Group theory

Leandro Vendramin

Contents

Introduction

The notes correspond to the bachelor course *Group Theory* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve two-hour lectures.

The material is somewhat standard. Basic texts on abstract algebra are for example [**1**], [**3**] and [**5**]. Lang's book [**6**] is also a standard reference, but maybe a bit more advanced.

We also mention a set of great expository papers by The notes are extremely well-written and are useful at every stage of a mathematical career.

Thanks go to Senne Trappeniers.

This version was compiled on June 24, 2024 at 08:50. Please send comments and corrections to me at `Leandro.Vendramin@vub.be`.

Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel
E-mail address: `Leandro.Vendramin@vub.be`.

Lecture 1. 15/02/2024

§ 1.1. Groups. Before defining groups, we recall that a binary operation on a set X is simply a map

$$X \times X \to X, \quad (x,y) \mapsto xy.$$

We have used juxtaposition to denote this generic binary operation. For example, $(x,y) \mapsto x-y$ is a binary operation in $\mathbb{Z}$ but not in $\mathbb{Z}_{\geq 0}$.

DEFINITION 1.1. A **group** is a non-empty set G with a binary operation $G \times G \to G$, $(x,y) \mapsto xy$, such that the following properties hold:

1) (Associativity) $(xy)z = x(yz)$ for all $x,y,z \in R$.
2) (Existence of a neutral element) There exists $e \in G$ such that $xe = ex = x$ for all $x \in G$.
3) (Existence of inverses) For each $x \in G$ there exists $y \in G$ such that $xy = yx = e$.

The associativity condition implies that all ordered products that we can form with, say, the elements $x_1, x_2, \dots, x_n$ will be equal. For example,

$$(x_1x_2)((x_3x_4)x_5) = x_1(x_2(x_3(x_4x_5)))$$

and hence we can write, without ambiguity and without using brackets,

$$x_1x_2 \cdots x_5.$$

This fact can be proved by induction; see for example Lang's book [**6**]. We will provide an alternative proof as an application of Cayley's theorem 7.27.

PROPOSITION 1.2. *In a group G, every element $x \in G$ admits a unique inverse.*

PROOF. Let $y,z \in G$ be inverses of $x \in G$. Then $z = z(xy) = (zx)y = ey = y$. □

EXERCISE 1.3. Prove that the neutral element of a group is unique.

In general, when the binary operation is written multiplicatively, one writes the neutral element e of a group as 1_G or simply as 1. The inverse of x will be denoted by x^{-1}.

EXAMPLE 1.4. Let $n \geq 1$. The set $\mathbf{GL}_n(\mathbb{R})$ of $n \times n$ invertible real matrices forms a group with the usual matrix multiplication. The neutral element is the identity matrix. The product of matrices is associative. And, by definition, every element of $\mathbf{GL}_n(\mathbb{R})$ admits an inverse.

It is a good idea to keep in mind the *group of invertible matrices*. With this, the following properties (valid in every group) look familiar:

1) $(x^{-1})^{-1} = x$ for all x.
2) $(xy)^{-1} = y^{-1}x^{-1}$ for all x,y.

EXERCISE 1.5. Prove that in a group, the equation $ax = b$ has a unique solution: $x = a^{-1}b$. Similarly, $x = ba^{-1}$ is the unique solution of the equation $xa = b$.

DEFINITION 1.6. A group G is **abelian** if $xy = yx$ for all $x,y \in G$.

Most of the time, for abelian groups, we will use the *additive notation*. This means that the binary operation of the group will be denoted by $(x,y) \mapsto x+y$, the neutral element by 0 and the inverse of an element x will be $-x$.

Example 1.7. Let us see some examples abelian groups:

1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual addition.
2) Let $n \geq 2$. The set $\mathbb{Z}/n$ of integers modulo n with the usual addition modulo n.
3) $\mathbb{Q}^\times = \setminus\{0\}$, $\mathbb{R}^\times = \setminus\{0\}$ and $\mathbb{C}^\times = \setminus\{0\}$ with the usual multiplication.
4) Let p be a prime number. The set $(\mathbb{Z}/p)^\times = \mathbb{Z}/p \setminus \{0\}$ of invertible integers modulo p with the usual multiplication modulo p.

The groups of the first two items will be written in additive notation.

The **trivial group** is the (unique) group containing exactly one element, the neutral element. We can write this group additively, so we have the group $\{0\}$ with the addition $0+0=0$, or multiplicatively as $\{1\}$ with multiplication $1 \cdot 1 = 1$.

Definition 1.8. The **order** $|G|$ of a group G is the cardinality of G. A group G is said to be **finite** if $|G|$ is finite and **infinite** otherwise.

The group $\mathbb{Z}/n$ of integers modulo n is a finite group of order n. The group $(\mathbb{Z}/p)^\times$ of units modulo p is a finite group of order $p-1$. The other groups of Example 1.7 are infinite.

Exercise 1.9. Let G be a group and $g \in G$. Prove that the maps $L_g \colon G \to G$, $x \mapsto gx$, and $R_g \colon G \to G$, $x \mapsto xg$, are bijective.

Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group. The **table** of G is the matrix that in position (i, j) has the element $g_i g_j$. For example, the table of the (additive) group $\mathbb{Z}/4$ of integers modulo 4 is the following:

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

We know that $\mathbb{Z}$ is a group with the usual addition. We now discuss a multiplicative version of this group, as it will be very important later. We first need a little bit of notation. Let G be a group and $g \in G$. For $k \in \mathbb{Z} \setminus \{0\}$, we write

$$\begin{aligned} g^k &= g \cdots g \quad (k-\text{times}) && \text{if } k > 0, \\ g^k &= g^{-1} \cdots g^{-1} \quad (|k| - \text{times}) && \text{if } k < 0. \end{aligned}$$

By convention, $g^0 = 1$. The following facts are left as an exercise:

1) $(x^k)^l = x^{kl}$ for all $x \in G$ and $k, l \in \mathbb{Z}$.
2) If G is abelian, then $(xy)^k = x^k y^k$ for all $x, y \in G$ and $k \in \mathbb{Z}$.

Example 1.10. Fix a symbol g. Consider the set

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

of integers powers of g (with the usual convention $g^0 = 1$). Then $\langle g \rangle$ with the operation $g^i g^j = g^{i+j}$ is an abelian group.

We will see later that $\mathbb{Z}$ and the group of Example 1.10 are “indistinguishable” as groups, even if they appear to be completely different.

EXAMPLE 1.11. Let n be a positive integer. The set $G_n = \{z \in \mathbb{C} : z^n = 1\}$ is an abelian group with the usual multiplication of complex numbers. Moreover, the set $\cup_{n \geq 1} G_n$ is an abelian group.

EXAMPLE 1.12. Let X be a non-empty set. The set $\mathbb{S}_X$ of bijective maps $X \to X$ is a group with the usual composition of maps. If $|X| \geq 3$, the group $\mathbb{S}_X$ is non-abelian. To prove this, let $a, b, c \in X$ be three different elements. Let $f \colon X \to X$ be such that $f(a) = b$, $f(b) = c$ and $f(c) = a$ and $g \colon X \to X$ be such that $g(a) = b$, $g(b) = a$ and $g(x) = x$ for all $x \in X \setminus \{a, b\}$. Then $fg \neq gf$.

If $X = \{1, 2, \dots, n\}$, the group $\mathbb{S}_X$ will be written as $\mathbb{S}_n$. This is the **symmetric group** of degree n. The elements of $\mathbb{S}_n$ are called **permutations** of degree n. Note that $|\mathbb{S}_n| = n!$ and $\mathbb{S}_n$ is abelian if and only if $n \in \{1, 2\}$. Each element of $\mathbb{S}_n$ is a bijective map $f \colon \{1, \dots, n\} \to \{1, \dots, n\}$. To denote permutations, we can use the following convention. The symbol

$$\begin{pmatrix} 12345 \\ 32145 \end{pmatrix}$$

denotes the map $f \colon \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ such that

$$f(1) = 3, \quad f(2) = 2, \quad f(3) = 1, \quad f(4) = 4, \quad f(5) = 5.$$

Here 2 and 4 are **fixed points** of the permutation f.

As we said, the operation of $\mathbb{S}_n$ is the usual composition of maps. For example,

$$\begin{pmatrix} 12345 \\ 32145 \end{pmatrix} \begin{pmatrix} 12345 \\ 13452 \end{pmatrix} = \begin{pmatrix} 12345 \\ 32145 \end{pmatrix} \circ \begin{pmatrix} 12345 \\ 13452 \end{pmatrix} = \begin{pmatrix} 12345 \\ 31452 \end{pmatrix}.$$

EXAMPLE 1.13 (Klein group). The set

$$K = \left\{ \mathrm{id}, \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}, \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}, \begin{pmatrix} 1234 \\ 4321 \end{pmatrix} \right\}$$

together with the usual composition of maps is an abelian group. Note that K is included in $\mathbb{S}_4$. Can you compute the table of this group?

Every permutation can be written as a product of disjoint cycles. The fact is proved by induction but is relatively intuitive. Let us decompose the permutation

$$\sigma = \begin{pmatrix} 123456789 \\ 638915724 \end{pmatrix} \in \mathbb{S}_9$$

as a product of cycles. We need to draw a picture for σ:

$$\begin{tikzcd}
1 \arrow[r] & 6 \arrow[d] & 2 \arrow[r] & 3 \arrow[d] & 4 \arrow[d, leftrightarrow] & \\
& 5 \arrow[ul] & & 8 \arrow[ul] & 9 & 7 \arrow[loop above]
\end{tikzcd}$$

We see that σ has two 3-cycles, one 2-cycle and one loop. Therefore

$$\sigma = (165)(238)(49)(7).$$

Generally, one omits loops and orders the cycles according to the length. Thus

$$\sigma = (49)(165)(238).$$

EXAMPLE 1.14. The set $\mathbb{S}_3$ of bijective maps $\{1,2,3\} \to \{1,2,3\}$ together with the composition of maps is a group of order six. Its elements are the permutations

$$\mathrm{id}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

Writing permutations as a product of disjoint cycles, the elements of $\mathbb{S}_3$ are then

$$\mathrm{id}, (12), (13), (23), (123), (132),$$

where, as we know, the symbol (12) represents the map $\{1,2,3\} \to \{1,2,3\}$ such that $1 \mapsto 2$, $2 \mapsto 1$ and $3 \mapsto 3$. Can you construct the table for this group?

