}) = \{g \in G; \varphi(g) = 1\} \trianglelefteq G$ is a normal subgroup.

For $g \in G$ and $h = \varphi(g) \in \mathrm{im}(\varphi)$, we have $\varphi^{-1}(\{h\}) = g\ker(\varphi) \in G/\ker(\varphi)$; in particular, φ is injective if and only if $\ker(\varphi) = \{1\}$: For $u \in \ker(\varphi)$ we have $\varphi(gu) = \varphi(g)\varphi(u) = h$, thus $g\ker(\varphi) \subseteq \varphi^{-1}(\{h\})$, and for $g' \in \varphi^{-1}(\{h\})$ we have $\varphi(g^{-1}g') = 1$, thus $g' = gg^{-1}g' \in g\ker(\varphi)$.

c) For example, we have the **trivial** homomorphism $\varphi\colon G \to \{1\}\colon g \mapsto 1$, with kernel $\ker(\varphi) = G$; and the identity homomorphism $\mathrm{id}_G\colon G \to G\colon g \mapsto g$ with image $\mathrm{im}(\varphi) = G$ and kernel $\ker(\mathrm{id}_G) = \{1\}$.

Given $g \in G$, the map $\mathbb{Z} \to \langle g\rangle\colon i \mapsto g^i$ is a surjective homomorphism from the additive group $\mathbb{Z}$ to the multiplicative group $\langle g\rangle$, which for $\langle g\rangle$ finite has kernel $|g| \cdot \mathbb{Z}$; for $\langle g\rangle$ infinite it has kernel $\{0\}$, thus in this case is an isomorphism.

The exponential function $\exp\colon \mathbb{R} \to \mathbb{R}^*\colon x \mapsto e^x$ is a homomorphism from the additive group $\mathbb{R}$ to the multiplicative group $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, with image $\mathrm{im}(\exp) = \mathbb{R}_{>0}$ and kernel $\ker(\exp) = \{0\}$; in particular exp is injective.

The sign map $\mathrm{sgn}\colon \mathcal{S}_n \to \{\pm 1\}$ is a homomorphism, where $\{\pm 1\}$ is considered as a multiplicative group, with image $\mathrm{im}(\mathrm{sgn}) = \{\pm 1\}$ if and only if $n \geq 2$, and kernel $\mathcal{A}_n := \ker(\mathrm{sgn}) \trianglelefteq \mathcal{S}_n$.

(1.8) Actions. a) Let G be a group, and let $X \neq \emptyset$ be a set. Then G is said to **act** on X, and the latter is called a **G-set**, if there is an **action map** $G \times X \to X\colon [g, x] \mapsto gx$ fulfilling the following conditions: We have **i)** $1 \cdot x = x$, and **ii)** $(gh)x = g(hx)$ for $g, h \in G$ and $x \in X$.

If X and Y are G-sets, then a map $\alpha\colon X \to Y$ such that $\alpha(gx) = g(\alpha(x)$, for all $x \in X$ and $g \in G$, is called a **(G-set) homomorphism**; if α is bijective, then it is called an isomorphism, in which case $X \cong Y$ are also called **equivalent**.

The connection to group homomorphisms is given as follows: Given an action of G on X, for $g \in G$ let $\varphi_g\colon X \to X\colon x \mapsto gx$. Hence from $\varphi_g\varphi_{g^{-1}} = \varphi_{g^{-1}}\varphi_g = \varphi_1 = \mathrm{id}_X$ we infer that $\varphi_g \in \mathcal{S}_X$ 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 $G \times X \to X \colon [g, x] \mapsto \varphi_g(x)$ 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 $(gh)x = g(hx)$ for all $g, h \in G$ and $x \in X$.

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

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

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

c) Here are a few examples: For $n \in \mathbb{N}$ the group $\mathcal{S}_n$ acts **naturally** on $\{1, \ldots, n\}$ by $\varphi_\pi = \pi$, for all $\pi \in \mathcal{S}_n$, that is with action homomorphism $\mathrm{id}_{\mathcal{S}_n}$; the action is transitive. Hence for $\pi \in \mathcal{S}_n$ the subgroup $\langle \pi \rangle \leq \mathcal{S}_n$ also acts on $\{1, \ldots, n\}$; its orbits coincide with the cycles of π.

G acts **trivially** on X by $\varphi_g \colon X \to X \colon x \mapsto x$, for $g \in G$; the associated action homomorphism is $G \to \mathcal{S}_X \colon g \mapsto \mathrm{id}_X$, the orbits are the singleton subsets of X.

G acts by **conjugation** on G by $\kappa_g \colon G \to G \colon x \mapsto {}^g x = gxg^{-1}$, for $g \in G$: We have $\kappa_1 = \mathrm{id}_G$, and $\kappa_g \kappa_h = \kappa_{gh} \colon x \mapsto g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1}$. The associated orbits are called the **conjugacy classes** of G. Note that, in particular, any normal subgroup of G is a union of conjugacy classes.

G acts **(left) regularly** on G by $\rho_g \colon G \to G \colon x \mapsto gx$, for all $g \in G$: We have $\rho_1 = \mathrm{id}_G$, and $\rho_g \rho_h = \rho_{gh}$ by associativity. Since $g \cdot 1 = g$, for $g \in G$, the action is transitive. Let $\rho \colon G \to \mathcal{S}_G \colon g \mapsto \rho_g$ be the associated action homomorphism. For $g \in \ker(\rho)$ we have $g = g \cdot 1 = \rho_g(1) = \mathrm{id}_G(1) = 1$, implying that $\ker(\rho) = \{1\}$, that is ρ is injective. Thus we have **Cayley's Theorem**, saying that G is isomorphic to a subgroup of $\mathcal{S}_G$.

(1.9) Transitive actions. a) We provide prototypes first: To this end let G be a group and let $U \leq G$. Then U acts on G by **right multiplication** $\rho_u \colon G \to G \colon x \mapsto xu^{-1}$ for all $u \in U$: We have $\rho_1(u) = u \cdot 1^{-1} = u$ and $\rho_{uv}(x) = x(uv)^{-1} = xv^{-1}u^{-1} = \rho_u(\rho_v(x))$ for all $x \in G$ and $u, v \in U$. Hence the U-orbit of $x \in G$ is the (left) coset $xU := \{xu \in G; u \in U\} \subseteq G$, and the set of U orbits coincides with G/U. Moreover, G acts transitively on G/U by **left multiplication** $\rho_g \colon G/U \to G/U \colon xU \mapsto gxU$ for all $g \in G$: We have $1 \cdot xU = xU$ and $gh \cdot xU = g \cdot hxU$ for all $g, h, x \in G$,

Let now X be a transitive G-set. For $x \in X$ let $G_x = \mathrm{Stab}_G(x) := \{g \in G; gx =$

$x\}$ be the **stabilizer** of x in G. Actually we have $G_x \leq G$: We have $1 \in G_x$, and for $g, h \in G_x$ from $gx = x = hx$ we get $g^{-1}x = x = ghx$, hence $g^{-1}, gh \in G_x$.

Note that the elements of X have conjugate stabilizers: Indeed, for $g \in G$ we have $G_{gx} = {}^gG_x$: For $h \in G_x$, from $ghg^{-1}(gx) = gx$ we get $gG_xg^{-1} \subseteq G_{gx}$, and thus we have $G_{gx} = gg^{-1}G_{gx}gg^{-1} \subseteq gG_{g^{-1}gx}g^{-1} = gG_{gx}g^{-1}$ as well.

Then for $x \in X$ the natural map $\nu\colon G/G_x \rightarrow X\colon gG_x \mapsto gx$ is a G-set isomorphism, where G acts on G/G_x by left multiplication; in other words, the G-sets X and G/G_x are equivalent: For $g, h \in G$ and $u \in G_x$ we have $gux = gx$, hence ν is well-defined; and $\nu(ghG_x) = (gh)x = g(hx) = g \cdot \nu(hG_x)$, hence ν is a G-set homomorphism; since X is transitive, ν is surjective; and whenever $gx = hx$ then we have $h^{-1}g \in G_x$, hence $g \in hG_x$, thus ν is injective as well.

Thus, if G is finite then we have the **orbit-stabilizer theorem**, saying that for any $x \in X$ we have $|X| = [G\colon G_x] = \frac{|G|}{|G_x|}$; in particular we have $|X| \mid |G|$.

b) We proceed to give a classification of transitive G-sets, and again we consider the prototypes first: Whenever $V \leq G$ is conjugate to U, then G/U and G/V are equivalent: Indeed, letting $h \in G$ such that $V = {}^hU$, the map $\eta\colon G/U \rightarrow G/{}^hU\colon xU \mapsto xh^{-1} \cdot {}^hU = xUh^{-1}$ is a G-set isomorphism: For $u \in U$, from $xUh^{-1} = xuUh^{-1}$ we infer that η is well-defined; for $g \in G$ we have $\eta(g \cdot xU) = gxUh^{-1}$ and $g \cdot \eta(xU) = gxUh^{-1}$, hence η is a G-set homomorphism; η is surjective; and for $x, y \in G$ we have $xUh^{-1} = yUh^{-1}$ if and only if $xU = yU$, thus η is injective as well.

This yields the following classification of transitive G-sets: If Y is a transitive G-set, then X and Y are equivalent if and only if for some (and hence any) $x \in X$ and $y \in Y$ the stabilizers G_x and G_y are conjugate in G: If $\alpha\colon X \rightarrow Y$ is a G-set isomorphism, then for any $x \in X$ we have $G_x = G_{\alpha(x)}$: For $g \in G_x$ we have $g\alpha(x) = \alpha(gx) = \alpha(x) \in Y$, and for $g \in G_{\alpha(x)}$ we have $\alpha^{-1}\alpha(gx) = \alpha^{-1}(g \cdot \alpha(x)) = \alpha^{-1}\alpha(x) = x \in X$. Conversely, if $G_y = {}^gG_x$ for some $g \in G$, then we have $Y \cong G/G_y = G/{}^gG_x \cong G/G_x \cong X$.

We show a useful statement allowing to determine (easily) the number of orbits of a finite group action on a finite set; example applications are given in (1.18):

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

Proof. Letting $\mathcal{F} := \{[g, x] \in G \times X; gx = x\}$, we determine $|\mathcal{F}|$ in two different ways: On the one hand we have $|\mathcal{F}| = \sum_{g \in G} |\{x \in X; gx = x\}| = \sum_{g \in G} |\mathrm{Fix}_X(g)|$. On the other hand we have $|\mathcal{F}| = \sum_{x \in X} |\{g \in G; gx = x\}| = \sum_{x \in X} |G_x|$. For $y \in Gx$ we have $|Gx| = |Gy|$, and thus $|G_x| = |G_y|$. Letting $\mathcal{S} \subseteq X$ be a set of orbit representatives, we get $\sum_{x \in X} |G_x| = \sum_{x \in \mathcal{S}} \sum_{y \in Gx} |G_y| = \sum_{x \in \mathcal{S}} |Gx| \cdot |G_x| = \sum_{x \in \mathcal{S}} |G| = |G \backslash X| \cdot |G|$. ♯

(1.11) Symmetries in geometry. Groups are the abstract concept to describe all kinds symmetries occurring in mathematics, physics or elsewhere in nature: Let $\mathcal{X}$ be an 'object', that is a set X together with 'additional structure'. Then a **symmetry** of $\mathcal{X}$ is a bijective map $\pi\colon X \to X$ respecting the 'additional structure'. Hence, typically, given symmetries π and ρ, the composition $\pi\rho$, the inverse map π^{-1}, and the identity map id_X are symmetries as well. Thus the set of symmetries of $\mathcal{X}$ forms a subgroup of $\mathcal{S}_X$, being called the **symmetry group** of $\mathcal{X}$. From our point of view, where groups are considered as abstract mathematical objects in their own right, we need the notion of group actions to facilitate their application to describe symmetries.

a) We consider the $\mathbb{R}$-vector space $\mathbb{R}^{n\times 1}$, for $n \in \mathbb{N}$. Then the symmetries of $\mathbb{R}^{n\times 1}$ are its $\mathbb{R}$-linear automorphisms. Hence its symmetry group is the **general linear group** $\mathrm{GL}_n(\mathbb{R}) := \{A \in \mathbb{R}^{n\times n}; A \text{ invertible}\} = \{A \in \mathbb{R}^{n\times n}; \mathrm{rk}_{\mathbb{R}}(A) = n\} = \{A \in \mathbb{R}^{n\times n}; \det(A) \neq 0\}$ of degree n, where $A \in \mathrm{GL}_n(\mathbb{R})$ acts **naturally** on $\mathbb{R}^{n\times 1}$ by $\varphi_A\colon v \mapsto Av$; the orbits are given as $\{0\}$ and $\mathbb{R}^{n\times 1} \setminus \{0\}$.

We have $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$, which is abelian, but the following shows that $\mathrm{GL}_n(\mathbb{R})$ is non-abelian for $n \geq 2$:

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

Moreover, the determinant map $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ is is an epimorphism, where $\mathbb{R}^*$ is considered as a multiplicative group. Its kernel $\mathrm{SL}_n(\mathbb{R}) := \ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}); \det(A) = 1\} \trianglelefteq \mathrm{GL}_n(\mathbb{R})$ is called the **special linear group** of degree n. We have $\mathrm{SL}_1(\mathbb{R}) = \{1\}$, while for $n \geq 2$ the orbits of the action of $\mathrm{SL}_n(\mathbb{R})$ on $\mathbb{R}^{n\times 1}$ are again given as $\{0\}$ and $\mathbb{R}^{n\times 1} \setminus \{0\}$.

b) The $\mathbb{R}$-vector space $\mathbb{R}^{n\times 1}$ can be viewed as an Euclidean space, with respect to the standard scalar product $\langle\cdot,\cdot\rangle\colon \mathbb{R}^{n\times 1} \times \mathbb{R}^{n\times 1} \to \mathbb{R}$, which is given by $\langle [x_1, \ldots, x_n]^{\mathrm{tr}}, [y_1, \ldots, x_y]^{\mathrm{tr}}\rangle := \sum_{i=1}^n x_i y_i$. Thus $\mathbb{R}^{n\times 1}$ becomes a metric topological space, and we may speak of the length of a vector and of the angle between two non-zero vectors. Hence the symmetries of $\mathbb{R}^{n\times 1}$ as an Euclidean space are the $\mathbb{R}$-linear automorphisms $A \in \mathrm{GL}_n(\mathbb{R})$ leaving $\langle\cdot,\cdot\rangle$ invariant, that is the length- and angle-preserving $\mathbb{R}$-linear automorphisms, where the latter means that $\langle Av, Aw\rangle = \langle v, w\rangle$ for all $v, w \in \mathbb{R}^{n\times 1}$.