EXAMPLE 1.15. Let $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ (here ∞ is just a symbol) and assume that the following rules hold:

$$1/\infty = 0, \quad 1/0 = \infty, \quad \infty/\infty = 1, \quad 1 - \infty = \infty - 1 = \infty.$$

We now consider some maps $\overline{\mathbb{R}} \to \overline{\mathbb{R}}$ such as $x \mapsto x$, $x \mapsto 1-x$ and $x \mapsto \frac{1}{x}$. We claim that the set

$$G = \left\{ x, \frac{1}{x}, 1-x, \frac{1}{1-x}, \frac{x}{x-1}, \frac{x-1}{x} \right\} \subseteq \{f \colon \overline{\mathbb{R}} \to \overline{\mathbb{R}} : f \text{ is a map}\}$$

is a non-abelian group with the usual composition of maps. How is this group "acting" on the set $\{0,1,\infty\}$? The group G can be identified with the set of bijective maps $\{0,1,\infty\} \to \{0,1,\infty\}$. For example, the map $x \mapsto \frac{1}{x}$ can be identified with the permutation of the set $\{0,1,\infty\}$ that permutes 0 and ∞ and fixes 1. Similarly, $\frac{1}{1-x}$ permutes the elements $\{0,1,\infty\}$ cyclically in the following way:

$$\begin{tikzcd} 0 \arrow[dr] & \\ & 1 \arrow[dl] \\ \infty \arrow[uu] & \end{tikzcd}$$

Writing the elements of G as cycles,

$$G = \{\mathrm{id}, (0\,\infty), (0\,1), (1\,\infty\,0), (\infty\,1), (1\,0\,\infty)\}.$$

We will see later that the groups of Examples 1.14 and 1.15 are indeed "indistinguishable" as groups.

EXAMPLE 1.16. Let $n \geq 2$. The multiplicative units of $\mathbb{Z}/n$ form a group with the usual multiplication modulo n. We will use the following notation:

$$\mathscr{U}(\mathbb{Z}/n) = \{x \in \mathbb{Z}/n : \gcd(x,n) = 1\}.$$

The order of $\mathscr{U}(\mathbb{Z}/n)$ is $\varphi(n)$, where φ is the Euler's function, that is

$$\varphi(n) = |\{x \in \mathbb{Z} : 1 \leq x \leq n, \gcd(x,n) = 1\}|.$$

Let us show a concrete example. The table of $\mathscr{U}(\mathbb{Z}/8) = \{1,3,5,7\}$ is

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Exercise 1.17. Let G and H be groups. Prove that the set $G \times H$ of pairs (g,h), where $g \in G$ and $h \in H$ is a group with the operation

$$(g,h)(g_1,h_1) = (gg_1,hh_1).$$

This group is called the **direct product** of G and H.

The construction of Example 1.17 can be easily generalized to the product of three or more groups.

Lecture 2. 22/02/2024

§ 2.1. Subgroups.

DEFINITION 2.1. Let G be a group. A subset S of G is said to be a **subgrup** of G if the following properties are satisfied:

1) $1 \in S$,
2) $x \in S \implies x^{-1} \in S$, and
3) $x, y \in S \implies xy \in S$.

Notation: S is a subgroup of G if and only if $S \leq G$.

The first condition of the definition can be replaced by the following condition: $S \neq \emptyset$. Why?

EXAMPLE 2.2. If G is a group, then $\{1\}$ and G are always subgroups of G.

The subgroup $\{1\}$ is known as the **trivial subgroup** of G. A subgroup S of G is said to be **proper** if $S \neq G$.

EXAMPLE 2.3. Write $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$ to denote the set of even integers. Then

$$2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

is a chain of subgroups.

EXAMPLE 2.4. $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Note that one cannot prove that $S^1 \leq \mathbb{C}$. Why?

EXAMPLE 2.5. Let $n \geq 1$. Then $G_n = \{z \in \mathbb{C} : z^n = 1\}$ is a subgroup of $\mathbb{C}^\times$. Note that

$$G_n = \{1, \exp(2\pi i/n), \exp(4i\pi/n), \dots, \exp(2(n-1)i\pi/n)\}.$$

and

$$G_n \leq \bigcup_{k\geq 1} G_k \leq S^1 \leq \mathbb{C}^\times.$$

Why $\cup_{k\geq 1} G_k$ is a group?

EXERCISE 2.6. Let G be a group. Prove that the **center**

$$Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$$

of G is a subgroup of G.

One can prove that, if G is a group and $g \in G$, then the **centralizer**

$$C_G(g) = \{h \in G : gh = hg\}$$

is a subgroup of G. Moreover, $Z(G) = \cap_{g\in G} C_G(g)$.

EXERCISE 2.7. Let S be a subgroup of G and $g \in G$. Prove that the **conjugate** gSg^{-1} of S by g is a subgroup of G. Notation: ${}^gS = gSg^{-1}$.

EXERCISE 2.8. Prove that $Z(\mathbb{S}_3) = \{\mathrm{id}\}$ and compute $C_{\mathbb{S}_3}((12))$.

The following exercise is useful:

EXERCISE 2.9. Let G be a group and S be a subset of G. Prove that S is a subgroup of G if and only if $S \neq \emptyset$ and for all $x, y \in S$ one has $xy^{-1} \in S$.

Use the previous exercise and the fact that the determinant is a multiplicative function to solve the following problem:

EXERCISE 2.10. Prove that $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$.

EXERCISE 2.11. Prove that the intersection of subgroups is again a subgroup.

The previous exercise is easy but crucial. We need it to construct subgroups generated by a given subset of elements.

DEFINITION 2.12. Let G be a group and X a non-empty subset of G. The **subgroup generated** by X is the smallest subgroup of G that contains X, that is

$$\langle X \rangle = \bigcap \{S : S \leq G, X \subseteq S\}.$$

Why this is the smallest subgroup that contains X? Let $H \leq G$ be such that $X \subseteq H$. Since H is one of the subgroups appearing in the intersection,

$$\langle X \rangle = \bigcap \{S : S \leq G, X \subseteq S\} \subseteq H.$$

We will use the following notation: If $X = \{g_1, \dots, g_k\}$, then

$$\langle X \rangle = \langle \{g_1, \dots, g_k\} \rangle = \langle g_1, \dots, g_k \rangle.$$

EXERCISE 2.13. Prove that

$$\langle X \rangle = \{x_1^{n_1} \cdots x_k^{n_k} : k \geq 0, x_1, \dots, x_k \in X, -1 \leq n_1, \dots, n_k \leq 1\}.$$

The previous exercise shows that the subgroup generated by, say, the elements $x_1, \dots, x_n$ is nothing but the group formed by (some) words on the letters $x_1, \dots, x_n$ and their inverses $x_1^{-1}, \dots, x_n^{-1}$.

EXAMPLE 2.14. Let $n \geq 3$. Let

$$r = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The **dihedral group** $\mathbb{D}_n$ is the subgroup of $\mathbf{GL}_2(\mathbb{C})$ generated by r and s, that is $\mathbb{D}_n = \langle r, s \rangle$. A direct calculation shows that

$$r^n = s^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad srs = r^{-1}.$$

An element of $\mathbb{D}_n$ is a finite word of the form

$$r^{i_1} s^{j_1} r^{i_2} s^{j_2} \cdots$$

for some $i_1, i_2, \dots \in \{0, 1, \dots, n-1\}$ and $j_1, j_2, \dots \in \{0, 1\}$. Since $rs = sr^{-1}$, we conclude that every element of $\mathbb{D}_n$ can be written as $r^i s^j$ for some $i \in \{0, \dots, n-1\}$ and $j \in \{0, 1\}$. Since these elements are all different, we conclude that $|\mathbb{D}_n| = 2n$.

To understand better the previous example, we discuss a particular case. If $n = 4$, then the elements of $\mathbb{D}_4$ are

$$r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad r^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad r^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad rs = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad r^2 s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad r^3 s = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

This is (a representation of) the group of symmetries of the square.

Exercise 2.15. The group $\mathbb{D}_3$ is generated by

$$r = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Note that this is (another representation of) the group of symmetries of a regular triangle.

Exercise 2.16. The union of subgroups is not, in general, a subgroup. Can you give an example?

Example 2.17. Let Q_8 be the set of matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad -i = \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix},$$
$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, \quad -k = \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix}.$$

Then Q_8 is a subgroup of $\mathbf{GL}_2(\mathbb{C})$. It is known as the **quaternion group** of order eight. Sometimes, it is convenient just to write

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

but one needs to remember that 1 is playing the role of identity matrix, that is the neutral element of Q_8, -1 commutes with every element of Q_8 and that $i^2 = j^2 = k^2 = -1$ and $ijk = -1$. This is enough to compute the multiplication table of Q_8. For example, to show that $ji = -k$, we proceed as follows:

$$ijk = -1 \implies -jk = -i \implies jk = i \implies -k = ji.$$

Exercise 2.18. Compute the multiplication table of Q_8.

§ 2.2. Subgroups of $\mathbb{Z}$. What can we say about the subgroups of $\mathbb{Z}$?

Theorem 2.19. *If S is a subgroup of $\mathbb{Z}$, then $S = m\mathbb{Z} = \{mx : x \in \mathbb{Z}\}$ for some $m \geq 0$.*

Proof. If $S = \{0\}$, take $m = 0$. Assume now that $S \neq \{0\}$. Let $m = \min\{s \in S : s > 0\}$. Why does this m exist? Since $S \neq \{0\}$, it contains an element $n \in S \setminus \{0\}$. There are then two possible cases: $n > 0$ or $-n > 0$. Since S is a subgroup of $\mathbb{Z}$, $-n \in S$.

We claim that $S = n\mathbb{Z}$. If $x \in S$, then $x = my + r$ for $y, r \in \mathbb{Z}$ with $0 \leq r < m$. Suppose that $r \neq 0$. Since $x, m \in S$, it follows that $r \in S$, a contradiction to the minimality of n. Thus $r = 0$ and hence

$x = my \in m\mathbb{Z}$. Conversely, since $n \in S$, it follows that $nk \in S$ for all $k \in \mathbb{Z}$. In fact, if $k = 0$, then $nk = 0 \in S$. If $k > 0$, then

$$\underbrace{n + \cdots + n}_{k-\text{times}} \in S.$$

Finally, if $k < 0$, then

$$nk = \underbrace{-n + (-n) + \cdots + (-n)}_{|k|-\text{times}} \in S.$$ □

The previous theorem has nice applications. If $a, b \in \mathbb{Z}$, we say that a **divides** b (or b is divisible by a) if $b = ac$ for some $c \in \mathbb{Z}$. Notation:

$$a \mid b \Longleftrightarrow b = ac \text{ for some } c \in \mathbb{Z}.$$

If $a, b \in \mathbb{Z}$ are such that $ab \neq 0$, then

$$S = a\mathbb{Z} + b\mathbb{Z} = \{m \in \mathbb{Z} : m = ar + bs \text{ for } r, s \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$ (this is an exercise). By Theorem 2.19, $S = d\mathbb{Z}$ for some $d > 0$. This positive integer d is the **greatest common divisor** of a and b, that is $d = \gcd(a, b)$.

EXERCISE 2.20. Let $a, b \in \mathbb{Z}$ be such that $ab \neq 0$ and $d = \gcd(a, b)$. Prove the following statements:

1) d divides a and b.
2) If $e \in \mathbb{Z}$ divides a and b, then e divides d.
3) There are $r, s \in \mathbb{Z}$ such that $d = ar + bs$.