Using the standard $\mathbb{R}$-basis of $\mathbb{R}^{n\times 1}$, this condition translates into the equation $A^{\mathrm{tr}}A = E_n$. Hence as symmetry group we obtain the **general orthogonal group** $O_n(\mathbb{R}) = \mathrm{GO}_n(\mathbb{R}) := \{A \in \mathrm{GL}_n(\mathbb{R}); A^{\mathrm{tr}}A = E_n\} = \{A \in \mathrm{GL}_n(\mathbb{R}); A^{-1} = A^{\mathrm{tr}}\} \leq \mathrm{GL}_n(\mathbb{R})$, of degree n, its elements are called **isometries**; note that for $A, B \in O_n(\mathbb{R})$ we indeed have $(AB)^{\mathrm{tr}} \cdot AB = B^{\mathrm{tr}}A^{\mathrm{tr}}AB = E_n$ and $(A^{-1})^{\mathrm{tr}}A^{-1} = (A^{\mathrm{tr}})^{-1}A^{-1} = (AA^{\mathrm{tr}})^{-1} = E_n$, hence $AB, A^{-1} \in O_n(\mathbb{R})$. The orbits of the action of $O_n(\mathbb{R})$ on $\mathbb{R}^{n\times 1}$ are given as the sets of vectors of a fixed length, that is the sets $\{v \in \mathbb{R}^{n\times 1}; \langle v, v\rangle = a\}$ for $a \geq 0$.

Moreover, for $A \in O_n(\mathbb{R})$ we have $\det(A)^2 = \det(A^{\mathrm{tr}})\det(A) = \det(A^{\mathrm{tr}}A) = \det(E_n) = 1$, thus we get an epimorphism $\det\colon O_n(\mathbb{R}) \to \{\pm 1\}$, where $\{\pm 1\}$

is considered as a multiplicative group; note that $|\det(A)| = 1$ for $A \in O_2(\mathbb{R})$ reflects the fact that isometries are volume-preserving. The kernel $\mathrm{SO}_n(\mathbb{R}) := \ker(\det) = \{A \in O_n(\mathbb{R}); \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R}) \cap O_n(\mathbb{R}) \trianglelefteq O_n(\mathbb{R})$ is called the **special orthogonal group** of degree n, whose elements are called **rotations**, and we have $O_n(\mathbb{R}) = \mathrm{SO}_n(\mathbb{R}) \,\dot{\cup}\, \{A \in O_n(\mathbb{R}); \det(A) = -1\}$, where the elements of $O_n(\mathbb{R}) \setminus \mathrm{SO}_n(\mathbb{R})$ are called **reflections**. We have $\mathrm{SO}_1(\mathbb{R}) = \{1\}$, while for $n \geq 2$ the orbits of the action of $\mathrm{SO}_n(\mathbb{R})$ on $\mathbb{R}^{n\times 1}$ are again given as the sets $\{v \in \mathbb{R}^{n\times 1}; \langle v, v\rangle = a\}$ for $a \geq 0$.

(1.12) Dihedral groups. For $n \geq 3$ let $\mathbb{D}_n \subseteq \mathbb{R}^{2\times 1}$ be a regular n-gon centered at the origin, and let $\mathcal{D}_n := \{A \in O_2(\mathbb{R}); A \cdot \mathbb{D}_n = \mathbb{D}_n\} \leq O_2(\mathbb{R})$ be its symmetry group, where $\mathcal{C}_n := \mathcal{D}_n \cap \mathrm{SO}_2(\mathbb{R}) \trianglelefteq \mathcal{D}_n$ is called its group of rotations. Hence $\mathcal{D}_n$ permutes the n vertices of $\mathbb{D}_n$, and numbering the vertices counterclockwise yields an action homomorphism $\varphi\colon \mathcal{D}_n \to \mathcal{S}_n$, whose image $D_{2n} := \varphi(\mathcal{D}_n) \leq \mathcal{S}_n$ is called the associated **dihedral group**; note that, since the set of vertices of $\mathbb{D}_n$ contains an $\mathbb{R}$-basis of $\mathbb{R}^{2\times 1}$, we conclude that φ is injective.

We describe the elements of D_{2n}, showing that $|D_{2n}| = 2n$; for example, we have $D_6 = \{(), (1,2,3), (1,3,2); (2,3), (1,3), (1,2)\} = \mathcal{S}_3$ and

$$D_8 = \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2), (2,4); (1,3), (1,2)(3,4), (1,4)(2,3)\}.$$

Since rotations are determined by their rotation angle, see (1.16), the rotations in $\mathcal{D}_n$ 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 $\delta_n^k \in \mathcal{S}_n$ for $k \in \{0,\ldots,n-1\}$, where $\delta_n := (1,2,\ldots,n) \in \mathcal{S}_n$. Hence the group of rotations $\mathcal{C}_n \cong C_n := \{\delta_n^k; k \in \{0,\ldots,n-1\}\} = \langle \delta_n \rangle \leq D_{2n}$ is cyclic of order n, and acts regularly, that is transitively with $|\mathrm{Stab}_{C_n}(1)| = 1$.

Since reflections are determined by their reflection axis, see again (1.16), we distinguish the cases n odd and even: For n odd the axis of a reflection in $\mathcal{D}_n$ runs through one of the vertices of $\mathcal{D}_n$ 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 $\mathcal{D}_n$ 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 $(1,2)(3,n)(4,n-1)\cdots(\frac{n+2}{2}, \frac{n+4}{2}) \in \mathcal{S}_n$.

The group D_{2n} acting transitively, we have $|\mathrm{Stab}_{D_{2n}}(1)| = \frac{|D_{2n}|}{n} = 2$; in both cases we have $\mathrm{Stab}_{D_{2n}}(1) = \langle \sigma_n \rangle$. Moreover, $C_n \trianglelefteq D_{2n}$ is a normal subgroup of index 2, where from $\sigma_n \notin C_n$ we get $D_{2n} = C_n \,\dot{\cup}\, C_n\sigma_n = \langle \delta_n, \sigma_n \rangle$. Any element $\pi \in D_{2n}$ can be written uniquely as $\pi = \delta_n^k \sigma_n^i$, where $i \in \{0,1\}$ and $k \in \{0,\ldots,n-1\}$, and $\sigma_n \delta_n \sigma_n^{-1} = (1,n,n-1,\ldots,2) = \delta_n^{-1}$ shows that multiplication is given by $\delta_n^k \sigma_n^i \cdot \delta_n^l \sigma_n^j = \delta_n^{k-il} \sigma_n^{i+j}$; in particular D_{2n} is non-abelian.

(1.13) Platonic solids. A **platonic solid** $\mathbb{P}$ is a convex polyhedron in Euclidean space $\mathbb{R}^{3\times 1}$, whose faces are all regular n-gons, for some $n \geq 3$, such that any vertex is incident with the same number $k \in \mathbb{N}$ of edges.

We proceed to find all platonic solids: Subdividing the regular n-gon into triangles by connecting its barycenter with the vertices, the inner angle α at the circumference is seen to be given by $n\alpha + 2\pi = n\pi$, that is $\alpha = \frac{n-2}{n} \cdot \pi$. In order to form a convex body we necessarily have $k \geq 3$ and $k\alpha < 2\pi$. This yields $3 \cdot \frac{n-2}{n} < 2$, that is $n < 6$. Then for $n = 3$ we get $k \cdot \frac{1}{3} < 2$, thus $k < 6$; for $n = 4$ we get $k \cdot \frac{2}{4} < 2$, thus $k < 4$; and for $n = 5$ we get $k \cdot \frac{3}{5} < 2$, thus $k < 4$. This yields the five cases for $[n, k]$ listed below.

We show that $\mathbb{P}$ is uniquely determined from $[n, k]$. To this end, let $\mathbb{P}$ have v vertices, e edges and f faces. These figures are not independent from each other, but related by **Euler's polyhedron formula** $v - e + f = 2$:

Projecting $\mathbb{P}$, by stereographic projection, into the Euclidean plane yields a connected finite graph with v vertices and e edges, dividing the plane into f connected domains, one of which is unbounded. We proceed by induction on $f \in \mathbb{N}$: For $f = 1$ there only is the unbounded domain, implying that the graph under consideration is a tree, hence $v = e + 1$ and thus $v - e + f = 2$. For $f \geq 2$ there are at least two domains, and removing an edge incident to the unbounded domain, thereby loosing a bounded area as well, we obtain a graph having v vertices, $e - 1$ edges and $f - 1$ domains, thus by induction we get $2 = v - (e - 1) + (f - 1) = v - e + f$. ♯

Now, since any edge of $\mathbb{P}$ is incident with two faces and any face is incident with n edges, we have $2e = nf$; and since any edge is incident with 2 vertices and any vertex is incident with k edges, we have $2e = kv$; this implies that $nf = kv$. Then Euler's polyhedron formula $v - e + f = 2$ yields $2 = \frac{nf}{k} - \frac{nf}{2} + f = f \cdot (\frac{n}{k} - \frac{n}{2} + 1)$. Thus f is determined from $[n, k]$, and subsequently e and v are as well. For the five admissible cases we get:

n	k	v	e	f	$\mathbb{P}$
3	3	4	6	4	tetrahedron
3	4	6	12	8	octahedron
3	5	12	30	20	icosahedron
4	3	8	12	6	hexahedron
5	3	20	30	12	dodecahedron

For each of these five cases there actually exists a corresponding platonic solid, where the names are reminiscent of the number of faces. Moreover, as the pairs $[v, f]$ occurring already indicate, there is a duality between the octahedron and the hexahedron (also called the cube), and between the icosahedron and the dodecahedron, while the tetrahedron is self-dual: Connecting the barycenters of the faces one of the mutually dual polyhedra yields the other one. Hence polyhedra in duality have the same symmetry group, so that we can restrict ourselves to the tetrahedron, the hexahedron and the icosahedron:

(1.14) Polyhedral groups. a) Let $\mathbb{T} \subseteq \mathbb{R}^{3\times 1}$ be a tetrahedron centered at the origin, let $\widetilde{\mathcal{T}} := \{A \in O_3(\mathbb{R}); A \cdot \mathbb{T} = \mathbb{T}\} \leq O_3(\mathbb{R})$ be its symmetry group, and let $\mathcal{T} := \widetilde{\mathcal{T}} \cap \mathrm{SO}_3(\mathbb{R}) \trianglelefteq \widetilde{\mathcal{T}}$ be its group of rotations. Hence $\widetilde{\mathcal{T}}$ permutes the 4 vertices of $\mathbb{T}$, yielding an action homomorphism $\varphi\colon \widetilde{\mathcal{T}} \rightarrow \mathcal{S}_4$, with image $\widetilde{T} := \varphi(\widetilde{\mathcal{T}}) \leq \mathcal{S}_4$. Then $T := \varphi(\mathcal{T}) \trianglelefteq \widetilde{T}$ is a normal subgroup of index ≤ 2. Note that the set of vertices of $\mathbb{T}$ contains an $\mathbb{R}$-basis of $\mathbb{R}^{3\times 1}$, hence φ is injective.

The group $\widetilde{T}$ acts transitively on the vertices. Fixing vertex 4, there is a rotation of order 3 with respect to the axis given by connecting vertex 4 with the opposite face $\{1,2,3\}$, and fixing edge $\{3,4\}$ pointwise there is a reflection with respect to the hyperplane through $\{3,4\}$ and perpendicular to $\{1,2\}$. Hence we get $\mathcal{S}_3 = \langle (1,2,3),(1,2)\rangle \leq \mathrm{Stab}_{\widetilde{T}}(1)$, where from $|\mathrm{Stab}_{\widetilde{T}}(4)| = \frac{|\widetilde{T}|}{4} \mid \frac{|\mathcal{S}_4|}{4} = 6 = |\mathcal{S}_3|$ we infer equality, and thus $|\widetilde{T}| = |\mathrm{Stab}_{\widetilde{T}}(4)| \cdot 4 = 24$ yields $\widetilde{T} = \mathcal{S}_4$.

Since $\widetilde{T}$ contains a reflection, we have $[\widetilde{T}\colon T] = 2$, thus $|T| = 12$. As above, fixing the vertices in turn, we get $\langle (1,2,3),(1,2,4),(1,3,4),(2,3,4)\rangle \leq T$, where the left hand side equals $\mathcal{A}_4$, implying $T = \mathcal{A}_4$. In particular, T acts transitively on the vertices, where $C_3 \cong \langle (1,2,3)\rangle = \mathrm{Stab}_T(4)$. Hence $\mathcal{T}$ contains 8 rotations of order 3, with respect to the 4 axes obtained by connecting a vertex with the barycenter of the opposite face, and 3 rotations of order 2, with respect to the 3 axes obtained by connecting the centers of opposite edges.

b) Let $\mathbb{H} \subseteq \mathbb{R}^{3\times 1}$ be a hexahedron centered at the origin, let $\widetilde{\mathcal{H}} := \{A \in O_3(\mathbb{R}); A\cdot\mathbb{H} = \mathbb{H}\} \leq O_3(\mathbb{R})$ be its symmetry group, and let $\mathcal{H} := \widetilde{\mathcal{H}} \cap \mathrm{SO}_3(\mathbb{R}) \trianglelefteq \widetilde{\mathcal{H}}$ be its group of rotations. Hence $\widetilde{\mathcal{H}}$ permutes the 8 vertices of $\mathbb{H}$. Assuming these to have coordinates $[-1,-1,-1]^{\mathrm{tr}}, [-1,-1,1]^{\mathrm{tr}}, \ldots, [1,1,1]^{\mathrm{tr}}$, in lexicographic order, yields an action homomorphism $\varphi\colon \widetilde{\mathcal{H}} \rightarrow \mathcal{S}_8$, with image $\widetilde{H} := \varphi(\widetilde{\mathcal{H}}) \leq \mathcal{S}_8$. Then $H := \varphi(\mathcal{H}) \trianglelefteq \widetilde{H}$ is a normal subgroup of index ≤ 2. Note that the set of vertices of $\mathbb{H}$ contains an $\mathbb{R}$-basis of $\mathbb{R}^{3\times 1}$, hence φ is injective.

Both groups $\widetilde{H}$ and H act transitively on the vertices. Since $\widetilde{\mathcal{H}}$ contains the reflection given by $v \mapsto -v$, for all vertices v, in other words we have $\pi := (1,8)(2,7)(3,6)(4,5) \in \widetilde{H}$, we conclude that $[\widetilde{H}\colon H] = 2$ and $\widetilde{H} = \langle H, \pi\rangle$.

We proceed to describe H: Fixing vertex 1, we conclude that vertex 8, being the only of edge distance 3 from vertex 1, is fixed as well. Hence $\mathrm{Stab}_H(1)$ only contains rotations of order 3, with respect to the axis given by connecting vertices $\{1,8\}$. These permute vertices $\{2,3,5\}$ and $\{4,6,7\}$, that is those being of edge distance 1 and 2 from vertex 1, respectively. Hence we conclude that $\mathrm{Stab}_H(1) = \langle (2,5,3)(4,6,7)\rangle \cong C_3$, and thus $|H| = |\mathrm{Stab}_H(1)| \cdot 8 = 24$.

We consider the action of $\widetilde{\mathcal{H}}$ on the 4 axes obtained by connecting opposite vertices, in other words we consider the action of $\widetilde{H}$ on the set of 2-subsets $\mathcal{X} := \{\{1,8\},\{2,7\},\{3,6\},\{4,5\}\}$, in this order. This yields an action homomorphism $\psi\colon \widetilde{H} \rightarrow \mathcal{S}_4$, which since $\pi \in \ker(\psi)$ is not injective. But we show that the restriction of ψ to H indeed is injective, implying that $H \cong \mathcal{S}_4$:

Assume that $\rho \in H \cap \ker(\psi)$, thus ρ fixes all 2-sets in $\mathcal{X}$, in particular we have

$\rho(1) \in \{1, 8\}$. Assume that $\rho(1) = 8$, then ρ interchanges $1 \leftrightarrow 8$, and edge distances show that ρ interchanges the sets $\{2, 3, 5\} \leftrightarrow \{4, 6, 7\}$; hence from $\rho \in \ker(\psi)$ we infer that ρ interchanges $2 \leftrightarrow 7$, $3 \leftrightarrow 6$, $4 \leftrightarrow 5$, thus $\rho = \pi \notin H$, a contradiction. Hence we have $\rho(1) = 1$ and $\rho(8) = 8$, and edge distances show that ρ leaves the sets $\{2, 3, 5\}$ and $\{4, 6, 7\}$ invariant; hence from $\rho \in \ker(\psi)$ we infer that ρ fixes $\{2, \ldots, 7\}$ elementwise, hence $\rho = ()$.

In particular, H acts transitively on $\mathcal{X}$, where $|\mathrm{Stab}_H(\{1, 8\})| = \frac{|H|}{4} = 6$. Hence $\mathcal{H}$ contains 6 rotations of order 4, and 3 rotations of order 2, both with respect to the 3 axes obtained by connecting the barycenters of opposite faces, and 8 rotations of order 3, with respect to the 4 axes obtained by connecting opposite vertices, and 6 rotations of order 2, with respect to the 6 axes obtained by connecting the centers of opposite edges.

c) Let $\mathbb{I} \subseteq \mathbb{R}^{3\times 1}$ be an icosahedron centered at the origin, let $\widetilde{\mathcal{I}} := \{A \in O_3(\mathbb{R}); A \cdot \mathbb{I} = \mathbb{I}\} \leq O_3(\mathbb{R})$ be its symmetry group, and let $\mathcal{I} := \widetilde{\mathcal{I}} \cap \mathrm{SO}_3(\mathbb{R}) \trianglelefteq \widetilde{\mathcal{I}}$ be its group of rotations. Instead of considering $\mathbb{I}$ we consider the **truncated icosahedron (Buckminsterfullerene, soccer ball)** $\mathbb{I}'$, which is obtained from $\mathbb{I}$ by truncating at the 12 vertices, yielding a solid having 60 vertices, and 12 regular pentagonal and 20 regular hexagonal faces, where each pentagonal face is surrounded by hexagonal ones, and each hexagonal face is surrounded by hexagonal and pentagonal ones. Hence $\widetilde{\mathcal{I}}$ and $\mathcal{I}$ are also the symmetry group and group of rotations of $\mathbb{I}'$, respectively. We describe $\mathcal{I}$:

The group $\mathcal{I}$ acts regularly, that is transitively with trivial stabilizer, on the $12 \cdot 5 = 60$ pairs of adjacent pentagon-hexagon pairs, implying $|\mathcal{I}| = 60$. There are 24 rotations of order 5, with respect to the 6 axes obtained by connecting the barycenters of opposite pentagons, and 20 rotations of order 3, with respect to the 10 axes obtained by connecting the barycenters of opposite hexagons, and 15 rotations of order 2, with respect to the 15 axes obtained by connecting the centers of opposite hexagon-hexagon edges.

We proceed to specify a transitive action of $\mathcal{I}$ on a 5-set, whose associate action homomorphism $\varphi \colon \mathcal{I} \to \mathcal{S}_5$ is injective and whose image is contained in $\mathcal{A}_5$; this implies that $\mathcal{I} \cong \mathcal{A}_5$: In order to do so we consider the 15 rotation axes of order 2. Fixing such an axis, there are precisely two other such axes orthogonal to the given one; connecting the 6 points of intersection of these axes with $\mathbb{I}'$ yields the vertices of an octahedron. The orthogonality property implies that this partitions the set of these rotation axes into 5 subsets $\mathcal{T}_j$, for $j \in \{1, \ldots, 5\}$, of cardinality 3 each. Thus $\mathcal{I}$ acts transitively on $\{\mathcal{T}_1, \ldots, \mathcal{T}_5\}$, giving rise to an action homomorphism $\varphi \colon \mathcal{I} \to \mathcal{S}_5$. We show that $\varphi \colon \mathcal{I} \to \mathcal{A}_5$ is an isomorphism:

Considering the elements $\pi \in \mathcal{I}$ of order 2, 3 and 5 separately, their respective geometric interpretation shows that there always is some $\mathcal{T}_j$ which is not fixed by π. Hence we have $\varphi(\pi) \neq ()$ for all $\pi \neq \mathrm{id}$, implying that φ is injective. Moreover, if $\pi \in \mathcal{I}$ has order 5 or 3 then $\varphi(\pi) \in \mathcal{S}_5$ necessarily is a 5-cycle or 3-cycle, respectively, hence we have $\mathrm{sgn}(\varphi(\pi)) = 1$; if $\tau \in \mathcal{I}$ has order 2, thus is a rotation associated with one of the sets $\mathcal{T}_j$, the orthogonality property again implies that $\varphi(\tau) \in \mathcal{S}_5$ has precisely one fixed-point, hence is a **double transposition**, thus we have $\mathrm{sgn}(\varphi(\tau)) = 1$; this implies that $\varphi(\mathcal{I}) \leq \mathcal{A}_5$. ♯

Indeed, we have $|\mathrm{Stab}_{\mathcal{I}}(\mathcal{T}_5)| = \frac{|\mathcal{I}|}{5} = 12$. Letting $\tau_i \in \mathcal{I}$, for $i \in \{1, \ldots, 3\}$, be the rotations associated with $\mathcal{T}_5$, then $\tau_3 = \tau_1\tau_2$ implies that we get an abelian subgroup $V_4 \cong \mathcal{V} := \langle \tau_1, \tau_2 \rangle \leq \mathrm{Stab}_{\mathcal{I}}(\mathcal{T}_5)$ of order 4; where $\varphi(\mathcal{V}) = V_4 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \leq \mathcal{S}_4$ denotes the **Klein 4-group**. Moreover, there are precisely 4 rotation axes of order 3 whose associated rotations permute the elements of $\mathcal{T}_5$, hence letting $\rho \in \mathcal{I}$ be one of these rotations, by Lagrange's Theorem we get $\mathrm{Stab}_{\mathcal{I}}(\mathcal{T}_5) = \langle \tau_1, \tau_2, \rho \rangle$, where we may assume that $\varphi(\rho) = (1,2,3)$, and thus $\varphi(\mathrm{Stab}_{\mathcal{I}}(\mathcal{T}_5)) = \langle (1,2)(3,4), (1,2,3) \rangle = \mathcal{A}_4$.

(1.15) Finite subgroups of $\mathbf{O}_2(\mathbb{R})$. a) We first describe the elements of $O_2(\mathbb{R})$; recall that $\mathrm{SO}_2(\mathbb{R}) \trianglelefteq O_2(\mathbb{R})$ is a normal subgroup of index 2: Given $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O_2(\mathbb{R})$, from $E_2 = A^{\mathrm{tr}}A = \begin{bmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{bmatrix} \in \mathbb{R}^{2\times 2}$ we infer $a^2 + c^2 = 1 = b^2 + d^2$, hence there is a unique $0 \leq \alpha < 2\pi$ such that $[a,c]^{\mathrm{tr}} = [\cos\alpha, \sin\alpha]^{\mathrm{tr}}$, and from $ab + cd = 0$ we get $[b,d]^{\mathrm{tr}} = \pm[-c,a]^{\mathrm{tr}}$.

Hence in the '+' case we get $A = A_\alpha := \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \in \mathrm{SO}_2(\mathbb{R})$, a rotation with angle α. Extending this notation to allow for all $\alpha \in \mathbb{R}$, we have $A_\alpha = E_2$ if and only if $\alpha \in 2\pi\mathbb{Z}$. Then, by symmetry properties and addition theorems of trigonometric functions, we have $A_\alpha^{-1} = A_\alpha^{\mathrm{tr}} = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = A_{-\alpha}$, and for $\beta \in \mathbb{R}$ we get $A_\alpha A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\sin\alpha\cos\beta - \cos\alpha\sin\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix} = A_{\alpha+\beta}$. In particular, we infer that A_α has finite order if and only if $\alpha \in 2\pi\mathbb{Q}$. Note that A_α has characteristic polynomial $X^2 - 2\cos\alpha \cdot X + 1 \in \mathbb{R}[X]$, which does not have any roots in $\mathbb{R}$ unless $\alpha \in \pi\mathbb{Z}$, so that A_α does not have any eigenvector, apart from the cases $A_0 = E_2$ and $A_\pi = -E_2$.

In the '$-$' case we get $A = \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix} \in O_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$, having characteristic polynomial $X^2 - 1 = (X-1)(X+1) \in \mathbb{R}[X]$. Hence for $\alpha \notin \pi\mathbb{Z}$ we find $[\sin\alpha, 1-\cos\alpha]^{\mathrm{tr}} \in \mathbb{R}^{2\times 1}$ and $[\sin\alpha, -1-\cos\alpha]^{\mathrm{tr}} \in \mathbb{R}^{2\times 1}$ as eigenvectors of A with respect to the eigenvalues 1 and -1, respectively. Taking lengths into account, for all $\alpha \in \mathbb{R}$ we get $v_1 := [\cos\frac{\alpha}{2}, \sin\frac{\alpha}{2}]^{\mathrm{tr}}$ and $v_{-1} := [\sin\frac{\alpha}{2}, -\cos\frac{\alpha}{2}]^{\mathrm{tr}}$, where $\langle v_1, v_1 \rangle = 1 = \langle v_{-1}, v_{-1} \rangle$, and $\langle v_1, v_{-1} \rangle = \langle Av_1, v_{-1} \rangle = \langle v_1, A^{-1}v_{-1} \rangle = -\langle v_1, v_{-1} \rangle$, thus $\langle v_1, v_{-1} \rangle = 0$. Hence $\{v_1, v_{-1}\}$ is an orthonormal $\mathbb{R}$-basis of $\mathbb{R}^{2\times 1}$, giving rise to an orthogonal base change matrix P such that ${}^{P}A = \mathrm{diag}[1, -1] \in \mathbb{R}^{2\times 2}$, thus A is a reflection with respect to the axis $\langle v_1 \rangle_{\mathbb{R}}$; note that this is the principal axes transformation of the symmetric matrix A.

In conclusion, we have $\mathrm{SO}_2(\mathbb{R}) = \{A_\alpha \in O_2(\mathbb{R}); 0 \leq \alpha < 2\pi\}$ and $O_2(\mathbb{R}) = B \cdot \mathrm{SO}_2(\mathbb{R})$, where $B \in O_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$ is any reflection. Thus $\mathrm{SO}_2(\mathbb{R})$ is abelian, and multiplication in $O_2(\mathbb{R})$ is determined by writing ${}^{B}(A_\alpha)$ as a rotation A_β again. The latter is independent of the reflection chosen, and for

$B := \operatorname{diag}[1, -1]$ we get ${}^B(A_\alpha) = BA_\alpha B = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} = A_{-\alpha} = A_\alpha^{-1}$; in particular, $O_2(\mathbb{R})$ is non-abelian.

b) Let $G \leq \mathrm{SO}_2(\mathbb{R})$ be finite. Then, assuming that $G \neq \{1\}$, let $E_2 \neq A_\alpha \in G$ such that $0 < \alpha = \frac{2\pi k}{n} < 2\pi$ is the smallest non-trivial rotation angle occurring amongst the elements of G, where $n \in \mathbb{N}$ and $k \in \{0, \ldots, n-1\}$. We may assume that $\gcd(k, n) = 1$, hence there is $i \in \mathbb{Z}$ such that $ik \equiv 1 \pmod{n}$, implying that $A_\alpha^i = A_{\frac{2\pi}{n}} \in G$. Thus by the choice of α we have $\alpha = \frac{2\pi}{n}$, and hence $\langle A_{\frac{2\pi}{n}} \rangle \leq G$ is a cyclic group of order n. Now let $E_2 \neq A_{\frac{2\pi l}{m}} \in G$, and by the choice of α let $k \in \mathbb{N}$ be maximal such that $\frac{2\pi k}{n} \leq \frac{2\pi l}{m}$. Then we have $A_{\frac{2\pi l}{m}} A_{\frac{2\pi}{n}}^{-k} = A_{\frac{2\pi l}{m} - \frac{2\pi k}{n}} \in G$, where by the choice of k we have $0 \leq \frac{2\pi l}{m} - \frac{2\pi k}{n} < \frac{2\pi}{n}$, which by the choice of α implies $\frac{2\pi l}{m} - \frac{2\pi k}{n} = 0$, thus $A_{\frac{2\pi l}{m}} \in \langle A_{\frac{2\pi}{n}} \rangle$. Hence we have $G = \langle A_{\frac{2\pi}{n}} \rangle$ and thus $G = \mathcal{C}_n$ is cyclic, using the notation of (1.12), where for any $n \in \mathbb{N}$ there actually is a unique subgroup of order n.