Two integers a and b are said to be **coprime** if and only if the only positive integer dividing a and b is one, that is

$$\begin{aligned} a \text{ and } b \text{ are coprime} &\Longleftrightarrow \gcd(a, b) = 1 \\ &\Longleftrightarrow \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \\ &\Longleftrightarrow \text{there exist } r, s \in \mathbb{Z} \text{ such that } ar + bs = 1. \end{aligned}$$

EXERCISE 2.21. Let p be a prime and $a, b \in \mathbb{Z}$. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

If S and T are subgroups of $\mathbb{Z}$, then $S \cap T$ is a subgroup of $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$ be such that $ab \neq 0$. Since $a\mathbb{Z} \cap b\mathbb{Z}$ is a non-zero subgroup of $\mathbb{Z}$ (note that it contains $ab \neq 0$), we can write $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ for some $m \geq 1$. The integer m is the **least common multiple** of a and b and will be written as $m = \operatorname{lcm}(a, b)$.

EXERCISE 2.22. Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $m = \operatorname{lcm}(a, b)$. Prove the following statements:

1) m is divisible by both a and b.
2) If n is divisible by both a and b, then n is divisible by m.

EXERCISE 2.23. Let $a, b \in \mathbb{Z}_{\geq 1}$. Prove that $ab = \gcd(a, b) \operatorname{lcm}(a, b)$.

§ 2.3. Commutators. For a group G and $x,y \in G$, the **commutator** of x and y is defined as

$$[x,y] = xyx^{-1}y^{-1}$$

Note that $[x,y]yx = xy$ and $[x,y]^{-1} = [y,x]$ for all $x,y \in G$.

Definition 2.24. The **commutator subgroup** $[G,G]$ of G is the subgroup generated by the commutators of G, that is $[G,G] = \langle [x,y] : x,y \in G \rangle$.

For a group G,

$$G \text{ is abelian } \iff [x,y] = 1 \text{ for all } x,y \in G \iff [G,G] = \{1\}.$$

The commutator subgroup of a group G is also called the **derived subgroup** of G.

Example 2.25. In $\mathbb{Z}$, the commutator of $x,y \in \mathbb{Z}$ is the integer

$$[x,y] = x + y - x - y = 0.$$

This example uses additive notation! Thus $[\mathbb{Z},\mathbb{Z}] = \{0\}$.

Exercise 2.26. Prove that $[\mathbb{S}_3,\mathbb{S}_3] = \{\mathrm{id}, (123), (132)\}$.

Why do we need to consider the subgroup generated by commutators? Because the set of commutators is not always a subgroup. With the help of computers, one can verify the following examples. The first one is taken from Carmichael's book [**2**].

Example 2.27. Let G be the subgroup of $\mathbb{S}_{16}$ generated by the permutations

$$\begin{aligned} a &= (13)(24), & b &= (57)(68), \\ c &= (9\,11)(10\,12), & d &= (13\,15)(14\,16), \\ e &= (13)(57)(9\,11), & f &= (12)(34)(13\,15), \\ g &= (56)(78)(13\,14)(15\,16), & h &= (9\,10)(11\,12). \end{aligned}$$

Then $[G,G]$ has order 16, but the set of commutators of G has 15 elements:

```
gap> a := (1,3)(2,4);;
gap> b := (5,7)(6,8);;
gap> c := (9,11)(10,12);;
gap> d := (13,15)(14,16);;
gap> e := (1,3)(5,7)(9,11);;
gap> f := (1,2)(3,4)(13,15);;
gap> g := (5,6)(7,8)(13,14)(15,16);;
gap> h := (9,10)(11,12);;
gap> G := Group([a,b,c,d,e,f,g,h]);;
gap> D := DerivedSubgroup(G);;
gap> Size(D);
16
gap> Size(Set(Cartesian(G, G), x->Comm(x[1], x[2])));
15
gap> c*d in Difference(D, Set(Cartesian(G, G), Comm));
true
```

The following example goes back to Guralnick [**4**]. It was found by hand when computers were not as popular in group theory as now.

Example 2.28. The group

$$G = \langle (135)(246)(7\,11\,9)(8\,12\,10), (394\,10)(58)(67)(11\,12)\rangle.$$

has order 96. The set of commutators is different from the commutator subgroup:

```
gap> x := (1,3,5)(2,4,6)(7,11,9)(8,12,10);;
gap> y := (3,9,4,10)(5,8)(6,7)(11,12);;
gap> G := Group([x,y]);;
gap> Order(G);
96
gap> D := DerivedSubgroup(G);;
gap> Order(D);
32
gap> Size(Set(Cartesian(G, G), x->Comm(x[1], x[2])));
29
```

Moreover, G is the smallest group with the property that the set of commutators is not a subgroup.

§ 2.4. Cyclic groups.

Definition 2.29. A group G is said to be **cyclic** if $G = \langle g\rangle$ for some $g \in G$.

If G is a cyclic group generated by g, then $G = \langle g\rangle = \{g^k : k \in \mathbb{Z}\}$. Every cyclic group is, in particular, an abelian group.

Example 2.30.
1) $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$.
2) $\mathbb{Z}/n = \langle 1\rangle$.
3) $G_n = \langle \exp(2i\pi/n)\rangle$.

Example 2.31. $\mathscr{U}(\mathbb{Z}/8) \neq \langle 3\rangle$. In fact, $\langle 3\rangle = \{1,3\} \subsetneq \{1,3,5,7\} = \mathscr{U}(\mathbb{Z}/8)$.

Exercise 2.32. Prove that subgroups of a cyclic group are cyclic.

Definition 2.33. Let G be a group and $g \in G$. The **order** of g is the order of the subgroup generated by g. Notation: $|g| = |\langle g\rangle|$.

Theorem 2.34. *Let G be a group and $g \in G$ and $n \geq 1$. The following statements are equivalent:*
1) $|g| = n$.
2) $n = \min\{k \in \mathbb{Z}_{\geq 1} : g^k = 1\}$.
3) *For every* $k \in \mathbb{Z}$, $g^k = 1 \iff n \mid k$.
4) $\langle g\rangle = \{1, g, \dots, g^{n-1}\}$ *and the elements* $1, g, \dots, g^{n-1}$ *are all different.*

Proof. We first prove that $(1) \implies (2)$. If $g = 1$, then $n = 1$. Assume that $g \neq 1$. Since $\langle g\rangle = \{g^k : k \in \mathbb{Z}\}$, there exist integers i and j with $i > j$ such that $g^i = g^j$, that is $g^{i-j} = 1$. In particular, the set $\{k \in \mathbb{Z}_{\geq 1} : g^k = 1\}$ is non-empty and hence has a minimal element, say

$$d = \min\{k \in \mathbb{Z}_{\geq 1} : g^k = 1\}.$$

Thus $\langle g\rangle \subseteq \{1, g, \dots, g^{d-1}\} \subseteq \langle g\rangle$. If $g^k \in \langle g\rangle$, then $k = dq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Since $g^d = 1$,

$$g^k = g^{dq+r} = (g^d)^q g^r = g^r \in \{1 = g^0, g, g^2, \dots, g^{d-1}\}$$

Moreover, $\{1, g, \dots, g^{d-1}\} \subseteq \langle g\rangle$ and $\{1, g, \dots, g^{d-1}\}$ has d elements.

We now prove that $(2) \implies (3)$. Assume that $g^k = 1$. If we write $k = nt + r$ with $0 \leq r < n$, then $g^k = g^{nt+r} = g^r$. The minimality of n implies that $r = 0$. Hence n divides k. Conversely, if $k = nt$ for some $t \in \mathbb{Z}$, then $g^k = (g^n)^t = 1$.

Let us prove that $(3) \implies (4)$. Clearly, $\{1, g, \dots, g^{n-1}\} \subseteq \langle g \rangle$. To prove the other inclusion, we write $k = nt + r$ with $0 \leq r \leq n-1$. Then

$$g^k = g^{nt+r} = (g^n)^t g^r = g^r,$$

as, by assumption, $g^n = 1$. To see that the elements $1, g, \dots, g^{n-1}$ are all different, it is enough to show that if $g^k = g^l$ with $0 \leq k < l \leq n-1$, then, since $g^{l-k} = 1$ and $0 < l - k \leq n-1$, it follows that $n \leq l - k$ (because by assumption n divides $l - k$, a contradiction).

Finally, the implication $(4) \implies (1)$ is trivial. $\square$

Lecture 3. 29/02/2024

COROLLARY 3.1. *If G is a group and $g \in G$ has order n, then*

$$|g^m| = \frac{n}{\gcd(n,m)}.$$

PROOF. Let k be such that $(g^m)^k = 1 = g^{mk}$. This means that n divides km, as g has order n. This is also equivalent to the fact that n/d divides mk/d, where $d = \gcd(n,m)$. Therefore, since n/d and m/d are coprime, $(g^m)^k = 1$ is equivalent to n/d divides k, which implies that g^m has order n/d. □

EXERCISE 3.2. Let G be a group and $g \in G$. Prove that the following statements are equivalent:

1) g has infinite order.
2) The set $\{k \in \mathbb{Z}_{\geq 1} : g^k = 1\}$ is empty.
3) If $g^k = 1$, then $k = 0$.
4) If $k \neq l$, then $g^k \neq g^l$.

EXERCISE 3.3. Let G be an abelian group. Prove that $T(G) = \{g \in G : |g| < \infty\}$ is a subgroup of G. Compute $T(\mathbb{C}^\times)$.

EXERCISE 3.4. Let $G = \langle g \rangle$ be a cyclic group.

1) If G is infinite, only g and g^{-1} generate G.
2) If G is finite of order n, then $G = \langle g^k \rangle$ if and only if k and n are coprime.

The following exercise is a particular case of Cauchy's theorem; see Theorem 10.8.

EXERCISE 3.5. Prove that every group of odd order contains an element of order two.

Let us see some concrete examples:

EXAMPLE 3.6. In $\mathbb{S}_3$ we have the following order pattern:

$$|\operatorname{id}| = 1, \quad |(12)| = |(13)| = |(23)| = 2, \quad |(123)| = |(132)| = 3.$$

EXAMPLE 3.7. In $\mathbb{Z}$, every non-zero element has infinite order.

EXAMPLE 3.8. In $\mathbb{Z} \times \mathbb{Z}/6$ there are elements of (in)finite order. For example, $(1,0)$ has infinite order and $(0,1)$ has order six.

EXAMPLE 3.9. The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ has infinite order.

EXAMPLE 3.10. Let us compute the orders of $\mathbb{Z}/4 = \{0,1,2,3\}$. This is an additive group and 0 is the neutral element. Thus $|0| = 1$. Since we are using additive notations, "powers" really mean multiples. A direct calculation shows that $|1| = |3| = 4$ and $|2| = 2$.