Now let $G \leq O_2(\mathbb{R})$ be finite such that $G \not\leq \mathrm{SO}_2(\mathbb{R})$. Then $G' := G \cap \mathrm{SO}_2(\mathbb{R})$ is a normal subgroup of G of index 2, and by the above $G' = \langle A \rangle$ is cyclic of some order $n \in \mathbb{N}$, where $A := A_{\frac{2\pi}{n}}$. Moreover, there is a reflection $B \in G \setminus G'$, hence we have $G = \langle A, B \rangle = \{A^i B^j \in O_2(\mathbb{R}); i \in \{0, \ldots, n-1\}, j \in \{0, 1\}\}$, where multiplication in G by the above is given by ${}^B A = A^{-1}$. Hence we infer that G is conjugate in $O_2(\mathbb{R})$, that is up to choosing an orthonormal $\mathbb{R}$-basis of $\mathbb{R}^{2\times 1}$, to the subgroup $\langle A_{\frac{2\pi}{n}}, \operatorname{diag}[1, -1] \rangle$. Hence for $n \geq 3$ we recover a conjugate of the dihedral group $\mathcal{D}_n$ of order $2n$, using the notation of (1.12), where for any $n \geq 3$ there actually is a subgroup of order $2n$. For $n = 2$ the group G is conjugate to $\langle -E_2, \operatorname{diag}[1, -1] \rangle$, thus is isomorphic to the Klein 4-group V_4; and for $n = 1$ the group G is conjugate $\langle \operatorname{diag}[1, -1] \rangle$, a cyclic group of order 2.

(1.16) Finite subgroups of $\mathbf{SO}_3(\mathbb{R})$. a) We restrict ourselves to the group of rotations in Euclidean space $\mathbb{R}^{3\times 1}$, and first describe its elements: Let $A \in \mathrm{SO}_3(\mathbb{R})$. Its characteristic polynomial in $\mathbb{R}[X]$ having degree 3, we infer that there is a real eigenvalue $\lambda_0 \in \mathbb{R}$. Letting $\lambda_1, \lambda_2 \in \mathbb{C}$ be the further roots of the characteristic polynomial, we either have $\lambda_2 = \overline{\lambda_1} \in \mathbb{C} \setminus \mathbb{R}$ or $\lambda_1, \lambda_2 \in \mathbb{R}$; in particular, we have $1 = \det(A) = \lambda_0 \lambda_1 \lambda_2$. If $v \in \mathbb{R}^{3\times 1}$ is an eigenvector of A with respect to some eigenvalue $\lambda \in \mathbb{R}$, then we have $\langle v, v \rangle = \langle Av, Av \rangle = \lambda^2 \cdot \langle v, v \rangle$, implying that $\lambda \in \{\pm 1\}$. Thus, in the first case from $\lambda_1 \lambda_2 = |\lambda_1|^2 > 0$ we infer that $\lambda_0 = 1$ and $|\lambda_1| = |\lambda_2| = 1$; and in the second case up to reordering we have $\lambda_0 = 1$ and $[\lambda_1, \lambda_2] = \pm[1, 1]$. Hence in any case we may assume that $\lambda_0 = 1$.

Now let $v \in \mathbb{R}^{3\times 1}$ be a fixed vector of A, that is an eigenvector with respect to the eigenvalue $\lambda_0 = 1$, chosen to be of unit length, that is $\langle v, v \rangle = 1$, and let $U := \langle v \rangle_{\mathbb{R}}^{\perp} \leq \mathbb{R}^{3\times 1}$ be the orthogonal complement of $\langle v \rangle_{\mathbb{R}} \leq \mathbb{R}^{3\times 1}$. Then, for $u \in U$ we have $\langle Au, v \rangle = \langle u, A^{-1}v \rangle = \langle u, v \rangle = 0$, thus A leaves the orthogonal decomposition $\mathbb{R}^{3\times 1} = \langle v \rangle_{\mathbb{R}} \oplus U$ invariant. Moreover, A induces an orthogonal map on U, whose eigenvalues are λ_1 and λ_2, thus $\det(A|_U) = \lambda_1 \lambda_2 = 1$ says that $A|_U$ is a rotation in the Euclidean plane $U \cong \mathbb{R}^{2\times 1}$.

Thus geometrically A is a rotation of some angle $0 \leq \alpha < 2\pi$ with respect to the axis $\langle v\rangle_{\mathbb{R}}$. Hence choosing an orthonormal $\mathbb{R}$-basis $\{v_1, v_2\} \subseteq U$, with respect to the orthonormal $\mathbb{R}$-basis $\{v, v_1, v_2\} \subseteq \mathbb{R}^{3\times 1}$ we get $A = \mathrm{diag}[1, A_\alpha]$. Thus we have proved **Euler's Theorem**, saying that A is determined by a fixed vector v of unit length and a rotation angle α. Since A_α has a real eigenvalue if and only if $\alpha \in \pi\mathbb{Z}$, that is $A_\alpha \in \{\pm E_2\}$, we conclude that for $A \neq E_3$ the Euler description $[v, \alpha]$ of A is unique up to a sign; in particular, E_3 is the only element of $\mathrm{SO}_3(\mathbb{R})$ fixing a plane elementwise.

b) Next to the polyhedral subgroups of $\mathrm{SO}_3(\mathbb{R})$ already described in (1.14), we provide a few more finite subgroups. Subsequently, we proceed to prove (or at least to indicate) that this completes the list of all finite subgroups of $\mathrm{SO}_3(\mathbb{R})$, up to conjugacy, in particular implying that all these subgroups are rotational symmetry groups of regular polygons:

We have an injective homomorphism $O_2(\mathbb{R}) \to \mathrm{SO}(\mathbb{R})\colon B \mapsto \mathrm{diag}[\det(B), B]$. Hence, for any $n \in \mathbb{N}$ we get the cyclic group $\widehat{\mathcal{C}}_n := \langle \mathrm{diag}[1, A_{\frac{2\pi}{n}}]\rangle \leq \mathrm{SO}_3(\mathbb{R})$ of order n, which is the image of $\mathcal{C}_n \leq \mathrm{SO}_2(\mathbb{R})$, and the dihedral group $\widehat{\mathcal{D}}_n := \langle \mathrm{diag}[1, A_{\frac{2\pi}{n}}], \mathrm{diag}[-1, 1, -1]\rangle \leq \mathrm{SO}_3(\mathbb{R})$ of order $2n$, which for $n \geq 3$ is conjugate to the image of $\mathcal{D}_n \leq O_2(\mathbb{R})$, while $\widehat{\mathcal{D}}_2 = \langle \mathrm{diag}[1, -1, -1], \mathrm{diag}[-1, 1, -1]\rangle$ is isomorphic to V_4, and $\widehat{\mathcal{D}}_1 = \langle \mathrm{diag}[-1, 1, -1]\rangle$ is conjugate to $\widehat{\mathcal{C}}_2$.

Letting $n \geq 2$, the group $\widehat{\mathcal{C}}_n$ has a unique rotation axis, associated with n rotations of order dividing n. Moreover, $\widehat{\mathcal{D}}_n$ has a unique rotation axis associated with n rotations of order dividing n, being the images of the rotations in $\mathcal{D}_n$, as well as n rotation axes associated with n rotations of order 2, being the images of the reflections in $\mathcal{D}_n$.

c) Let $\{E_3\} \neq G \leq \mathrm{SO}_2(\mathbb{R})$ be finite. Let $\emptyset \neq \mathcal{V} \subseteq \mathbb{R}^{3\times 1}$ be the set of **poles** of G, that is the set of fixed vectors of unit length occurring in the Euler description of the non-trivial elements of G. Then G acts on $\mathcal{V}$: For $v \in \mathcal{V}$ there is $E_3 \neq A \in G$ such that $Av = v$, then for any $B \in G$ we have ${}^{B}A \neq E_3$ and ${}^{B}A \cdot Bv = Bv$, hence, since Bv has unit length, we conclude that $Bv \in \mathcal{V}$. Moreover, for $v \in \mathcal{V}$ the stabilizer $G_v = \{A \in G; Av = v\} \leq G$ is non-trivial; note that by the proof of Euler's Theorem G_v is isomorphic to a subgroup of $\mathrm{SO}_2(\mathbb{R})$, thus is cyclic.

We consider the set $\mathcal{X} := \{[A, v] \in G \times \mathcal{V}; A \neq E_3, Av = v\}$. We count $|\mathcal{X}|$ in two different ways: Firstly, since any $E_3 \neq A \in G$ has two fixed vectors in $\mathcal{V}$, we have $|\mathcal{X}| = 2(|G|-1)$. Secondly, since for any $v \in \mathcal{V}$ there are $|G_v|-1$ non-trivial elements of G keeping v fixed, we get $|\mathcal{X}| = \sum_{v\in\mathcal{V}}(|G_v|-1)$. Thus letting $\mathcal{S} \subseteq \mathcal{V}$ be a set of G-orbit representatives, and recalling that $|G_v| = \frac{|G|}{|Gv|}$ only depends on the G-orbit $v \in \mathcal{V}$ belongs to, this yields $|\mathcal{X}| = \sum_{v\in\mathcal{S}} |Gv| \cdot (|G_v| - 1) = |G| \cdot \sum_{v\in\mathcal{S}}(1 - \frac{1}{|G_v|})$. Combining the two expressions for $|\mathcal{X}|$, and dividing by $|G|$, we get $\frac{1}{2} \cdot |\mathcal{S}| \leq \sum_{v\in\mathcal{S}}(1 - \frac{1}{|G_v|}) = 2 - \frac{2}{|G|} < 2$, hence we conclude $|\mathcal{S}| \leq 3$.

Assume that $|\mathcal{S}| = 1$, then letting $\mathcal{S} = \{v\}$ we have $1 - \frac{1}{|G_v|} = 2 - \frac{2}{|G|}$, thus $|G| = 2 - \frac{|G|}{|G_v|} < 2$, a contradiction. Hence we have $|\mathcal{S}| \in \{2, 3\}$. Let first $|\mathcal{S}| = 2$, and $\mathcal{S} = \{v, w\}$. Then we have $\frac{1}{|G_v|} + \frac{1}{|G_w|} = \frac{2}{|G|}$. Since $|G_v|, |G_w| \mid |G|$ this implies $|G_v| = |G_w| = |G|$, and thus $|Gv| = |Gw| = 1$, hence $|\mathcal{V}| = 2$.

Let now $|\mathcal{S}| = 3$, and $\mathcal{S} = \{u, v, w\}$. Then we have $\frac{1}{|G_u|} + \frac{1}{|G_v|} + \frac{1}{|G_w|} = 1 + \frac{2}{|G|}$. Assume that $|G_u|, |G_v|, |G_w| \geq 3$, then we get $1 + \frac{2}{|G|} \leq 1$, a contradiction. Hence we may assume that $|G_w| = 2$, yielding $\frac{1}{|G_u|} + \frac{1}{|G_v|} = \frac{1}{2} + \frac{2}{|G|}$. Assume that $|G_u|, |G_v| \geq 4$, then we get $\frac{1}{2} + \frac{2}{|G|} \leq \frac{1}{2}$, a contradiction. Hence, assuming that $|G_u| \geq |G_v|$, we have $|G_v| \leq 3$. Let first $|G_v| = 2$, then we get $|G_u| = \frac{|G|}{2}$, and thus $|Gv| = |Gw| = \frac{|G|}{2}$ and $|Gu| = 2$, hence $|\mathcal{V}| = |G| + 2$; note that $|\mathcal{V}| \leq 2(|G| - 1)$ implies $|G| \geq 4$.

Let now $|G_v| = 3$, then we get $\frac{1}{|G_u|} = \frac{1}{6} + \frac{2}{|G|} > \frac{1}{6}$, hence $|G_u| \in \{3, 4, 5\}$. In these cases, if $|G_u| = 3$ we get $|G| = 12$, and thus $|Gw| = 6$, $|Gv| = 4$ and $|Gu| = 4$, hence $|\mathcal{V}| = 14$; if $|G_u| = 4$ we get $|G| = 24$, and thus $|Gw| = 12$, $|Gv| = 8$ and $|Gu| = 6$, hence $|\mathcal{V}| = 26$; if $|G_u| = 5$ we get $|G| = 60$, and thus $|Gw| = 30$, $|Gv| = 20$ and $|Gu| = 12$, hence $|\mathcal{V}| = 62$.

Hence we have the following five cases, where $n \geq 2$:

$\lvert G\rvert$	$\lvert\mathcal{V}\rvert$	$\lvert\mathcal{S}\rvert$	$\lvert Gw\rvert$	$\lvert G_w\rvert$	$\lvert Gv\rvert$	$\lvert G_v\rvert$	$\lvert Gu\rvert$	$\lvert G_u\rvert$	G
n	2	2	1	n	1	n			$\widehat{\mathcal{C}}_n \cong C_n$
$2n$	$2n+2$	3	n	2	n	2	2	n	$\widehat{\mathcal{D}}_n \cong D_{2n}$
12	14	3	6	2	4	3	4	3	$\mathcal{T} \cong \mathcal{A}_4$
24	26	3	12	2	8	3	6	4	$\mathcal{H} \cong \mathcal{S}_4$
60	62	3	30	2	20	3	12	5	$\mathcal{I} \cong \mathcal{A}_5$

(1.17) Theorem: Classification of finite subgroups of $\mathbf{SO}_3(\mathbb{R})$. Let G be a finite subgroup of the special orthogonal group $\mathrm{SO}_3(\mathbb{R})$. Then G is conjugate to precisely one of the following groups:

i) the cyclic group $\widehat{\mathcal{C}}_n$, for $n \in \mathbb{N}$, **ii)** the dihedral group $\widehat{\mathcal{D}}_n$, for $n \geq 2$, **iii)** the tetrahedral group $\mathcal{T}$, **iv)** the hexahedral group $\mathcal{H}$, **v)** the icosahedral group $\mathcal{I}$.