EXAMPLE 3.11. The group $G_\infty = \bigcup_{n \geq 1} G_n$ is abelian and infinite. Note that every element of G_∞ has finite order.

We conclude the topic with some exercises.

EXERCISE 3.12. Compute the orders of the elements of $\mathbb{Z}/6$.

EXERCISE 3.13. Prove that $a = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ has order four, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ has order three and compute the order of ab.

EXERCISE 3.14. Compute the order of $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

EXERCISE 3.15. Prove that in $\mathbb{D}_n$ one has $|r^j s| = 2$ and $|r^j| = n/\gcd(n, j)$.

EXERCISE 3.16. Prove that a group with finitely many subgroups is finite.

§ 3.1. Lagrange's theorem. Let G be a group and H be a subgroup of G. We say that the elements $x, y \in G$ are (left) equivalent modulo H if $x^{-1}y \in H$. We will use the following notation:

$$x \equiv y \bmod H \iff x^{-1}y \in H. \tag{3.1}$$

EXERCISE 3.17. Prove that (3.1) is an equivalence relation, that is

1) $x \equiv x \bmod H$ for all x;
2) if $x \equiv y \bmod H$, then $y \equiv x \bmod H$; and
3) if $x \equiv y \bmod H$ and $y \equiv z \bmod H$, then $x \equiv z \bmod H$.

The equivalence classes of this equivalence relation modulo H are the sets of the form $xH = \{xh : h \in H\}$, as the class of an element $x \in G$ is the set

$$\{y \in G : x \equiv y \bmod H\} = \{y \in G : x^{-1}y \in H\} = \{y \in G : y \in xH\} = xH.$$

The set xH is called a **left coset** of H in G and x is a **representative** of xH.

Having an equivalence relation modulo H in G allows us to decompose G as a disjoint union of certain subsets related to H.

PROPOSITION 3.18. *Let G be a group and H be a subgroup of G.*

1) *If $xH \cap yH \neq \emptyset$, then $xH = yH$.*
2) *The group G decomposes as a disjoint union of different left cosets of H.*

PROOF. Let us prove the first claim. If $g \in xH \cap yH$, we write $g = xh$ for some $h \in H$. Then

$$gH = (xh)H = x(hH) = xH.$$

Similarly, $gH = yH$. Hence $xH = yH$. The second claim follows from the first one. □

One can also define right cosets: $x \equiv y \bmod H$ if and only if $xy^{-1} \in H$. In this case, the equivalence classes are the sets of the form Hx with $x \in X$. The set Hx is called a **right coset** with **representative** x of H in G.

PROPOSITION 3.19. *If H is a subgroup of G, then $|Hx| = |H| = |xH|$ for all $x \in G$.*

PROOF. Let $x \in G$. The map $H \to Hx$, $h \mapsto hx$, is bijective with inverse $hx \mapsto h$. Similarly, the map $H \to xH$, $h \mapsto xh$, is bijective. $\square$

The map

$$\{\text{right cosets of } H \text{ in } G\} \to \{\text{left cosets of } H \text{ in } G\}$$

given by $Hx \mapsto x^{-1}H$ is a bijection, as

$$Hx = Hy \iff xy^{-1} \in H \iff (x^{-1})^{-1}y^{-1} \in H \iff x^{-1}H = y^{-1}H.$$

In particular, the number of right cosets of H in G equals the number of left cosets of H in G.

DEFINITION 3.20. If H is a subgroup of G, the **index** of H in G is the number $(G:H)$ of left (or right) cosets of H in G.

EXAMPLE 3.21. If $G = \mathbb{Z}$ and $S = n\mathbb{Z}$, then

$$a + S = \{a + nq : q \in \mathbb{Z}\} = \{k \in \mathbb{Z} : k \equiv a \bmod n\}.$$

EXAMPLE 3.22. The subgroups of $\mathbb{S}_3$ are $\{\mathrm{id}\}$, the order-two subgroups $\mathbb{S}_3$, $\langle(12)\rangle$, $\langle(13)\rangle$ and $\langle(23)\rangle$, and the order-three subgroup $\langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$. If $H = \langle(12)\rangle = \{\mathrm{id}, (12)\}$, then

$$H = (12)H = \{\mathrm{id}, (12)\},$$
$$(123)H = (13)H = \{(13), (123)\},$$
$$(132)H = (23)H = \{(23), (132)\}.$$

Note that our group decomposes as

$$\mathbb{S}_3 = H \cup (123)H \cup (132)H \quad \text{(disjoint union)}.$$

EXAMPLE 3.23. Let $G = \mathbb{R}^2$ with the usual addition and $v \in \mathbb{R}^2$. The line

$$L = \{\lambda v : \lambda \in \mathbb{R}\}$$

is a subgroup of G. For each $p \in \mathbb{R}^2$, the coset $p + L$ is the line parallel to L that passes through p.

The following important theorem will be used extensively.

THEOREM 3.24 (Lagrange). *If G is a finite group and H is a subgroup of G, then $|G| = |H|(G:H)$. In particular, $|H|$ divides $|G|$.*

PROOF. We decompose G into equivalence classes modulo H, that is

$$G = \bigcup_{i=1}^{n} x_i H \quad \text{(disjoint union)}$$

for some $x_1, \dots, x_n \in G$, where $n = (G:H)$. Since each of these equivalence classes has exactly $|H|$ elements,

$$|G| = \sum_{i=1}^{n} |x_i H| = \sum_{i=1}^{n} |H| = |H|(G:H). \qquad \square$$

Let us discuss some corollaries.

COROLLARY 3.25. *If G is a finite group and $g \in G$, then $g^{|G|} = 1$.*

PROOF. By definition. $|g| = |\langle g \rangle|$. Apply Lagrange's theorem to the subgroup $H = \langle g \rangle$ to obtain that

$$g^{|G|} = g^{|H|(G:H)} = (g^{|H|})^{(G:H)} = 1. \qquad \square$$

COROLLARY 3.26. *If G has prime order, then G is cyclic.*

PROOF. Let $g \in G \setminus \{1\}$ and $H = \langle g \rangle$. By Lagrange's theorem, $|H|$ divides $|G|$. Thus $|H| = |G|$, as $|G|$ is prime. Therefore $G = H = \langle g \rangle$. □

COROLLARY 3.27. *If G is a finite abelian group and $g, h \in G$ are elements of finite coprime orders, then $|gh| = |g||h|$.*

PROOF. Let $n = |g|$, $m = |h|$ and $l = |gh|$. Since G is abelian,

$$(gh)^{nm} = (g^n)^m (h^m)^n = 1.$$

Thus l divides nm. Since $(gh)^l = 1$, $g^l = h^{-l} \in \langle g \rangle \cap \langle h \rangle = \{1\}$ (because $|\langle g \rangle| = n$ and $|\langle h \rangle| = m$ are coprime, nm divides l by Lagrange's theorem). □

Fermat's little theorem is a particular case of Lagrange's theorem.

EXERCISE 3.28 (Fermat's little theorem). Let p be a prime number. Prove that

$$a^{p-1} \equiv 1 \bmod p$$

for all $a \in \{1, 2, \dots, p-1\}$.

For the next corollary, we need Euler's totient function. Recall that $\varphi(n)$ is the number of positive integers $k \in \{1, \dots, n\}$ coprime with n. The group of units of $\mathbb{Z}/n$ has $\varphi(n)$ elements (because $x \in \mathbb{Z}/n$ is invertible if and only if x and n are coprime).

EXERCISE 3.29 (Euler's theorem). Let a and n be coprime integers. Prove that

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

The converse of Lagrange's theorem does not hold.

EXAMPLE 3.30. Consider the group

$$\mathbb{A}_4 = \{\mathrm{id}, (234), (243), (12)(34), (123), (124), (132), (134), (13)(24), (142), (143), (14)(23)\}.$$

This is an important subgroup of $\mathbb{S}_4$ known as the **alternating group** in four symbols.

We claim that $\mathbb{A}_4$ has no subgroups of order six. If $H \leq \mathbb{A}_4$ is such that $|H| = 6$, then, since $(\mathbb{A}_4 : H) = 2$, for every $x \notin H$ we can decompose $\mathbb{A}_4$ as as disjoint union $\mathbb{A}_4 = H \cup xH$.

For each $g \in \mathbb{A}_4$ we have that $g^2 \in H$ (if $g \notin H$, then, since $g^2 \in \mathbb{A}_4 = H \cup gH$, it follows that $g^2 \in H$). In particular, since $(ijk) = (ikj)^2$, order-three elements of $\mathbb{A}_4$ belong to H, a contradiction, because $\mathbb{A}_4$ has eight elements of order three.

We all need a favorite group. Mine is $\mathbf{SL}_2(3)$, the group of 2×2 matrices with coefficients in $\mathbb{Z}/3$ and determinant one.

EXERCISE 3.31. Prove that

$$\mathbf{SL}_2(3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1,\, a, b, c, d \in \mathbb{Z}/3 \right\}$$

has order 24 and does not contain subgroups of order 12.

Lecture 4. 07/03/2024

§ 4.1. The symmetric group. Let $\sigma \in \mathbb{S}_n$. We say that the permutation σ is an r-cycle if there are $a_1, \dots, a_r \in \{1, \dots, n\}$ such that $\sigma(j) = j$ for all $j \notin \{a_1, \dots, a_r\}$ and

$$\sigma(a_i) = \begin{cases} a_{i+1} & \text{if } i < r, \\ a_1 & \text{if } i = r. \end{cases}$$

For example, (12), (13) and (23) are 2-cycles of $\mathbb{S}_3$. Note that 2-cycles are called **transpositions**. The permutations (123) and (132) are 3-cycles of $\mathbb{S}_3$.

We say that the permutations $\sigma, \tau \in \mathbb{S}_n$ are **disjoint** if for all $j \in \{1, \dots, n\}$ one has $\sigma(j) = j$ or $\tau(j) = j$. For example, (134) and (25) are disjoint. The permutations (134) and (24) are not disjoint.

If $\sigma \in \mathbb{S}_n$ and j is such that $\sigma(j) = j$, then j is a fixed point of σ. The elements j such that $\sigma(j) \neq j$ are the points moved by σ.

Claim. Disjoint permutations commute.

We now prove that every permutation can be written as product of disjoint cycles. The decomposition is unique up to the order of the factors. We start with a lemma (used to prove the uniqueness of the decomposition).