Proof. The finite subgroups given in the assertion have been described in (1.14) and (1.16); in particular the number of rotation axes of a given order is as follows:

G	$\lvert G\rvert$	2	3	4	5	n
$\widehat{\mathcal{C}}_n$	n					1
$\widehat{\mathcal{D}}_n$	$2n$	n				1
$\mathcal{T}$	12	3	4			
$\mathcal{H}$	24	6	4	3		
$\mathcal{I}$	60	15	10		6	

This shows that they match up with the cases listed in the table preceding the statement of the theorem as indicated; note that $D_4 := V_4$. It also follows that these cases are mutually disjoint. We have already shown that G belongs to one of these cases, hence it remains to be shown that the geometrical data determines G up to conjugacy. We give a sketch; for more details see [4, Ch.15]:

In the first case, G has a unique rotation axis, thus all elements of G are of the form $\mathrm{diag}[1, B]$, where $B \in \mathrm{SO}_3(\mathbb{R})$, hence G is conjugate to $\widehat{\mathcal{C}}_n$, where $n := |G|$.

In the second case, if $|G| = 2n \geq 6$, then G has a unique rotation axis $\langle v\rangle_{\mathbb{R}}$ associated with rotations of order n, and has an element mapping $v \mapsto -v$, which thus leaves $\langle v\rangle_{\mathbb{R}}^{\perp} \leq \mathbb{R}^{3\times 1}$ invariant; hence G is conjugate to $\widehat{\mathcal{D}}_n$. If $|G| = 4$, then G has three rotation axes associated with rotations of order 2; hence the latter are mutually orthogonal, implying that G is conjugate to $\widehat{\mathcal{D}}_2$.

In the third case, G has 4 rotation axes $\langle v_i\rangle_{\mathbb{R}}$, for $i \in \{1, \ldots, 4\}$, associated with rotations of order 3. Letting $\{v_1, \ldots, v_4\}$ be a single G-orbit, the stabilizer $\mathrm{Stab}_G(v_4)$, being of order 3, permutes $\{v_1, v_2, v_3\}$ transitively. It follows that $\langle v_i, v_j\rangle$ has the same value, for all $i \neq j \in \{1, \ldots, 4\}$, thus $\{v_1, \ldots, v_4\}$ forms a tetrahedron, implying that G is conjugate to $\mathcal{T}$.

In the fourth case, G has 3 rotation axes $\langle v_i\rangle_{\mathbb{R}}$, for $i \in \{1, 2, 3\}$, associated with rotations of order 4. Letting $\{\pm v_1, \pm v_2, \pm v_3\}$ be the associated G-orbit, the stabilizer $\mathrm{Stab}_G(v_3)$, being cyclic of order 4, fixes $-v_3$ as well, and permutes $\{\pm v_1, \pm v_2\}$ transitively. It follows that $\langle v_i, v_j\rangle = 0$, for all $i \neq j \in \{1, 2, 3\}$, thus $\{\pm v_1, \pm v_2, \pm v_3\}$ forms an octahedron, implying that G is conjugate to $\mathcal{H}$.

In the fifth case, which is the most complicated, G has 6 rotation axes $\langle v_i\rangle_{\mathbb{R}}$, for $i \in \{1, \ldots, 6\}$, associated with rotations of order 5. Let $\{\pm v_1, \ldots, \pm v_6\}$ be the associated G-orbit, and call $v \neq w \in \{\pm v_1, \ldots, \pm v_6\}$ adjacent, if $\langle v, w\rangle$ is maximal. Note that, since we have more than 6 vectors, if v and w are adjacent then we have $\langle v, w\rangle > 0$; in particular v is never adjacent to both w and $-w$.

Assume that v_6 is adjacent to v_1, then the stabilizer $\mathrm{Stab}_G(v_6)$, being cyclic of order 5, fixes $-v_6$ as well, and we may assume that it induces the 5-cycles $(v_1, \ldots, v_5)$ and $(-v_1, \ldots, -v_5)$ on $\{\pm v_1, \ldots, \pm v_5\}$; thus $-v_6$ is adjacent to $\{-v_1, \ldots, -v_5\}$. Then v_1 is not adjacent to v_3 and v_4. Assume that v_1 is not adjacent to v_2, hence also neither to v_5; then v_1 is adjacent to $\{-v_2, \ldots, -v_5, v_6\}$, and v_2 is adjacent to $\{-v_1, -v_3, -v_4, -v_5, v_6\}$; since both of these form a pentagon, their intersection being $\{-v_3, -v_4, -v_5, v_6\}$ implies that these pentagons coincide, contradicting the fact that $v_1 \neq v_2$.

Hence v_1 is adjacent to both v_2 and v_5. We infer that, for $i \in \{1, \ldots, 5\}$, the stabilizer $\mathrm{Stab}_G(v_i)$ induces the 5-cycle $(v_6, v_5, -v_3, -v_4, v_2)$, $(v_6, v_1, -v_4, -v_5, v_3)$, $(v_6, v_2, -v_5, -v_1, v_4)$, $(v_6, v_3, -v_1, -v_2, v_5)$, $(v_6, v_4, -v_2, -v_3, v_1)$ of neighbors of v_i, respectively. Hence these form a total of $\frac{12\cdot 5}{3} = 20$ regular triangles, thus $\{\pm v_1, \ldots, \pm v_6\}$ forms an icosahedron, implying that G is conjugate to $\mathcal{I}$. $\sharp$

(1.18) Example: Coloring problems. In combinatorics, group actions can be used to count the number of 'configurations' up to certain symmetry operations. More formally, the set of admissible 'configurations' is considered to be acted on by a suitable symmetry group, whence the relevant equivalence classes are just the orbits with respect to this action. We consider the following situation, which is only the starting point of so-called **Polya Theory**:

Given $n \in \mathbb{N}$ and $k \in \mathbb{N}$, let $\mathcal{M}_{n,k}$ be the set of all maps $f\colon \{1,\ldots,n\} \to \{1,\ldots,k\}$; in more combinatorial terms, $\mathcal{M}_{n,k}$ can be viewed as the set of all possible **colorings** of n objects with at most k colors. Then $\mathcal{S}_n$ acts on $\mathcal{M}_{n,k}$ by **pre-multiplication** $f \mapsto \pi(f) := f\pi^{-1}$, for all $\pi \in \mathcal{S}_n$: Indeed, we have $\mathrm{id}(f) = f$, and for $\pi, \rho \in \mathcal{S}_n$ we have $(\pi\rho)(f)\colon i \mapsto f(\pi\rho)^{-1}(i) = f\rho^{-1}\pi^{-1}(i) = \rho(f)(\pi^{-1}(i)) = \pi(\rho(f))(i)$, for all $i \in \{1,\ldots,n\}$, saying that $(\pi\rho)(f) = \pi(\rho(f))$. Note that, upon identifying f with the tuple $[f(1),\ldots,f(n)]$, $\mathcal{S}_n$ acts by **reordering** the entries.

Hence, given $G \leq \mathcal{S}_n$, the number $|G\backslash\mathcal{M}_{n,k}|$ of G-orbits on $\mathcal{M}_{n,k}$ can be determined by applying the Cauchy-Frobenius-Burnside Lemma: We observe that for $\pi \in \mathcal{S}_n$ and $f \in \mathcal{M}_{n,k}$ we have $\pi(f) = f$ if and only if $f\pi^{-1}(i) = f(i)$ for all $i \in \{1,\ldots,n\}$, which holds if and only if f is constant on the cycles of π; thus we have $|\mathrm{Fix}_{\mathcal{M}_{n,k}}(\pi)| = k^r$, where $r \in \mathbb{N}$ is the number of cycles of π.

a) A **necklace** with $n \geq 3$ pearls having k possible colors is just a map in $\mathcal{M}_{n,k}$, where the set $\{1,\ldots,n\}$ is considered as the set of vertices of a regular n-gon $\mathbb{D}_n$, and necklaces are equivalent if they arise from each other by a symmetry of $\mathbb{D}_n$. Hence the number of equivalence classes is given as the number $t_{n,k} = |D_{2n}\backslash\mathcal{M}_{n,k}| \in \mathbb{N}$ of D_{2n}-orbits in $\mathcal{M}_{n,k}$. Thus $t_{n,k}$ can be determined, using the cycle types of the elements of D_{2n} to count their fixed points in $\mathcal{M}_{n,k}$, by applying the Cauchy-Frobenius-Burnside Lemma.

For example, for $n = 3$ and $n = 4$ we 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 $t_{4,k} = \frac{1}{8} \cdot (k^4 + 2k^3 + 3k^2 + 2k) = \frac{1}{8} \cdot k(k+1)(k^2+k+2)$:

$\pi \in D_6$	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

b) We consider the possible colorings of the vertices $\{1,\ldots,4\}$ of the tetrahedron $\mathbb{T}$ with at most $k = 4$ colors, that is the set of maps in $\mathcal{M}_{4,4}$, being acted on by the polyhedral groups $\widetilde{\mathcal{T}} \cong \mathcal{S}_4$ and $\mathcal{T} \cong \mathcal{A}_4$. Hence the number of equivalence classes, with respect to rotations and reflections, and with respect to rotations alone, is given as $|\mathcal{S}_4\backslash\mathcal{M}_{4,4}| \in \mathbb{N}$ and $|\mathcal{A}_4\backslash\mathcal{M}_{4,4}| \in \mathbb{N}$, respectively. In order to determine these numbers, we collect the cycle types of the elements of $\mathcal{S}_4$, the former three types constituting those belonging to $\mathcal{A}_4$, together with their frequency of occurrence:

card.	type	r
8	$[3,1]$	2
3	$[2^2]$	2
1	$[1^4]$	4
6	$[4]$	1
6	$[2,1^2]$	3

From this, counting fixed points in $\mathcal{M}_{4,4}$ and applying the Cauchy-Frobenius-Burnside Lemma, we get $|\mathcal{S}_4\backslash\mathcal{M}_{4,4}| = \frac{1}{24}\cdot(8\cdot 4^2+3\cdot 4^2+1\cdot 4^4+6\cdot 4^1+6\cdot 4^3) = 35$ and $|\mathcal{A}_4\backslash\mathcal{M}_{4,4}| = \frac{1}{12}\cdot(8\cdot 4^2+3\cdot 4^2+1\cdot 4^4) = 36$. Since the $\mathcal{S}_4$-orbits in $\mathcal{M}_{4,4}$ are unions of $\mathcal{A}_4$-orbits, the above result implies that there is precisely one $\mathcal{S}_4$-orbit in $\mathcal{M}_{4,4}$ which splits into two $\mathcal{A}_4$-orbits. Actually, it is given as follows:

Let $f = [1,2,3,4] \in \mathcal{M}_{4,4}$, which is a coloring where all 4 possible colors actually occur. Then we have $\text{Stab}_{\mathcal{S}_4}(f) = \{()\}$, thus $\mathcal{S}_4$ acts regularly on the associated $\mathcal{S}_4$-orbit of length 24, which hence consists of all surjective, that is bijective maps. Similarly, $\text{Stab}_{\mathcal{A}_4}(f) = \{()\}$ implies that $\mathcal{A}_4$ acts regularly on the associated $\mathcal{A}_4$-orbit of length 12. Moreover, letting $f' := (1,2)\cdot f = [2,1,3,4]$, from $\mathcal{S}_4 = \mathcal{A}_4 \,\dot\cup\, \mathcal{A}_4\cdot(1,2)$ we get $\mathcal{S}_4\cdot f = \mathcal{A}_4\cdot f \,\dot\cup\, \mathcal{A}_4\cdot f'$, This phenomenon is known to chemists as **chirality**.

2 Rings

(2.1) Commutative rings. a) A set R together with an addition $+\colon R\times R\to R$ and a multiplication $\cdot\colon R\times R\to R$ fulfilling the following conditions is called a **commutative ring**:
i) With respect to addition R is a commutative group with neutral element 0;
ii) with respect to multiplication R is a commutative **monoid**, that is we have associativity and commutativity, and there is a neutral element 1;
iii) and we have **distributivity** $a(b+c) = ab+ac$, for all $a,b,c\in R$.

We derive a few immediate consequences: We have $0\cdot a = 0$ and $(-1)\cdot a = -a$, as well as $(-a)b = -(ab)$, for all $a,b\in R$: From $0+0=0$ we get $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$ and hence $0\cdot a = 0$; we have $(-1)\cdot a + a = (-1)\cdot a + 1\cdot a = (-1+1)\cdot a = 0\cdot a = 0$, hence $(-1)\cdot a = -a$; thus we have $-(ab) = (-1)\cdot ab = (-a)b$.

A subset $S\subseteq R$ being an additive subgroup, containing 1 and being closed closed with respect to multiplication is called a **subring**; then S is again a ring.

Letting S be a commutative ring, a map $\varphi\colon R\to S$ is called a **(ring) homomorphism**, if $\varphi(1_R) = 1_S$ and $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$, for all $a,b\in R$. Note that from $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$ we get $\varphi(0) = 0$; and hence from $\varphi(1)+\varphi(-1) = \varphi(1-1) = \varphi(0) = 0$ we get $\varphi(-1) = -\varphi(1)$, and thus $\varphi(-a) = \varphi((-1)\cdot a) = (-1)\cdot\varphi(a) = -\varphi(a)$, for all $a\in R$.

For example, $R := \{0\}$ with addition $0 + 0 = 0$ and multiplication $0 \cdot 0 = 0$, hence $1 := 0$, is a commutative ring, called the **zero ring**; note that conversely, if R fulfills $1 = 0$, then $a = a \cdot 1 = a \cdot 0 = 0$, for all $a \in R$, hence $R = \{0\}$.

b) Let $R \neq \{0\}$. Then let $R^* \subseteq R$ be the set of all $a \in R$ having an **inverse** $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$; hence R^* becomes a commutative multiplicative group with neutral element 1, being called the **group of units** of R. The latter can be characterized as follows: For $a \in R$ the map $\lambda_a \colon R \to R \colon x \mapsto ax$ is surjective if and only if $a \in R^*$: If λ_a is surjective, then there is $b \in R$ such that $ab = 1$, hence $a \in R^*$; if $a \in R^*$, then for all $x \in R$ we have $x = aa^{-1}x = \lambda_a(a^{-1}x)$, hence λ_a is surjective.

Note that $0 \notin R^*$: Assume that $0 \in R^*$, then $1 = 0 \cdot 0^{-1} = 0$, a contradiction. If $R^* = R \setminus \{0\}$, then R is called a **field**; a subring $S \subseteq R$ of a field R, such that for all $0 \neq a \in S$ we have $a^{-1} \in S$, is called **subfield**, then S is again a field.

An element $0 \neq a \in R$ such that $ab = 0$ for some $0 \neq b \in R$ is called a **zero-divisor**. The latter can be characterized as follows: For $0 \neq a \in R$ the map $\lambda_a \colon R \to R \colon x \mapsto ax$ is injective if and only if a is not a zero-divisor: If λ_a is injective, then $ax = 0 = a \cdot 0$ implies $x = 0$, for all $x \in R$, thus a is not a zero-divisor; if a is not a zero-divisor, then $ax = ax'$, where $x, x' \in R$, implies $a(x - x') = 0$ and thus $x = x'$, hence λ_a is injective.

If there are no zero-divisors, that is for all $a, b \neq 0$ we have $ab \neq 0$, then R is called an **integral domain**; note that in integral domain we have a **cancellation law** saying that for $0 \neq a \in R$ we have $ab = ac \in R$ if and only if $b = c$. Moreover, units are not zero-divisors; in particular, any field is an integral domain: Assume that for $a \in R^*$ there is $0 \neq b \in R$ such that $ab = 0$, then we have $0 = a^{-1} \cdot 0 = a^{-1} \cdot ab = 1 \cdot b = b$, a contradiction.

Here finally are the prototypical examples: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are integral domains, where we have $\mathbb{Z}^* = \{\pm 1\}$, while $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are fields; note that neither $\mathbb{N}$ nor $\mathbb{N}_0$ are even rings.

(2.2) Residue class rings. For $n \in \mathbb{N}$ the associated **congruence relation** is defined as $R_n := \{[a, b] \in \mathbb{Z}^2; a \equiv b \pmod{n}\} = \{[a, b] \in \mathbb{Z}^2; n \mid (a - b)\}$. Since $n \mid 0 = (a - a)$, and $n \mid (-a)$ whenever $n \mid a$, and from $n \mid (a - b)$ and $n \mid (b - c)$ get $n \mid (a - b) + (b - c) = (a - c)$ as well, for all $a, b, c \in \mathbb{Z}$, we infer that R_n is reflexive, symmetric and transitive, thus is an equivalence relation on $\mathbb{Z}$. The associated equivalence classes $[a]_n = \{a + kn \in \mathbb{Z}; k \in \mathbb{Z}\} \subseteq \mathbb{Z}$, for $a \in \mathbb{Z}$, are called **congruence classes** modulo n.

Let $\mathbb{Z}_n := \{0, \ldots, n-1\}$, and let $\overline{} \colon \mathbb{Z} \to \mathbb{Z}_n$ be defined by letting $\overline{a} \in \mathbb{Z}_n$ be the **remainder** of $a \in \mathbb{Z}$ upon division by n. Hence we have $[a]_n \cap \mathbb{Z}_n = \{\overline{a}\}$, for all $a \in \mathbb{Z}$, implying that there are precisely n congruence classes $\{[0]_n, \ldots, [n-1]_n\}$, which are thus also called **residue classes** modulo n; for example, for $n = 2$ these are $[0]_2 = \{0, 2, -2, 4, -4, \ldots\}$ and $[1]_2 = \{1, -1, 3, -3, \ldots\}$, that is the even and odd integers, respectively. We proceed to develop an arithmetic on the set of residue classes modulo n, where in order to do so we henceforth just identify the latter with the set $\mathbb{Z}_n$:

b) We define an addition $+\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ and a multiplication $\cdot\colon \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ by $a + b := \overline{a+b}$ and $a \cdot b := \overline{ab}$; in other words addition and multiplication are inherited from $\mathbb{Z}$, by adding respectively multiplying in $\mathbb{Z}$ first, and subsequently taking remainders upon division by n. We show that with respect to these operations $\mathbb{Z}_n$ becomes a commutative ring, being called the associated **residue class ring**; in other words $^{-}\colon \mathbb{Z} \to \mathbb{Z}_n$ is a ring homomorphism:

We first show that the definition of addition and multiplication is independent of the choice of **representatives**: Let $a, a', b, b' \in \mathbb{Z}$ such that $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$. Hence there are $k, l \in \mathbb{Z}$ such that $a' = a + kn$ and $b' = b + ln$. Thus we have $a' + b' = (a + kn) + (b + ln) = (a + b) + (k + l)n$, implying $\overline{a' + b'} = \overline{a + b}$, as well as $a'b' = (a + kn)(b + ln) = ab + (al + bk + kln)n$, implying $\overline{a'b'} = \overline{ab}$.

Then associativity and distributivity follow from $\overline{(\overline{a+b}) + c} = \overline{a + b + c} = \overline{a + (\overline{b + c})}$ and $\overline{(\overline{a \cdot b}) \cdot c} = \overline{a \cdot b \cdot c} = \overline{a \cdot (\overline{b \cdot c})}$ and $\overline{a \cdot (\overline{b + c})} = \overline{a \cdot (b + c)} = \overline{(\overline{ab}) + (\overline{ac})}$, for all $a, b, c \in \mathbb{Z}_n$. Hence $\mathbb{Z}_n$ becomes a commutative additive group with neutral element $0 \in \mathbb{Z}_n$, the additive inverse of $a \in \mathbb{Z}_n$ being $\overline{-a} \in \mathbb{Z}_n$, where $\overline{-a} = n - a \in \mathbb{Z}_n$ for $a \neq 0$; and $\mathbb{Z}_n$ becomes a commutative multiplicative monoid, with neutral element $1 \in \mathbb{Z}_n$ for $n \geq 2$, while $\mathbb{Z}_1 = \{0\}$ anyway. ♯

For example, we consider the cases $p = 2, 3, 5$, and by way of comparison $n = 4$. Then addition and multiplication in $\mathbb{Z}_n$ are described as given below; note that the case $p = 2$ is reminiscent of boolean algebra, by identifying 0 and 1 with the logical values false and true, respectively, and '+' and '·' with the logical operations xor and and, respectively:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

c) Given $n \geq 2$, we show that $\mathbb{Z}_n$ is an integral domain if and only if n is a prime, in which case it is a field, being called the **finite (prime) field** of **order** n: If n is composite, then we have $n = ab$ for some $1 \neq a, b \in \mathbb{N}$, hence $a, b \neq 0 \in \mathbb{Z}_n$ but $ab = 0 \in \mathbb{Z}_n$, thus $a, b \in \mathbb{Z}_n$ are zero-divisors.

If n is a prime, we have to show that $\mathbb{Z}_n^* := \mathbb{Z}_n \setminus \{0\}$: Letting $0 \neq a \in \mathbb{Z}_n$, we first show that $\lambda_a\colon \mathbb{Z}_n \to \mathbb{Z}_n\colon x \mapsto ax$ is injective, that is a is not a zero-divisor:

Let $x, x' \in \mathbb{Z}_n$ such that $ax = ax' \in \mathbb{Z}_n$, hence we have $n \mid a(x - x') \in \mathbb{Z}$; thus, since n is a prime, we conclude that $n \mid a$ or $n \mid (x - x')$, or equivalently that $a = 0 \in \mathbb{Z}_n$ or $\overline{x - x'} = 0 \in \mathbb{Z}_n$; since $a \neq 0 \in \mathbb{Z}_n$, we infer $x = x' \in \mathbb{Z}_n$. Now, since $\mathbb{Z}_n$ is finite, we conclude that $\lambda_a \colon \mathbb{Z}_n \to \mathbb{Z}_n$ is surjective, hence $a \in \mathbb{Z}_n^*$. $\sharp$

Note that the above argument does not give a description of $\mathbb{Z}_n^*$ whenever n is composite, and only shows the existence of multiplicative inverses of all elements of $\mathbb{Z}_n \setminus \{0\}$ whenever n is a prime, but does not allow to compute them; we will come back to this in (2.10).

(2.3) Example: Fermat numbers. For $n \in \mathbb{N}_0$ let $F_n := 2^{2^n} + 1 \in \mathbb{N}$ be the n-th **Fermat number**, where $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$ are primes; it was conjectured [Fermat, 1640] that F_n always is a prime. But for $F_5 := 2^{2^5} + 1 = 4\,294\,967\,297 \sim 4 \cdot 10^9$ we have $F_5 = 641 \cdot 6\,700\,417$ [Euler, 1732]; nowadays all F_n for $n \in \{5, \ldots, 30\}$ are known to be composite, but it is still an open problem whether $\{F_0, \ldots, F_4\}$ are the only Fermat primes:

We have $641 = 640 + 1 = 5 \cdot 2^7 + 1 \in \mathbb{Z}$, thus $\overline{5 \cdot 2^7} = -\overline{1} \in \mathbb{Z}_{641}$, and $641 = 625 + 16 = 5^4 + 2^4 \in \mathbb{Z}$, thus $\overline{2}^4 = -\overline{5}^4 \in \mathbb{Z}_{641}$, hence $\overline{F_5} = \overline{2}^{32} + \overline{1} = \overline{2}^4\overline{2}^{28} + \overline{1} = -\overline{5 \cdot 2^7}^4 + \overline{1} = -(-\overline{1})^4 + \overline{1} = -\overline{1} + \overline{1} = \overline{0} \in \mathbb{Z}_{641}$. $\sharp$

(2.4) Divisibility. a) Let R be an integral domain. 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 $a \mid b$. Elements $a, b \in R$ are called **associate** if $a \mid b$ and $b \mid a$; we write $a \sim b$, where in particular $\sim$ is an equivalence relation on R.

Moreover, we have $a \sim b$ if and only if there is $u \in R^*$ such that $b = au \in R$: If $b = au$ then we also have $a = bu^{-1}$, thus $a \mid b$ and $b \mid a$; if conversely $a \mid b$ and $b \mid a$, then 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 $u, v \in R^*$.

Let $\emptyset \neq M \subseteq R$ be a subset. Then $d \in R$ such that $d \mid a$ for all $a \in M$ is called a **common divisor** of M; any $u \in R^*$ always is a common divisor of M. If for all common divisors $c \in R$ of M we have $c \mid d$, then $d \in R$ is called a **greatest common divisor** of M. Let $\gcd(M) \subseteq R$ be the set of all greatest common divisors of M. In general greatest common divisors do not exist; but if $\gcd(M) \neq \emptyset$ then, since for $d, d' \in \gcd(M)$ we have $d \mid d'$ and $d' \mid d$, it consists of a single associate class. 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**. Similarly, we get the notion and basic properties of **lowest common multiples** $\operatorname{lcm}(M) \subseteq R$.

b) Let $0 \neq a \in R \setminus R^*$. Then a is called **irreducible** or **indecomposable**, if $a = bc \in R$ implies $b \in R^*$ or $c \in R^*$; otherwise a is called **reducible** or **decomposable** or **composite**; hence if a is irreducible then all its associates also are. The element a is called a **prime**, if $a \mid bc \in R$ implies $a \mid b$ or $a \mid c$; hence if a is a prime then all its associates also are.

These notions are not independent, inasmuch if $a \in R$ is a prime, then it is irreducible as well: Let $a = bc$ for some $b, c \in R$, hence we may assume that $a \mid b$, thus there is $d \in R$ such that $ad = b$, hence $a = adc$, yielding $a(1-dc) = 0$, implying $c \in R^*$. But the converse does not hold in general, that is an irreducible element in general is not a prime:

c) It seems worth-while to have a closer look at the prototype integral domain $\mathbb{Z}$, taking the existence of greatest common divisors, as well as the equivalence of being irreducible and being a prime for granted, see (2.7). We recall the proof of the irrationality of $\sqrt{2} \in \mathbb{R}$, where the property of being a prime is used:

Assume to the contrary that $\sqrt{2} = \frac{a}{b} \in \mathbb{Q} \subseteq \mathbb{R}$, where we may assume additionally that $1 \in \gcd(a, b)$. Then we have $2b^2 = a^2 \in \mathbb{Z}$, hence $2 \mid a^2$, and since $2 \in \mathbb{Z}$ is a prime, we infer $2 \mid a$, which implies $2^2 \mid 2b^2$, thus $2 \mid b^2$, and hence $2 \mid b$ as well, a contradiction. $\sharp$

(2.5) Example: Irreducible vs. prime. We consider the integral domain $R := \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \in \mathbb{C}; a, b \in \mathbb{Z}\}$, a subring of $\mathbb{C}$. We have $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in R$. We show that $2 \in R$ is neither a unit, nor a prime, but is irreducible; similarly, $3 \in R$ and $1 \pm \sqrt{-5} \in R$ can be shown to have the same properties:

Assume that there are $a, b \in \mathbb{Z}$ such that $1 = 2 \cdot (a + b\sqrt{-5}) = 2a + 2b\sqrt{-5} \in R$, then we have $2a = 1$ and $b = 0$, a contradiction. Hence we have $2 \not\in R^*$.

Assume that there are $a, b \in \mathbb{Z}$ such that $1 + \sqrt{-5} = 2 \cdot (a + b\sqrt{-5}) = 2a + 2b\sqrt{-5} \in R$, then we have $2a = 1$ and $2b = 1$, a contradiction; similarly, assume that there are $a, b \in \mathbb{Z}$ such that $1 - \sqrt{-5} = 2 \cdot (a + b\sqrt{-5}) = 2a + 2b\sqrt{-5} \in R$, then we have $2a = 1$ and $2b = -1$, a contradiction. Hence we have $2 \nmid 1 \pm \sqrt{-5} \in R$, but $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) \in R$, thus $2 \in R$ is not a prime.

Finally, let $a, b, c, d, \in \mathbb{Z}$ such that $2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}$, thus we have $ac - 5bd = 2$ and $ad + bc = 0$. Assume that $b \neq 0$, then we get $c = -\frac{ad}{b}$, and thus $2 = -\frac{a^2d}{b} - 5bd$, hence $(a^2 + 5b^2)d = -2b$, which since $d \neq 0$ and $a^2 + 5b^2 \geq 5b^2 > |2b|$ is a contradiction. Hence we have $b = 0$, implying $ad = 0$ and $ac = 2$, thus $d = 0$ as well, and either $a = \pm 1$ or $c = \pm 1$, saying that one of the factors considered is in R^*. Hence $2 \in R$ is irreducible. $\sharp$

(2.6) Factorial domains. Let R be an integral domain. Then R is called **factorial** or a **Gaussian domain**, if any element $0 \neq a \in R$ can be written uniquely, up to reordering and taking associates, in the form $a = u \cdot \prod_{i=1}^n p_i \in R$, where the $p_i \in R$ are irreducible, $n \in \mathbb{N}_0$ and $u \in R^*$.