Lemma 4.1. *Let $\sigma = \alpha\beta \in \mathbb{S}_n$ with α and β disjoint permutations. If $\alpha(i) \neq i$, then $\sigma^k(i) = \alpha^k(i)$ for all $k \geq 0$.*

Proof. Without loss of generality, we may assume that $k > 0$. Let $i \in \{1, \dots, n\}$. Then

$$\sigma^k(i) = (\alpha\beta)^k(i) = \alpha^k(\beta^k(i)) = \alpha^k(i). \qquad \square$$

Theorem 4.2. *Each $\sigma \in \mathbb{S}_n \setminus \{\mathrm{id}\}$ can be written as a product of disjoint cycles of length ≥ 2. The decomposition is unique up to the order of the factors.*

Proof. We proceed by induction on the number k of elements of $\{1, \dots, n\}$ moved by σ. If $k = 2$, the result is trivial. Assume that the result holds for all permutations moving $< k$ points. Let σ be a permutation that moves $k \geq 2$ points and $i_1 \in \{1, \dots, n\}$ be such that $\sigma(i_1) \neq i_1$. We consider the cycle that contains i_1. So let $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$... We know that there exists r such that $\sigma(i_r) = i_1$ (otherwise, if $\sigma(i_r) = i_j$ for some $j \geq 2$, then

$$\sigma(i_{j-1}) = i_j = \sigma(i_r),$$

a contradiction to the bijectivity of σ, as $i_{j-1} \neq i_r$). Let $\sigma_1 = (i_1 \cdots i_r)$. By the inductive hypothesis, since $\sigma_1^{-1}\sigma$ moves $< k$ points (because the i_j are fixed points of $\sigma_1^{-1}\sigma$), we can write

$$\sigma_1^{-1}\sigma = \sigma_2 \cdots \sigma_s,$$

where $\sigma_2, \dots, \sigma_s$ are disjoint cycles. This implies that $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$.

We now prove the uniqueness of the decomposition. Assume that

$$\sigma = \sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_t$$

with $s > 0$. Let $i_1 \in \{1, \dots, n\}$ be such that $\sigma_1(i_1) \neq i_1$. By the previous lemma, $\sigma^k(i_1) = \sigma_1^k(i_1)$ for all $k \geq 0$. There exists $j \in \{1, \dots, t\}$ such that $\tau_j(i_1) \neq i_1$. Since the t_k's commute, without loss of generality, we may assume that $j = 1$. Thus $\sigma^k(i_1) = \tau_1^k(i_1)$ for all $k \geq 0$. This implies that $\sigma_1 = \tau_1$, as σ_1 and τ_1 are cycles. Thus $\sigma_2 \cdots \sigma_s = \tau_2 \cdots \tau_t$. Repeating this procedure, we obtain that $s = t$. Therefore $\sigma_j = \tau_j$ for all j. $\square$

COROLLARY 4.3.

1) $\mathbb{S}_n = \langle (ij) : i < j \rangle$.
2) $\mathbb{S}_n = \langle (12), (13), \dots, (1n) \rangle$.
3) $\mathbb{S}_n = \langle (12), (23), \dots, (n-1\,n) \rangle$.
4) $\mathbb{S}_n = \langle (12), (12\cdots n) \rangle$.

PROOF. The first claim follows from the previous theorem, as

$$(a_1 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2).$$

If we write $\sigma \in \mathbb{S}_n$ as a product of disjoint cycles, the previous formula implies that $\mathbb{S}_n \subseteq \langle (ij) : i < j \rangle$. The other inclusion is trivial.

For the second claim, one uses the first claim and the formulas

$$(1i)(1j)(1i) = (ij),$$

where $i \neq j$.

To prove the third claim, write σ as a product of transpositions and note that

$$(13) = (12)(23)(12), \quad (1\,k+1) = (k\,k+1)(1k)(k\,k+1)$$

for all $k \geq 3$.

Finally, the fourth claim follows from the third claim and the formula

$$(12\cdots n)^{k-1}(12)(12\cdots n)^{1-k} = (k\,k+1),$$

where $k \geq 1$. $\square$

Here is an alternative proof of the first claim of Corollary 4.3. We must show that every permutation can be written as a product of transpositions. Let us assume that n persons are invited to a concert. They sit in the first row without following the seat number on their tickets. How can we put each person in the right seat? First, we locate the person that should be seated in the first place. Then we ask this person to interchange seats with the person seated in the first place. Then we identify the person that should be seated in the second spot. We then ask this person to interchange seats with the person seated in the second spot. We do the same with the third spot, the fourth spot... Once the process is finished, we have decomposed our permutation into a product of transpositions.

EXERCISE 4.4. Following the tricks of the proof of Corollary 4.3, find the different decompositions of the permutation $(1324)(56)(789) \in \mathbb{S}_9$.

Every permutation yields a permutation matrix. For example, the matrix corresponding to $\sigma = \mathrm{id} \in \mathbb{S}_3$ is the 3×3 identity matrix. The permutation $\sigma = (123)$ yields the matrix

$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

If e_1, e_2, e_3 is the standard basis of $\mathbb{R}^{3\times 1}$, then

$$P_\sigma(e_1) = e_2, \quad P_\sigma(e_2) = e_3, \quad P_\sigma(e_3) = e_1.$$

We can write P_σ as a sum of elementary matrices:

$$P_\sigma = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

In general, the permutation matrix P_σ associated with a permutation $\sigma \in \mathbb{S}_n$, permutes the elements of the standard basis of $\mathbb{R}^{n\times 1}$ in the way σ permutes the elements of $\{1,2,\dots,n\}$.

Recall that the **elementary matrix** $E_{i,j}$ is the matrix with a one in position (i,j) and zero in all other entries. Recall the following formulas:

$$E_{i,j}E_{k,l} = \begin{cases} E_{i,l} & \text{if } j=k, \\ 0 & \text{if } j \neq k \end{cases}$$

EXERCISE 4.5. Let $\sigma \in \mathbb{S}_n$. Prove that

$$P_\sigma = \sum_{i=1}^{n} E_{\sigma(i),i}.$$

The determinant of a permutation matrix equals ± 1. Why?

PROPOSITION 4.6. *If $\sigma, \tau \in \mathbb{S}_n$, then $P_{\sigma\tau} = P_\sigma P_\tau$.*

PROOF. We compute

$$\begin{aligned} P_\sigma P_\tau &= \left(\sum_{i=1}^{n} E_{\sigma(i),i}\right)\left(\sum_{j=1}^{n} E_{\tau(j),j}\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} E_{\sigma(i),i}E_{\tau(j),j} \\ &= \sum_{j=1}^{n} E_{\sigma(\tau(j)),j} \\ &= P_{\sigma\tau}, \end{aligned}$$

where the double sum is zero unless $i = \tau(j)$. □

DEFINITION 4.7. The **sign** of a permutation $\sigma \in \mathbb{S}_n$ is the determinant of the matrix P_σ, that is $\operatorname{sign}(\sigma) = \det P_\sigma$. A permutation σ is said to be **even** if $\operatorname{sign}(\sigma) = 1$ and **odd** if $\operatorname{sign}(\sigma) = -1$.

The identity is an even permutation. Every 3-cycle is an even permutation. Each transposition is an odd permutation.

PROPOSITION 4.8. *If $\sigma, \tau \in \mathbb{S}_n$, then* $\operatorname{sign}(\sigma\tau) = (\operatorname{sign}\sigma)(\operatorname{sign}\tau)$.

PROOF. We compute

$$\operatorname{sign}(\sigma\tau) = \det(P_\sigma P_\tau) = (\det P_\sigma)(\det P_\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau).$$ □

Each permutation can be written as a product of transpositions. There is no uniqueness of this decomposition. For example,

$$(13) = (12)(23)(12) = (12)(23)(12)$$

However, the following result holds: If $\sigma = \sigma_1 \cdots \sigma_s$ is a product of transpositions, then $\operatorname{sign}(\sigma) = (-1)^s$. In particular, σ is even if and only if s is even.

EXAMPLE 4.9. We claim that if $n \geq 3$ then $Z(\mathbb{S}_n) = \{\mathrm{id}\}$. Assume that $Z(\mathbb{S}_n) \neq \{\mathrm{id}\}$. Let $\sigma \in Z(\mathbb{S}_n)$ be such that $\sigma(i) = j$ for some $i \neq j$. Since $n \geq 3$, there exists $k \in \{1,\dots,n\} \setminus \{i,j\}$. Thus $\tau = (jk) \in \mathbb{S}_n$. Since σ is central,

$$j = \sigma(i) = \tau\sigma\tau^{-1}(i) = \tau(\sigma(i)) = \tau(j) = k,$$

a contradiction.

DEFINITION 4.10. The **alternating group**

$$\mathbb{A}_n = \{\sigma \in \mathbb{S}_n : \mathrm{sign}(\sigma) = 1\}$$

is the subgroup of $\mathbb{S}_n$ formed by even permutations.

PROPOSITION 4.11. $|\mathbb{A}_n| = n!/2$.

PROOF. Let $\sigma = (12) \notin \mathbb{A}_n$. We claim that $\mathbb{S}_n = \mathbb{A}_n \cup \mathbb{A}_n\sigma$ (disjoint union), where

$$\mathbb{A}_n\sigma = \{\tau\sigma : \tau \in \mathbb{A}_n\}$$

is the right coset of $\mathbb{A}_n$ in $\mathbb{S}_n$ with representative σ. (We could have used, of course, left cosets.) If $\tau \in \mathbb{S}_n$ is such that $\tau \notin \mathbb{A}_n$, then

$$\mathrm{sign}(\tau\sigma) = (\mathrm{sign}\,\tau)(\mathrm{sign}\,\sigma) = 1.$$

Thus $\tau\sigma \in \mathbb{A}_n$. Therefore $\tau \in \mathbb{A}_n\sigma$. Since $|\mathbb{A}_n\sigma| = |\mathbb{A}_n|$ (because the map $\mathbb{A}_n \to \mathbb{A}_n\sigma$, $x \mapsto x\sigma$, is bijective), we conclude that $n! = |\mathbb{S}_n| = 2|\mathbb{A}_n|$. □

A direct calculation shows that

$$\mathbb{A}_3 = \{\mathrm{id}, (123), (132)\}.$$

The group $\mathbb{A}_3$ is abelian. In Example 3.30, we used the alternating group

$$\mathbb{A}_4 = \{\mathrm{id}, (234), (243), (12)(34), (123), (124), (132), (134), (13)(24), (142), (143), (14)(23)\}.$$

If $n \geq 4$, then $\mathbb{A}_n$ is non-abelian. For example, (123) and (124) do not commute.

PROPOSITION 4.12. $\mathbb{A}_n = \langle\{\text{3-cycles}\}\rangle$.

PROOF. Each 3-cycle is an even permutation, as $(ijk) = (ik)(ij)$. To prove the other inclusion, let $\sigma \in \mathbb{A}_n$. Write $\sigma = \sigma_1 \cdots \sigma_s$ for some even integer s and transpositions $\sigma_1, \dots, \sigma_s$. Now the claim follows from the formulas

$$(kl)(ij) = (kl)(ki)(ki)(ij) = (kil)(ijk), \quad (ik)(ij) = (ijk).$$ □

Proposition 4.12 has several important applications.

EXERCISE 4.13. Prove that $[\mathbb{A}_4 : \mathbb{A}_4] = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

EXAMPLE 4.14. If $n \geq 5$, then $[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n$. To prove the non-trivial inclusion, it is enough to note that $\mathbb{A}_n$ is generated by 3-cycles and that, since $n \geq 5$, each 3-cycle is a product of commutators:

$$(abc) = [(acd), (ade)][(ade), (abd)],$$

where $\#\{a,b,c,d,e\} = 5$.