Let $\mathcal{P} \subseteq R$ be a set of representatives of the associate classes of irreducible elements of R; this exists by the Axiom of Choice. If R is factorial, then any $0 \neq a \in R$ has a unique **factorization** $a = u_a \cdot \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$, where $u_a \in R^*$ and $\nu_p(a) \in \mathbb{N}_0$ is called the associated **multiplicity**; we have $\nu_p(a) = 0$ for almost all $p \in \mathcal{P}$, thus $\sum_{p \in \mathcal{P}} \nu_p(a) \in \mathbb{N}_0$ is called the **length** of the factorization, and a is called **square-free** if $\nu_p(a) \leq 1$ for all $p \in \mathcal{P}$.

For any subset $\emptyset \neq M \subseteq R \setminus \{0\}$ we have $\prod_{p\in\mathcal{P}} p^{\min\{\nu_p(a);a\in M\}} \in \gcd(M)$, and if M is finite then we have $\prod_{p\in\mathcal{P}} p^{\max\{\nu_p(a);a\in M\}} \in \mathrm{lcm}(M)$. But note that in order to use this to compute greatest common divisors in practice, the relevant elements of R have to be factorized completely first.

If R is factorial, then any irreducible element $a \in R$ is a prime; thus in this case the irreducible elements and the primes of R indeed coincide: Let $0 \neq b, c \in R$ such that $a \mid bc$. Hence there is $d \in R$ such that $ad = bc = u \cdot \prod_{p\in\mathcal{P}} p^{\nu_p(b)+\nu_p(c)}$, where $u \in R^*$. Since a is irreducible, uniqueness of factorization implies $a \sim p$ for some $p \in \mathcal{P}$ such that $\nu_p(b) + \nu_p(c) > 0$, hence $a \mid b$ or $a \mid c$.

(2.7) Theorem: Fundamental Theorem of Arithmetic. $\mathbb{Z}$ is factorial.

Hence any $0 \neq z \in \mathbb{Z}$ can be written uniquely as $z = \mathrm{sgn}(z) \cdot \prod_{p\in\mathcal{P}_\mathbb{Z}} p^{\nu_p(z)}$, where the **sign** $\mathrm{sgn}(z) \in \{\pm 1\} = \mathbb{Z}^*$ is defined by $z \cdot \mathrm{sgn}(z) > 0$, and $\nu_p(z) \in \mathbb{N}_0$, and $\mathcal{P}_\mathbb{Z} \subseteq \mathbb{N}$ is the set of positive primes, being a set of representatives of the associate classes of irreducible elements.

Moreover, we have **Euclid's Theorem** saying that $\mathcal{P}_\mathbb{Z}$ is infinite.

Proof. We give an immediate direct proof, using the principle of induction; in (2.9) a more conceptual proof will be given: Letting $n \in \mathbb{Z} \setminus \{0, \pm 1\}$, we may assume that $n > 0$, and we prove the existence of a factorization by induction on $n \geq 2$: If n is irreducible, we are done, in particular settling the case $n = 2$. If n is reducible, there are $2 \leq a, b < n$ such that $n = ab$, hence both a, b have a factorization, thus n has a factorization as well.

As for uniqueness of factorizations, assume that $n = \prod_{i=1}^r p_i = \prod_{j=1}^s q_j$, where $2 \leq p_1 \leq \cdots \leq p_r$ and $2 \leq q_1 \leq \cdots \leq q_s$ are irreducible. We may assume that both $r, s \geq 1$, since otherwise we have $r = s = 1$, and that $p_1 \neq q_1$, since otherwise we are done by dividing by $p_1 = q_1$ and using induction. We may assume that $p_1 < q_1$, and let $n' := (q_1 - p_1) \cdot \prod_{j=2}^s q_j = n - p_1 \cdot \prod_{j=2}^s q_j = p_1 \cdot (\prod_{i=2}^r p_i - \prod_{j=2}^s q_j)$. Hence we have $2 \leq n' < n$, and thus by induction n' has a unique factorization, which since $p_1 \nmid (q_1 - p_1)$ and $p_1 \nmid \prod_{j=2}^s q_j$ cannot possibly involve p_1, contradicting the fact that $p_1 \mid n'$.

Finally, as for the last statement, assume to the contrary that $\mathcal{P}_\mathbb{Z} = \{p_1, \ldots, p_n\}$, for some $n \in \mathbb{N}$, and let $z := 1 + \prod_{i=1}^n p_i \in \mathbb{Z}$. Then we have $p_i \nmid z$ for all $i \in \{1, \ldots, n\}$, and since z has a factorization we infer $z = 1$, a contradiction. ♯

(2.8) Euclidean domains. a) An integral domain R is called **Euclidean**, if R has a **degree map** $\delta \colon R \setminus \{0\} \to \mathbb{N}_0$ fulfilling the following condition: For all $a, b \in R$ such that $b \neq 0$ there are $q, r \in R$, called **quotient** and **remainder** respectively, such that $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$; note that no uniqueness assumption is made here.

We may additionally assume **monotonicity**, that is $\delta(a) \leq \delta(b)$ whenever $a \mid b \neq 0$: Letting $\delta' \colon R \setminus \{0\} \to \mathbb{N}_0 \colon a \mapsto \min\{\delta(b) \in \mathbb{N}_0; b \in R \setminus \{0\}, a \mid b\}$, we show that δ' is a degree function: For $a, b \in R$ such that $b \neq 0$, letting $0 \neq c \in R$ such that $\delta'(b) = \delta(bc)$, there are $q, r \in R$ such that $a = q(bc) + r = (qc)b + r$, where $r = 0$ or $\delta'(r) \leq \delta(r) < \delta(bc) = \delta'(b)$.

Assuming monotonicity, we in particular have $\delta(a) = \delta(b)$ whenever $a \sim b \neq 0$. Moreover, kind of conversely, if $a \mid b \neq 0$ such that $\delta(a) = \delta(b)$, then we have $a \sim b$: There are $q, r \in R$ such that $a = qb + r$, where $r = 0$ or $\delta(r) < \delta(b)$; but assuming $r \neq 0$ from $a \mid a - qb = r$ we get $\delta(a) \leq \delta(r) < \delta(b)$, a contradiction; hence we infer $r = 0$, that is $b \mid a$ as well.

Again, our most prominent example is $\mathbb{Z}$, which is Euclidean with respect to the degree map $\delta\colon \mathbb{Z} \setminus \{0\} \to \mathbb{N}_0\colon z \mapsto |z|$; note that upon dividing with respect to $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ remainders are not unique, but may be chosen in $\{-|n| + 1, \ldots, 0, \ldots, |n| - 1\}$. Moreover, any field K is Euclidean with respect to the degree map $\delta\colon K^* \to \mathbb{N}_0\colon x \mapsto 0$, and polynomial rings over fields will turn out to be Euclidean as well, see (2.13). Note that for all these examples monotonicity is fulfilled right away.

b) The major feature of Euclidean domains is that they allow for computing greatest common divisors without factorizing the relevant elements first: Given $a, b \in R$ such that $a \neq 0$, a greatest common divisor $r \in R$ of a, b, together with **Bézout coefficients** $s, t \in R$ such that $r = sa + tb \in R$ can be computed by the **extended Euclidean algorithm**; leaving out the steps indicated by $\circ$, only needed to determine Bézout coefficients, leaves the **Euclidean algorithm** to compute a greatest common divisor alone:

```
• $r_0 \leftarrow a$, $r_1 \leftarrow b$, $i \leftarrow 1$
○ $s_0 \leftarrow 1$, $t_0 \leftarrow 0$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$
• 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 $\delta(r_{i+1}) < \delta(r_i)$
    ○ $s_{i+1} \leftarrow s_{i-1} - q_i s_i$, $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
    • $i \leftarrow i + 1$
• return $[r; s, t] \leftarrow [r_{i-1}; s_{i-1}, t_{i-1}]$
```

Since $\delta(r_i) > \delta(r_{i+1}) \geq 0$ for $i \in \mathbb{N}$, there is $l \in \mathbb{N}_0$ such that $r_l \neq 0$ and $r_{l+1} = 0$, hence the algorithm terminates. We have $r_i = s_i a + t_i b$ for all $i \in \{0, \ldots, l+1\}$, hence $r = r_l = sa + tb$. From $r_{i+1} = r_{i-1} - q_i r_i$, for all $i \in \{1, \ldots, l\}$, we get $r = r_l \in \gcd(r_l, 0) = \gcd(r_l, r_{l+1}) = \gcd(r_i, r_{i+1}) = \gcd(r_0, r_1) = \gcd(a, b)$. ♯

For example, let $R := \mathbb{Z}$ and $a := 2 \cdot 3^2 \cdot 7 = 126$ and $b := 5 \cdot 7 = 35$, then we have $7 = 2a - 7b \in \gcd(a, b)$, where $7 = 2 \cdot a - 7 \cdot b$:

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

(2.9) Theorem: Euclid implies Gauß. Any Euclidean domain is factorial.

Proof. Let R be an Euclidean domain with monotonous degree function δ. We first show that any $0 \neq a \in R\backslash R^*$ is a product of irreducible elements: Assuming the contrary, let a be chosen of minimal degree not having this property. Then a is reducible, hence there are $b, c \in R \setminus R^*$ such that $a = bc$. Thus we have $\delta(b) < \delta(a)$ and $\delta(c) < \delta(a)$, implying that both b and c are irreducible, hence a is a product of irreducible elements, a contradiction.

In order to show uniqueness of factorizations, we next show that any irreducible element $0 \neq a \in R \setminus R^*$ is a prime: Let $b, c \in R$ such that $a \mid bc$, where may assume that $a \nmid b$. Then we have $1 \in \gcd(a, b)$, hence there are Bézout coefficients $s, t \in R$ such that $1 = sa + tb$. Thus we have $a \mid sac + tbc = c$.

Now let $a = u \cdot \prod_{i=1}^n p_i \in R$, where the p_i are irreducible, $n \in \mathbb{N}_0$ and $u \in R^*$. 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 that $p_n \mid q_m$, hence since $q_m \in R$ is irreducible we infer $p_n \sim q_m$. Thus we have $u' \cdot \prod_{i=1}^{n-1} p_i = \prod_{j=1}^{m-1} q_j \in R$ for some $u' \in R^*$, and we are done by induction. ♯

(2.10) Example: Residue class rings, revisited. We consider again the residue class ring $\mathbb{Z}_n$, where $n \geq 2$. Then its group of units is given as $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n; 1 \in \gcd(a, n)\}$; note that this yields an alternative proof that $\mathbb{Z}_n$ is a field if and only if n is a prime:

If $a \in \mathbb{Z}_n^*$ then there are $k, l \in \mathbb{Z}$ such that $ka + ln = 1 \in \mathbb{Z}$, implying that $1 \in \gcd(a, n)$; if $a \in \mathbb{Z}_n$ such that $1 \in \gcd(a, n)$, then there are Bézout coefficients $s, t \in \mathbb{Z}$ such that $1 = sa + tn \in \mathbb{Z}$, hence we have $sa = 1 \in \mathbb{Z}_n$, thus $a \in \mathbb{Z}_n^*$. ♯

Note that in the latter case we have $a^{-1} = s \in \mathbb{Z}_n^*$, thus the extended Euclidean algorithm allows to actually compute inverses of the elements of $\mathbb{Z}_n^*$.

(2.11) Polynomial rings. a) Let R be an integral domain. Then any element of $\text{Maps}'(\mathbb{N}_0, R) := \{[a_i \in R; i \in \mathbb{N}_0]; a_i = 0 \text{ for all } i > d \text{ for some } d \in \mathbb{N}_0\}$ can be identified with an expression of the form $f = f(X) := \sum_{i=0}^d a_i X^i = \sum_{i \geq 0} a_i X^i$, being called a **polynomial** in the **indeterminate** X, where a_i is called its i-th **coefficient**. If $f \neq 0$ let $\deg(f) := \max\{i \in \mathbb{N}_0; a_i \neq 0\} \in$

$\mathbb{N}_0$ be its **degree**, and let $\mathrm{lc}(f) := a_{\deg(f)} \in R$ be its **leading coefficient**; polynomials of degree $0, 1, 2, 3$ are called **constant**, **linear**, **quadratic** and **cubic**, respectively, and if $\mathrm{lc}(f) = 1$ then f is called **monic**.

We write $R[X] := \mathrm{Maps}'(\mathbb{N}_0, R)$, which becomes a commutative ring, called the associated **polynomial ring**, with respect to **pointwise** addition, and **convolutional** multiplication, for $f = \sum_{i \geq 0} a_i X^i \in R[X]$ and $g = \sum_{j \geq 0} b_j X^j \in R[X]$ being given as $fg := \sum_{i \geq 0} \sum_{j \geq 0} a_i b_j X^{i+j} = \sum_{k \geq 0} (\sum_{l=0}^{k} a_l b_{k-l}) X^k \in R[X]$:

Indeed, $R[X]$ is a commutative additive group; we have $fg = gf$ and $(fg)h = \sum_{i \geq 0} \sum_{j \geq 0} \sum_{k \geq 0} a_i b_j c_k X^{i+j+k} = f(gh)$, where $h = \sum_{k \geq 0} c_k X^k \in R[X]$, and letting $1_{R[X]} := 1_R \cdot X^0 \in R[X]$ we get $1_{R[X]} \cdot f = f$, thus $R[X]$ is a commutative multiplicative monoid; and we have distributivity $f(g+h) = \sum_{i \geq 0} \sum_{j \geq 0} a_i (b_j + c_j) X^{i+j} = \sum_{i \geq 0} \sum_{j \geq 0} a_i b_j X^{i+j} + \sum_{i \geq 0} \sum_{j \geq 0} a_i c_j X^{i+j} = fg + fh$. $\sharp$

Hence for $0 \neq f, g \in R[X]$ we have $fg \neq 0$ as well, where $\deg(fg) = \deg(f) + \deg(g)$ and $\mathrm{lc}(fg) = \mathrm{lc}(f)\mathrm{lc}(g) \neq 0$. Hence $R[X]$ is an integral domain. Moreover, for any unit $f \in R[X]$ we hence necessarily have $\deg(f) = 0$, and thus, identifying R with $R \cdot X^0 \subseteq R[X]$, for the group of units we have $R[X]^* = R^*$; in particular, $R[X]$ is not a field.

b) Given $f \in R[X]$ and $z \in R$, we have the **evaluation map** $\epsilon_z \colon R[X] \to R \colon f = \sum_{i \geq 0} a_i X^i \mapsto \sum_{i \geq 0} a_i z^i =: f(z)$; in particular, if $f(z) = 0$ then z is called a **root** or **zero** of f. Letting $g = \sum_{i \geq 0} b_i X^i \in R[X]$ we have $(f + g)(z) = \sum_{i \geq 0} (a_i + b_i) z^i = \sum_{i \geq 0} a_i z^i + \sum_{i \geq 0} b_i z^i = f(z) + g(z)$ and $(fg)(z) = \sum_{i \geq 0} \sum_{j \geq 0} a_j b_j z^{i+j} = (\sum_{i \geq 0} a_i z^i) \cdot (\sum_{j \geq 0} b_j z^j) = f(z)g(z)$, as well as $\epsilon_z(1) = 1$, thus ϵ_z is a ring homomorphism.