EXAMPLE 4.15. If $n \geq 3$, then $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$. First, we prove that $[\mathbb{S}_n, \mathbb{S}_n] \subseteq \mathbb{A}_n$. If $\sigma \in [\mathbb{S}_n, \mathbb{S}_n]$, say $\sigma = [\sigma_1, \tau_1][\sigma_2, \tau_2] \cdots [\sigma_k, \tau_k]$, then

$$\operatorname{sign}(\sigma) = \operatorname{sign}([\sigma_1, \tau_1]) \cdots \operatorname{sign}([\sigma_k, \tau_k]) = 1.$$

Conversely, if $\sigma \in \mathbb{A}_n$, by the previous proposition, we can write σ as a product of 3-cycles. From this, the claim follows, as each 3-cycle is a commutator:

$$(abc) = (ab)(ac)(ab)(ac) = [(ab), (ac)] \in [\mathbb{S}_n, \mathbb{S}_n].$$

Lecture 5. 14/03/2024

§ 5.1. Quotients. If G is a group and N is a subgroup of G, we want to know when the set G/N of left cosets of N in G is a group with the operation

$$G/N \times G/N \to G/N, \quad (xN, yN) \mapsto xyN, \tag{5.1}$$

that is, when this operation is well-defined. What does this mean? We need to check that (5.1) is indeed a function. For that purpose, we need to prove that (5.1) does not depend on the representatives of left cosets used. Thus we need to show that $xN = x_1N$ and $yN = y_1N$, then $xyN = x_1y_1N$.

Let us try to understand this condition. If $x^{-1}x_1 \in N$ and $y^{-1}y_1 \in N$, then $x_1 = xn$ and $y_1 = ym$ for some $m, n \in N$. Thus

$$(xy)^{-1}(x_1y_1) = y^{-1}x^{-1}x_1y_1 = y^{-1}nym \in N$$

if and only if $y^{-1}ny \in N$.

Example 5.1. If $G = \mathbb{S}_3$ and $H = \langle (12) \rangle$, then $(xN, yN) \mapsto xyN$ is not a function. Recall that $G/N = \{N, (123)N, (132)N\}$, where $N = (12)N$, $(123)N = (13)N$ and $(132)N = (23)N$. Then

$$(132)N = (13)(23)N = (13)N(23)N = (123)N(132)N = N,$$

a contradiction.

Definition 5.2. Let G be a group. A subgroup N of G is said to be **normal** if $gNg^{-1} \subseteq N$ for all $g \in G$. Notation: If N is normal in G, then $N \trianglelefteq G$.

In an abelian group, every subgroup is normal.

Proposition 5.3. *Let N be a subgroup of G. The following statements are equivalent:*

1) *$gNg^{-1} \subseteq N$ for all $g \in G$.*
2) *$gNg^{-1} = N$ for all $g \in G$.*
3) *$gN = Ng$ for all $g \in G$.*

Proof. We only prove that 1) $\implies$ 2), as the other implications are trivial. If $n \in N$ and $g \in G$, then $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$. □

Proposition 5.4. *Let N be a subgroup of G. The following statements are equivalent:*

1) *N is normal in G.*
2) *$(gN)(hN) = (gh)N$ for all $g, h \in G$.*

Proof. We first prove that 1) $\implies$ 2). Let $g \in G$. Since $gNg^{-1} = N$,

$$(gN)(hN) = g(Nh)N = g(hN)N = (gh)N.$$

We now prove that 2) $\implies$ 1). If $g \in G$, then

$$gNg^{-1} \subseteq (gN)(g^{-1}N) = (gg^{-1})N = N.$$ □

If G is a group, then $\{1\}$ and G are always normal subgroups.

Example 5.5. If G is a group, then $Z(G)$ is a normal subgroup of G. Moreover, if $N \leq Z(G)$, then $N \trianglelefteq G$.

EXAMPLE 5.6. If G is a group, then $[G,G]$ is a normal subgroup of G. If $x \in [G,G]$ and $g \in G$, then $gxg^{-1} = (gxg^{-1}x^{-1})x = [g,x]x \in [G,G]$. Alternatively,

$$g\left(\prod_{i=1}^{k}[x_i,y_i]\right)g^{-1} = \prod_{i=1}^{k}[gx_ig^{-1},gy_ig^{-1}]$$

for all $g,x_1,\dots,x_k,y_1,\dots,y_k \in G$.

EXAMPLE 5.7. Let $n \geq 2$. Then $\mathbb{A}_n$ is a normal subgroup of $\mathbb{S}_n$. If $\sigma \in \mathbb{A}_n$ and $\tau \in \mathbb{S}_n$, then $\tau\sigma\tau^{-1} \in \mathbb{A}_n$, as

$$\operatorname{sign}(\tau\sigma\tau^{-1}) = \operatorname{sign}(\sigma) = 1.$$

EXAMPLE 5.8. If N is a subgroup of G such that $(G:N) = 2$, then N is normal in G. We need to show that $gN = Ng$ for all $g \in G$. Let $g \in G$. If $g \in N$, then $gN = Ng$. If $g \notin N$, then $gN \neq N$. Since $(G:N) = 2$, we can decompose G as the disjoint union $G = N \cup gN$. Hence $gN = G \setminus N$. Similarly, $Ng = G \setminus N$ and therefore $gN = Ng$.

EXAMPLE 5.9. As a particular case of the previous example, $\langle(123)\rangle = \{\mathrm{id},(123),(132)\} \trianglelefteq \mathbb{S}_3$. Note that $\langle(12)\rangle = \{\mathrm{id},(12)\}$ is not normal in $\mathbb{S}_3$. For example, $(13)(12)(13) = (23) \notin \langle(12)\rangle$.

EXAMPLE 5.10. The subgroup $\mathbf{SL}_n(\mathbb{R})$ is normal in $\mathbf{GL}_n(\mathbb{R})$. If $g \in \mathbf{GL}_n(\mathbb{R})$ and $x \in \mathbf{SL}_n(\mathbb{R})$, then $\det(gxg^{-1}) = (\det g)(\det x)(\det g)^{-1} = 1$.

EXAMPLE 5.11. The Klein group $K = \{\mathrm{id},(12)(34),(13)(24),(14)(23)\}$ is normal in $\mathbb{S}_4$. We need to show that $\sigma K\sigma^{-1} \subseteq K$ for all $\sigma \in \mathbb{S}_4$. Do we need to check this for every element of $\mathbb{S}_4$? No. One always has tricks! Recall that $\mathbb{S}_4$ is generated by (12) and (1234). Since every element of $\mathbb{S}_4$ is a word on (12) and (1234), it is enough to see that $\sigma K\sigma^{-1} \subseteq K$ for all $\sigma \in \{(12),(1234)\}$. We left as an exercise to show that

$$(12)K(12)^{-1} \subseteq K, \quad (1234)K(1234)^{-1} \subseteq K.$$

EXERCISE 5.12. Let $G = \mathbb{R} \times \mathbb{R}^{\times}$ with the operation

$$(x,y)(u,v) = (x+yu,yv).$$

Prove that $\{(x,1) : x \in \mathbb{R}\}$ is normal in G and that $\{(0,y) : y \in \mathbb{R}^{\times}\}$ is not.

Let us compute the list of normal subgroups of $\mathbb{A}_4$.

EXAMPLE 5.13. We claim that $\{\mathrm{id}\}$, $K = \{\mathrm{id},(12)(34),(13)(24),(14)(23)\}$ and $\mathbb{A}_4$ are the normal subgroups of $\mathbb{A}_4$.

Since $\mathbb{A}_4 = \{\text{3-cycles}\} \cup K$, K is the only subgroup of $\mathbb{A}_4$ of order four. This implies that K is normal in $\mathbb{A}_4$ (because every conjugate gKg^{-1} of K is a subgroup of $\mathbb{A}_4$ of order four). Let $N \neq \{\mathrm{id}\}$ be a normal subgroup of $\mathbb{A}_4$.

If N contains a 3-cycle, say $(abc) \in N$, then

$$(acd) = (bcd)(abc)(bcd)^{-1} \in N$$

and hence $N = \mathbb{A}_4$ (because N contains every 3-cycle).

Assume that N does not contain 3-cycles. Then some non-trivial element of K belongs to N, say $(ab)(cd) \in N$. Hence

$$(ac)(bd) = (bcd)(ab)(cd)(bcd)^{-1} \in N, \quad (ad)(bc) = (ab)(cd)(ac)(bd) \in N$$

and therefore $N = K$.

Normality is not transitive.

EXERCISE 5.14. Let $G = \mathbb{D}_4$ be the dihedral group of order eight. Let $N = \langle s, r^2 \rangle$ and $H = \langle s \rangle$. Prove that H is normal in N, N is normal in G but H is not normal in G.

EXAMPLE 5.15. We claim that $\{\mathrm{id}\}$, K, $\mathbb{A}_4$ and $\mathbb{S}_4$ are the normal subgroups of $\mathbb{S}_4$.

Let N be a normal subgroup of $\mathbb{S}_4$. If $N \subseteq \mathbb{A}_4$, then N is normal in $\mathbb{A}_4$ and hence either $N = \{\mathrm{id}\}$, $N = K$ or $N = \mathbb{A}_4$. Assume that $N \not\subseteq \mathbb{A}_4$, that is N contains an odd permutation. If $\sigma \in \mathbb{S}_4$ is odd, then σ is either a transposition or a 4-cycle.

If N contains a transposition, then all transpositions belong to N, as

$$\tau(i\,j)\tau^{-1} = (\tau(i)\,\tau(j))$$

for all $\tau \in \mathbb{S}_4$. In this case, $N = \mathbb{S}_4$ because the transpositions generate $\mathbb{S}_4$.

If N contains a 4-cycle, all 4-cycles belong to N, as

$$\tau(i\,jkl)\tau^{-1} = (\tau(i)\,\tau(j)\,\tau(k)\,\tau(l))$$

for all $\tau \in \mathbb{S}_4$ and $K \subseteq N$ because

$$(ac)(bd) = (abcd)^2.$$

This implies that $|N| \geq 10$. Since $K \subseteq N$, $|N \cap \mathbb{A}_4| \geq 5$. Moreover, $N \cap \mathbb{A}_4$ is a normal subgroup of $\mathbb{A}_4$. Hence $N \cap \mathbb{A}_4 = \mathbb{A}_4 \subseteq N$. Since $N \neq \mathbb{A}_4$, $|N| > 12$ and hence $N = \mathbb{S}_4$.

The following theorem is crucial.

THEOREM 5.16. *If N is a normal subgroup of G, then G/N is a group with the operation $(xN)(yN) = (xy)N$.*

EXERCISE 5.17. Prove Theorem 5.16.

We will see examples of quotient groups later.

EXERCISE 5.18. Let H be a normal subgroup of G. Prove that G/H is abelian if and only if $[G, G] \subseteq H$.

As an application, we compute the commutator subgroup of $\mathbb{A}_4$.

EXAMPLE 5.19. $[\mathbb{A}_4, \mathbb{A}_4] = K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. We know that K is normal in $\mathbb{A}_4$. Since $\mathbb{A}_4/K$ has order three, it is abelian. Then $[\mathbb{A}_4, \mathbb{A}_4] \subseteq K$. Since

$$(ab)(cd) = [(abc), (cda)],$$

we conclude that $K \subseteq [\mathbb{A}_4, \mathbb{A}_4]$.

EXERCISE 5.20. If $G/Z(G)$ is cyclic, then G is abelian.

EXERCISE 5.21. If S is a subgroup of G, the **normalizer** of S in G is the set

$$N_G(S) = \{g \in G : gSg^{-1} = S\}.$$

Prove the following statements:

1) $N_G(S) \leq G$.
2) $S \trianglelefteq N_G(S)$.
3) If $S \leq T \leq G$ and $S \trianglelefteq T$, then $T \leq N_G(S)$.

The normalizer of a subgroup S in G is the largest subgroup of G that contains S as a normal subgroup.

DEFINITION 5.22. A group G is **simple** if $G \neq \{1\}$ and G and $\{1\}$ are the only normal subgroups of G.

If p is a prime number, then Lagrange's theorem implies that $\mathbb{Z}/p$ is a simple group. For $n \geq 5$, the alternating group $\mathbb{A}_n$ is simple. However, we will not prove this in this course.

EXERCISE 5.23. Let H be a subgroup of G such that $p = (G : H)$ is a prime number. Prove that the following statements are equivalent:

1) H is normal in G.
2) If $g \in G \setminus H$, then $g^p \in H$.
3) If $g \in G \setminus H$, then $g^n \in H$ for some n with no prime divisors $< p$.
4) If $g \in G \setminus H$, then $g^k \notin H$ for all $k \in \{2, \dots, p-1\}$.

We now present two applications of the previous exercise.

EXERCISE 5.24. Let G be a finite group and p be the smallest prime number dividing G. Prove that if H is a subgroup of G with $(G : H) = p$, then H is normal in G.

EXERCISE 5.25. Let p be a prime number and G be a group such that every element of G has order a power of p. If H is a subgroup of G of index p, then H is normal in G.

Lecture 6. 21/03/2024

§ 6.1. Permutable subgroups. If H and K are subgroups of G, let

$$HK = \{hk : h \in H, k \in K\}.$$

Note that

$$H \cup K \subseteq HK \subseteq \langle H \cup K \rangle.$$

When HK is a subgroup of G? Note that $HK \leq G$ if and only if $\langle H \cup K \rangle = HK$.

Proposition 6.1. *Let H and K be subgroups of G. Then HK is a subgroup of G if and only if $HK = KH$.*

Proof. Assume that $HK = KH$. Since $1 \in H \cap K$, $HK \neq \emptyset$. If $h \in H$ and $k \in K$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Moreover,

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK.$$

Thus HK is closed under multiplication.

Now assume that HK is a subgroup of G. Since $H \subseteq HK$, $K \subseteq HK$ and HK closed under multiplication, $KH \subseteq (HK)(HK) \subseteq HK$. Conversely, let $g \in HK$. Since $g^{-1} \in HK$, there exist $h \in H$ and $k \in K$ such that $g^{-1} = hk$. Thus $HK \subseteq KH$, as $g = k^{-1}h^{-1} \in KH$. □

Exercise 6.2. Let H and K be subgroups of G. Prove that if H is normal in G, then HK is a subgroup of G.

Example 6.3. Let $G = \mathbb{S}_4$. The subgroups $H = \langle (12) \rangle$ and $K = \langle (34) \rangle$ are such that

$$HK = KH = \{\mathrm{id}, (12), (34), (12)(34)\}$$

is a subgroup of $\mathbb{S}_4$. Note that not H nor K are normal in G.

Exercise 6.4. Let G be a group and S be a subgroup of G. If $T \leq N_G(S)$, then TS is a group and $S \leq TS$.

Two subgroups H and K of G are said to be **permutable** if $HK = KH$.

Theorem 6.5. *Let H and K be finite subgroups of G. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Let $L = H \cap K$. We decompose H as a disjoint union of left coclases of L, say $H = \cup_{i=1}^{k} x_i L$, where $k = (H : L)$. Note that $LK = K$, as $L \subseteq K$ and $K \subseteq 1K \subseteq LK$. Then

$$HK = \bigcup_{i=1}^{k} x_i LK = \bigcup_{i=1}^{k} x_i K,$$

In particular, since the union is disjoint,

$$|HK| = \sum_{i=1}^{k} |x_i K| = k|K| = \frac{|H||K|}{|H \cap K|}.$$ □

In the theorem, we do not assume that HK is a subgroup of G.

As an application, the theorem yields a different solution to Exercise 5.24 of page 26. If $\{gHg^{-1} : g \in G\} = \{H\}$, then H is normal in G. Assume that there exists $g \in G$ such that $H \neq g^{-1}Hg = K$. Since $(H : H \cap K)$ divides $|H|$ and all prime divisors of $|G|$ are $\geq p$, it follows that $(H : H \cap K) \geq p$. Thus

$$|HK| = \frac{|H||K|}{|H \cap K|} \geq p|K| = |G|$$

as $(G : H) = p$ and $|K| = |H|$. In particular, $HK = G$. Since $K = g^{-1}Hg$, $g = h(g^{-1}h_1g)$ for some $h, h_1 \in H$. Thus

$$1 = hg^{-1}h_1 \implies h_1h = g \in H \implies H = K,$$

a contradiction.

Example 6.6. Let $G = \mathbb{S}_3$, $H = \langle(12)\rangle$ and $K = \langle(23)\rangle$. Then

$$HK = \{\mathrm{id}, (12), (23), (123)\}$$

is not a subgroup of G, as by Lagrange's theorem, G cannot have subgroups of four elements. Another way to see that HK is not a subgroup of G follows from the fact that

$$KH = \{\mathrm{id}, (12), (23), (132)\} \neq HK.$$

Example 6.7. Let $G = \mathbb{S}_3$, $H = \langle(12)\rangle$ and $K = \langle(123)\rangle$. Since K is normal in G, HK is a subgroup of G. By Lagrange's theorem, $|HK| = 6$ and hence $G = HK$. Each $g \in G$ can be written uniquely as $g = hk$ for some $h \in H$ and $k \in K$ (one can prove this either considering all possible cases or using the fact that $H \cap K = \{\mathrm{id}\}$). It follows that the map

$$H \times K \to G, \quad (h,k) \mapsto hk,$$

is bijective. Note that this bijective map is not compatible with the operation of G, as

$$(h_1k_1)(h_2k_2) \neq (h_1h_2)(k_1k_2).$$

§ 6.2. Homomorphisms.

Definition 6.8. Let G and H be groups. A map $f\colon G \to H$ is said to be a **group homomorphism** if $f(xy) = f(x)f(y)$ for all $x, y \in G$.

If $f\colon G \to H$ is a group homomorphism, then $f(1) = 1$. Why?

If a group homomorphism is injective, it will be called a **monomorphism**. If it is subjective, an **epimorphism**. If it is bijective, an **isomorphism**. Two groups G and H are said to be **isomorphic** (notation: $G \simeq H$) is there exists an isomorphism $G \to H$.

Example 6.9.

1) If G is a group, the identity map $\mathrm{id}\colon G \to G$ is a group homomorphism.
2) If G and H are groups, the map $e\colon G \to H$, $e(g) = 1_H$, is a group homomorphism.
3) For each $n \in \mathbb{Z}$, the map $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto nx$, is a group homomorphism.
4) If G is an abelian group and $n \in \mathbb{Z}$, the map $G \to G$, $g \mapsto g^n$, is a group homomorphism.

Example 6.10. Let G be a group and $g \in G$. The map $\gamma_g\colon G \to G$, $\gamma_g(x) = gxg^{-1}$, is called **conjugation** by g and it is a group homomorphism.

Example 6.11. The map $\exp\colon \mathbb{R} \to \mathbb{R}^\times$, $\exp(x) = e^x$, is a group homomorphism.

Example 6.12. The inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an injective group homomorphism.

Generally, if S is a subgroup of G, then the **inclusion map** $S \hookrightarrow G$ is a group homomorphism.

EXAMPLE 6.13. The determinant $\det\colon \mathbf{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism.

EXAMPLE 6.14. Let $f\colon G \to H$ be a group homomorphism and S be a subgroup of G. The **restriction** $f|_S\colon S \to H$ is a group homomorphism.

EXAMPLE 6.15. The map $f\colon \mathbb{R} \to \mathbb{C}^\times$, $f(x) = \cos x + i \sin x$, is a group homomorphism, as $f(x+y) = f(x)f(y)$ for all $x, y \in \mathbb{R}$.

EXERCISE 6.16. Let $f\colon G \to H$ be a group homomorphism. Prove the following properties:

1) $f(1) = 1$.
2) $f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.
3) $f(g^n) = f(g)^n$ for all $g \in G$ and $n \in \mathbb{Z}$.

EXAMPLE 6.17. Let $f\colon \mathbb{R}_{>0} \to \mathbb{R}$, $f(x) = \log(x)$. The formula

$$\log(xy) = \log(x) + \log(y)$$

implies that f is a group homomorphism. The previous exercise resembles the following properties of the logarithm function:

$$\log(1) = 0, \quad \log\left(\frac{1}{x}\right) = -\log(x), \quad \log(x^n) = n\log(x).$$

DEFINITION 6.18. Let $f\colon G \to H$ be a group homomorphism. The **kernel** of f is the set $\ker f = \{x \in G : f(x) = 1\}$.

The following property of the kernel is crucial: If $f\colon G \to H$ is a group homomorphism, then $f(x) = f(y)$ if and only if $x = yk$ for some $k \in \ker f$.

EXAMPLE 6.19. Let $f\colon \mathscr{U}(\mathbb{Z}/21) \to \mathscr{U}(\mathbb{Z}/21)$, $f(x) = x^3$. Then f is a group homomorphism and $\ker f = \{1, 4, 16\}$ and $f(\mathscr{U}(\mathbb{Z}/21)) = \{1, 8, 13, 20\}$.

EXERCISE 6.20. Let

$$\mathrm{Aff}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^\times, b \in \mathbb{R} \right\} \leq \mathbf{GL}_2(\mathbb{R}).$$

Prove that the map

$$f\colon \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}^\times, \quad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$$

is a group homomorphism such that

$$\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}.$$

Show that $g\colon \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}$, $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto b$, is not a group homomorphism.