Letting $z \in R$ vary, this gives rise to the **polynomial map** $\widehat{f} \colon R \to R \colon z \mapsto \epsilon_z(f) = f(z)$ associated with fixed $f \in R[X]$. Now the set $\mathrm{Maps}(R, R)$ is a ring with pointwise addition $f + g \colon R \to R \colon z \mapsto f(z) + g(z)$ and multiplication $fg \colon R \to R \colon z \mapsto f(z)g(z)$, neutral elements being the constant maps $R \to R \colon z \mapsto 0$ and $R \to R \colon z \mapsto 1$, respectively. Hence the fact that the evaluation map $\epsilon_z \colon R[X] \to R$ is a ring homomorphism, for all $z \in R$, implies that $\widehat{\ } \colon R[X] \to \mathrm{Maps}(R, R) \colon f \mapsto \widehat{f}$ is a ring homomorphism as well.

Note that $\widehat{\ }$ in general is not injective, not even if $R = K$ is a field; for example, considering the finite field $\mathbb{Z}_2$, for $0 \neq f = X(X + 1) = X^2 + X \in \mathbb{Z}_2[X]$ we have $f(0) = f(1) = 0 \in \mathbb{Z}_2$, implying that $\widehat{f} = 0 \in \mathrm{Maps}(\mathbb{Z}_2, \mathbb{Z}_2)$. But we will show in (2.13) that $\widehat{\ } \colon K[X] \to \mathrm{Maps}(K, K)$ is injective whenever K is an infinite field, thus in this case we may identify any polynomial $f \in K[X]$ with the polynomial map $\widehat{f} \in \mathrm{Maps}(K, K)$.

(2.12) Theorem: Polynomial division. Let R be an integral domain, 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 $r' = r$ or $\deg(r' - r) < \deg(g)$, and $q = q'$ or $\deg((q - q')g) = \deg(g) + \deg(q - q') \geq \deg(g)$. Hence we have $r' = r$ and $q = q'$, showing uniqueness.

To show existence, we may assume that $f \neq 0$ and $m := \deg(f) \geq \deg(g) := n$. We proceed by induction on $m \in \mathbb{N}_0$: 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 $f = (q'g + r') + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}gX^{m-n} = (q' + \mathrm{lc}(f)\mathrm{lc}(g)^{-1}X^{m-n})g + r'$. ♯

(2.13) Polynomial rings over fields. a) Let K be a field. Then we have $K^* = K[X]^* = \{f \in K[X] \setminus \{0\}; \deg(f) = 0\}$, that is the set of non-zero constant polynomials. Thus we conclude that the polynomial ring $K[X]$ is Euclidean with respect to the monotonous degree map deg.

Hence any $0 \neq f \in K[X]$ can be written uniquely as $f = \mathrm{lc}(f) \cdot \prod_{p \in \mathcal{P}_K} p^{\nu_p(f)}$, where $\nu_p(f) \in \mathbb{N}_0$ and $\mathcal{P}_K \subseteq K[X]$ is the set of irreducible monic polynomials, being a set of representatives of the associate classes of irreducible polynomials; we have $\deg(f) = \sum_{p \in \mathcal{P}_K} \nu_p(f) \deg(p) \in \mathbb{N}_0$. In particular, any linear polynomial is irreducible, and we have $\{X - a \in K[X]; a \in K\} \subseteq \mathcal{P}_K$.

For example, for $f := (X^3+2)(X+1)(X-1) = X^5 - X^3 + 2X^2 - 2 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ and $g := (X^2 + X + 1)(X + 1) = X^3 + 2X^2 + 2X + 1 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ we get $f = qg + r$ where $q := X^2 - 2X + 1 \in \mathbb{Z}[X]$ and $r := 3X^2 - 3 \in \mathbb{Z}[X]$. We have $X+1 \in \gcd(f, g) \subseteq \mathbb{Q}[X]$, where $X+1 = -\frac{1}{9}(X+2) \cdot f + \frac{1}{9}(X^3 - 3X + 5) \cdot g \in \mathbb{Q}[X]$:

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

b) Over any integral domain R, polynomial division encompasses the following particular case: Given $f \in R[X]$, an element $a \in R$ is a root of f if and only if $(X - a) \mid f \in R[X]$: There are $q, r \in R[X]$ such that $f = q \cdot (X - a) + r$, where $r = 0$ or $\deg(r) < \deg(X - a) = 1$; hence we have $r \in R$, where $r = 0$ if and only if $(X - a) \mid f$, and $r = f(a) - q(a) \cdot (a - a) = f(a)$ says that $r = 0$ if and only if a is a root of f.

c) In the Euclidean domain $K[X]$ this leads to the following observations: Given $0 \neq f \in K[X]$, any element $a \in K$ is called a root of f of **multiplicity** $\nu_a(f) := \nu_{X-a}(f) \in \mathbb{N}_0$; hence the roots of f are the roots of non-zero multiplicity. From $\sum_{a \in K} \nu_a(f) \leq \deg(f)$ we conclude that f has at most $\deg(f) \in \mathbb{N}_0$ roots, counted with multiplicity. Moreover, if f is quadratic or cubic, then considering its factorization shows that f is irreducible if and only if f does not have any root; for example, $X^2 + 1 \in \mathbb{Q}[X] \subseteq \mathbb{R}[X]$ is irreducible.

The field K is called **algebraically closed** if any non-constant polynomial in $K[X]$ has a root, or equivalently if $\mathcal{P}_K = \{X - a \in K[X]; a \in K\}$. For example, while $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed, the **Fundamental Theorem of Algebra [Gauß, 1801]** says that $\mathbb{C}$ is algebraically closed.

Finally, we show that the ring homomorphism $\widehat{\ }\colon K[X] \to \mathrm{Maps}(K, K)$ is injective if and only if K is infinite: If K is finite, then for $0 \neq f := \prod_{a \in K}(X - a) \in K[X]$ we get $f(z) = 0 \in K$ for all $z \in K$, thus $\widehat{f} = 0 \in \mathrm{Maps}(K, K)$. If K is infinite, then let $f \in K[X]$ such that $\widehat{f} = 0 \in \mathrm{Maps}(K, K)$; assume that $f \neq 0$, then f has all infinitely many elements of K as its roots, a contradiction; hence we conclude that $f = 0$ and thus $\widehat{\ }$ is injective.

(2.14) Polynomial residue class rings. a) By way of comparison of the integers $\mathbb{Z}$ and the polynomial ring $K[X]$, where K is a field, we mimic the construction of the residue class ring $\mathbb{Z}_n$, where $n \in \mathbb{N}$, whose arithmetic is inherited from $\mathbb{Z}$ by virtue of taking remainders upon division by n:

Let $0 \neq f \in K[X]$ have degree $d := \deg(f) \in \mathbb{N}_0$. Then the set of remainders occurring for division by f equals $K[X]_f := K[X]_{<d} := \{0\} \mathbin{\dot\cup} \{g \in K[X] \setminus \{0\}; \deg(g) < d\}$; in particular, we have $K[X]_f = \{0\}$ if and only if $f \in K[X]^*$. Anyway, this gives rise to the map $\overline{\ }\colon K[X] \to K[X]_f$, being defined by letting $\overline{g} \in K[X]_f$ be the remainder of g upon division by f.

We define an addition $+\colon K[X]_f \times K[X]_f \to K[X]_f$ and a multiplication $\cdot\colon K[X]_f \times K[X]_f \to K[X]_f$ by $g + h := \overline{g + h}$ and $g \cdot h := \overline{gh}$. In other words addition and multiplication are inherited from $K[X]$, by adding respectively multiplying in $K[X]$ first, and subsequently taking remainders upon division by f; but note that here we actually have $g + h \in K[X]_f$ whenever $g, h \in K[X]_f$.

Then, entirely similar to the case of $\mathbb{Z}$, it follows that the definition of addition and multiplication is independent of the choice of representatives, and thus the properties needed to make $K[X]_f$ into a commutative ring follow from those of $K[X]$; in other words $\overline{\ }\colon K[X] \to K[X]_f$ becomes a ring homomorphism. The latter ring is again called the associated **residue class ring**, as it can be identified with the set of **congruence classes** modulo f, that is the set of equivalence classes with respect to the **congruence relation** $R_f := \{[g, h] \in K[X]^2; g \equiv h \pmod{f}\} = \{[g, h] \in K[X]^2; f \mid (g - h)\}$ on $K[X]$.

Again in parallel to the integers $\mathbb{Z}$, we show that $K[X]_f$, where $0 \neq f \in K[X] \setminus K[X]^*$, is a field if and only if f is irreducible:

If $f = gh$ is reducible, where $g, h \in K[X] \setminus K[X]^*$, then we have $\deg(g), \deg(h) < \deg(f)$, hence $g, h \neq 0 \in K[X]_f$ but $gh = 0 \in K[X]_f$, thus $g, h \in K[X]_f$ are zero-divisors. If f is irreducible and $0 \neq g \in K[X]_f$, then $f \nmid g$ implies that f does not occur in the factorization of g, hence we have $1 \in \gcd(g, f) \subseteq K[X]$; then there are Bézout coefficients $s, t \in K[X]$ such that $1 = sg + tf \in K[X]$, hence we have $sg = 1 \in K[X]_f$, thus $g \in K[X]^*$. $\sharp$

b) We present a few examples: For $z \in K$ the polynomial $X - z \in K[X]$ is irreducible, hence $K[X]_{X-z} = \{a \in K[X]; a \in K\}$ is a field, where addition and multiplication are as in K, hence $K[X]_{X-z}$ can be identified with K.

The polynomial $X^2+1 \in \mathbb{R}[X]$ is irreducible, hence $\mathbb{R}[X]_{X^2+1} = \{a+bX \in \mathbb{R}[X]; a, b \in \mathbb{R}\}$ is a field, where multiplication is determined by $X^2 = -1 \in \mathbb{R}[X]_{X^2+1}$, hence is given by $(a+bX)(a'+b'X) = (aa'-bb') + (ab'+a'b)X \in \mathbb{R}[X]_{X^2+1}$; thus $\mathbb{R}[X]_{X^2+1} \to \mathbb{C}\colon a+bX \mapsto a+bi$ is a ring isomorphism.

The polynomial $X^2+X+1 \in \mathbb{Z}_2[X]$ is the unique irreducible one of degree 2 over $\mathbb{Z}_2$, hence $\mathbb{F}_4 := \mathbb{Z}_2[X]_{X^2+X+1} = \{a+bX \in \mathbb{Z}_2[X]; a, b \in \mathbb{Z}_2\}$ is a field, having 4 elements, where $X^2 = 1+X \in \mathbb{F}_4$ shows that $\mathbb{F}_4 = \{0, 1, X, X^2\}$, and $X^3 = 1 \in \mathbb{F}_4$ implies that $\mathbb{F}_4^* = \langle X \rangle$ is cyclic of order 3.

Similarly, the polynomials $X^3+X+1 \in \mathbb{Z}_2[X]$ and $X^3+X^2+1 \in \mathbb{Z}_2[X]$ are the unique irreducible ones of degree 3 over $\mathbb{Z}_2$, hence $\mathbb{Z}_2[X]_{X^3+X+1} = \mathbb{Z}_2[X]_{X^3+X^2+1} = \{a+bX+cX^2 \in \mathbb{Z}_2[X]; a, b, c \in \mathbb{Z}_2\}$, having 8 elements, becomes a field in two different ways, being called $\mathbb{F}_8$ and $\mathbb{F}'_8$, respectively: In $\mathbb{F}_8$ we have $X^3 = 1+X$, $X^4 = X+X^2$, $X^5 = 1+X+X^2$, $X^6 = 1+X^2$, showing that $\mathbb{F}_8 = \{0, 1, X, \ldots, X^6\}$, where $X^7 = 1$ implies that $\mathbb{F}_8^* = \langle X \rangle$ is cyclic of order 7; in $\mathbb{F}'_8$ we have $X^3 = 1+X^2$, $X^4 = 1+X+X^2$, $X^5 = 1+X$, $X^6 = X+X^2$, showing that $\mathbb{F}'_8 = \{0, 1, X, \ldots, X^6\}$, where $X^7 = 1$ implies that $(\mathbb{F}'_8)^* = \langle X \rangle$ is cyclic of order 7. Actually, the cyclicity of the above groups of units is a special case of **Artin's Theorem**. Finally, we have the ring isomorphism $\mathbb{F}'_8 \to \mathbb{F}_8\colon a+bX+cX^2 \mapsto a+b(1+X)+c(1+X^2) = (a+b+c)+bX+cX^2$: Since multiplication is determined by $X^3 = 1+X \in \mathbb{F}_8$ respectively $X^3 = 1+X^2 \in \mathbb{F}'_8$, it suffices to show that $1+X \in \mathbb{F}_8$ is a root of $T^3+T^2+1 \in \mathbb{Z}_2[T]$; indeed we have $(1+X)^3+(1+X)^2+1 = X^3+X+1 = 0 \in \mathbb{F}_8$.

3 References

[1] S. Bosch: Algebra, Springer, 7. Aufl., 2009.

[2] G. Fischer: Lehrbuch der Algebra, Birkhuser, 2. Aufl., 2011.

[3] H. Henn: Elementare Geometrie und Algebra, Vieweg, 1. Aufl., 2003.

[4] P. Neumann, G. Stoy, E. Thompson: Groups and geometry, Oxford Univ. Press, 1st ed., 1994.

[5] R. Schulze-Pillot: Einfhrung in Algebra und Zahlentheorie, Springer, 3. Aufl., 2014.

[6] G. Stroth: Elementare Algebra und Zahlentheorie, Birkhuser, 1. Aufl., 2011.