EXAMPLE 6.21. Sea $f\colon \mathbb{R} \to \mathbb{C}^\times$, $f(x) = \cos x + i \sin x$. Then

$$\ker f = \{2\pi k : k \in \mathbb{Z}\} = 2\pi\mathbb{Z}.$$

DEFINITION 6.22. The **image** of a group homomorphism $f\colon G\to H$ is the set

$$f(G)=\{f(x):x\in G\}.$$

PROPOSITION 6.23. *Let $f\colon G\to H$ be a group homomorphism. The following properties hold:*

1) $\ker f$ *is a normal subgroup of* G.

2) $f(G)$ *is a subgroup of* H.

PROOF. We only prove the first claim. We first need to show that $\ker f$ is a subgroup of G. Note that $1\in\ker f$. If $x,y\in\ker f$, then $xy^{-1}\in\ker f$ (because f is a group homomorphism, $f(xy^{-1})=f(x)f(y)^{-1}=1$). Now we prove that $\ker f$ is normal in G. Let $x\in\ker f$ and $g\in G$. Then $gxg^{-1}\in\ker f$, as

$$f(gxg^{-1})=f(g)f(x)f(g)^{-1}=f(g)f(g)^{-1}=1. \qquad\square$$

The image of a group homomorphism is not always a normal subgroup.

EXAMPLE 6.24. The inclusion map $\langle(12)\rangle\hookrightarrow\mathbb{S}_3$ is a group homomorphism. Its image is not a normal subgroup of $\mathbb{S}_3$.

EXAMPLE 6.25. Recall that $\mathscr{U}(\mathbb{Z}/21)=\{1,2,4,5,8,10,11,13,16,17,19,20\}$ is an abelian group. The map $f\colon\mathscr{U}(\mathbb{Z}/21)\to\mathscr{U}(\mathbb{Z}/21)$, $f(x)=x^3$, is a group homomorphism. The image of f equals $\{1,8,13,20\}$, a subgroup of $\mathscr{U}(\mathbb{Z}/21)$.

EXAMPLE 6.26. The map $\mathrm{sign}\colon\mathbb{S}_n\to\{-1,1\}$ is a surjective group homomorphism such that $\ker(\mathrm{sign})=\mathbb{A}_n$. In particular, $\mathbb{A}_n$ is a normal subgroup of $\mathbb{S}_n$.

EXAMPLE 6.27. If N is a normal subgroup of G, the map $\pi\colon G\to G/N$, $x\mapsto xN$, is a subjective group homomorphism such that $\ker\pi=N$. The map π is called the **canonical homomorphism** $G\to G/N$.

The previous example implies that every normal subgroup of a group G is the kernel of a group homomorphism with domain G.

EXERCISE 6.28. Let $f\colon G\to H$ be a group homomorphism. Prove the following statements:

1) If $S\leq G$, then $f(S)\leq H$ and $f^{-1}(f(S))=S\ker f$.

2) If $T\leq H$, then $\ker f\leq f^{-1}(T)\leq G$ and $f(f^{-1}(T))=T\cap f(G)$.

3) f is injective if and only if $\ker f=\{1\}$.

4) If $g\in G$ has finite order, then $|f(g)|$ divides $|g|$.

If $f\colon G\to H$ is a group isomorphism, then $f^{-1}\colon H\to G$ is an isomorphism. A group homomorphism $f\colon G\to H$ is an isomorphism if and only if there exists a group homomorphism $g\colon H\to G$ such that $g\circ f=\mathrm{id}_G$ and $f\circ g=\mathrm{id}_H$.

EXAMPLE 6.29. $\mathbb{S}_2\simeq\mathbb{Z}/2\simeq G_2$.

EXAMPLE 6.30. $\mathbb{D}_3\simeq\mathbb{S}_3$ and an isomorphism is given by $\mathbb{D}_3\to\mathbb{S}_3$,

$$1\mapsto\mathrm{id},\quad r\mapsto(123),\quad r^2\mapsto(132),\quad s\mapsto(12),\quad rs\mapsto(13),\quad r^2s\mapsto(23).$$

EXAMPLE 6.31. $\mathbb{Z}/2\times\mathbb{Z}/3\simeq\mathbb{Z}/6$ and an isomorphism is given by

$$(0,0)\mapsto 0,\quad(1,0)\mapsto 3,\quad(0,1)\mapsto 4,\quad(1,1)\mapsto 1,\quad(0,2)\mapsto 2,\quad(1,2)\mapsto 5.$$

EXAMPLE 6.32. The map $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ is a group homomorphism. Since log is bijective, $\mathbb{R}_{>0} \simeq \mathbb{R}$.

If $f\colon G \to H$ is an isomorphism, then $|g| = |f(g)|$ for all $g \in G$.

EXAMPLE 6.33. $\mathbb{Z}/2 \times \mathbb{Z}/2 \not\simeq \mathbb{Z}/4$, as $\mathbb{Z}/2 \times \mathbb{Z}/2$ has no elements of order four.

EXAMPLE 6.34. $\mathbb{Q}/\mathbb{Z} \not\simeq \mathbb{Q}$. Both groups are abelian, but they are not isomorphic. To show this, note that every non-trivial element of $\mathbb{Q}$ has infinite order (if $kx = 0$ for some $k \in \mathbb{Z}$ and $x \in \mathbb{Q} \setminus \{0\}$, then $k = 0$). However, every non-trivial element of $\mathbb{Q}/\mathbb{Z}$ has finite order. In fact, if $x = r/s \in \mathbb{Q}$, then, since

$$s(x+\mathbb{Z}) = sx+\mathbb{Z} = r+\mathbb{Z} = \mathbb{Z}$$

we conclude that $|x+\mathbb{Z}| \leq s$.

EXAMPLE 6.35. Note that $\mathscr{U}(\mathbb{Z}/5) \simeq \mathscr{U}(\mathbb{Z}/10)$, as both groups are cyclic of order four.

EXERCISE 6.36. Prove that $\mathscr{U}(\mathbb{Z}/10) \not\simeq \mathscr{U}(\mathbb{Z}/12)$.

EXERCISE 6.37. Prove that $F = \{\sigma \in \mathbb{S}_n : \sigma(n) = n\} \leq \mathbb{S}_n$ and $F \simeq \mathbb{S}_{n-1}$.

If G and H are groups, let

$$\mathrm{Hom}(G,H) = \{f\colon G \to H : f \text{ is a group homomorphism}\}.$$

EXAMPLE 6.38. We claim that $\mathrm{Hom}(\mathbb{Q},\mathbb{Z}) = \{0\}$. Let $f \in \mathrm{Hom}(\mathbb{Q},\mathbb{Z})$ and p be a prime number. If $x \in \mathbb{Q}$, then, since

$$f(x) = f\left(p(x/p)\right) = pf(x/p),$$

p divides $f(x)$. It follows that $f(x) = 0$ for all $x \in \mathbb{Q}$, as p is arbitrary.

EXAMPLE 6.39. If G is a group, then $\mathrm{Hom}(\mathbb{Z},G) = \{k \mapsto g^k : g \in G\}$. For each $g \in G$, the map $\mathbb{Z} \to G$, $k \mapsto g^k$, is a group homomorphism, as $k+l \mapsto g^{k+l} = g^k g^l$. Let $f \in \mathrm{Hom}(\mathbb{Z},G)$ and $g = f(1)$. If $k > 0$,

$$f(k) = f(\underbrace{1+\cdots+1}_{k-\text{times}}) = f(1)^k = g^k.$$

If $k < 0$, then

$$f(k) = f(\underbrace{(-1)+\cdots+(-1)}_{|k|-\text{times}}) = f(-1)^{-k} = (g^{-1})^{-k} = g^k.$$

EXAMPLE 6.40. We claim that $\mathrm{Hom}(\mathbb{Z}/8,\mathbb{Z}/10)$ has exactly two elements. Let $f\colon \mathbb{Z}/8 \to \mathbb{Z}/10$ be a non-trivial homomorphism. If $n = |f(1)|$, then n divides 8, that is $n \in \{1,2,4,8\}$. Since $f(1) \in \mathbb{Z}/10$ and f is non-trivial, $n = 2$. Thus $f(1) = 5$ and f is univocally determined. This means that $f(k) = 5k$ for $k \in \{0,1,\dots,7\}$.

EXERCISE 6.41. Compute $\mathrm{Hom}(\mathbb{Z}/n,G)$ for any group G.

EXERCISE 6.42. Let A, B and C be groups. If $f \in \mathrm{Hom}(A,B)$ and $g \in \mathrm{Hom}(B,C)$, then $g \circ f \in \mathrm{Hom}(A,C)$.

EXERCISE 6.43. Prove that $\mathbb{Z}/2\times\mathbb{Z}/2$ and $\mathbb{Z}/4$ are the only groups of order four (up to isomorphism). In particular, groups of order four are abelian.

The following example is harder than Exercise 6.43.

EXAMPLE 6.44. If G is a group of order six, then either $G\simeq\mathbb{S}_3$ or G is cyclic of order six. Since $|G|$ is even, there exists an element of G that has order two (see Exercise 3.5). If every element of $G\setminus\{1\}$ has order two, then $xy=yx$ for all $x,y\in G$. Hence

$$\langle x,y\rangle=\{1,x,y,xy\}\leq G,$$

a contradiction to Lagrange's theorem. Thus there exist $x\in G$ of order two and $y\in G\setminus\{1\}$ of order >2. By Lagrange's theorem, $|y|\in\{3,6\}$, as the order of y divides $|G|$. If $|y|=6$, then $G\simeq\mathbb{Z}/6$. It follows that there exists $z\in G$ of order three. Thus

$$\langle x,z\rangle=\{1,x,z,z^2,xz,xz^2\}=G.$$

Now we have the group $\langle x,z\rangle$. To "recognize" this group, we need to understand the product zx. We know that $zx\in\{xz,xz^2\}$. If $xz=zx$, then $|xz|=6$ (because $(xz)^k\neq 1$ for all $k\in\{1,\dots,5\}$ and $(xz)^6=1$). Thus $G=\langle xz\rangle\simeq\mathbb{Z}/6$. If, otherwise, $zx=xz^2$, then

$$G=\langle x,z:x^2=z^3=1,\,xzx^{-1}=z^2\rangle\simeq\mathbb{D}_3.$$

How many (isomorphism classes of) groups are there? We are now ready to collect our results and give a classification of isomorphism classes of groups of order ≤ 7; see Table 1. For the classification of groups of order eight, we need more tools.

TABLE 1. Groups of order ≤ 7 (up to isomorphism).

Order	Number	Group(s)
1	1	$\{1\}$
2	1	$\mathbb{Z}/2$
3	1	$\mathbb{Z}/3$
4	2	$\mathbb{Z}/4$
		$\mathbb{Z}/2\times\mathbb{Z}/2$
5	1	$\mathbb{Z}/5$
6	2	$\mathbb{Z}/6$
		$\mathbb{S}_3$
7	1	$\mathbb{Z}/7$

EXERCISE 6.45. Prove that the groups of order nine are $\mathbb{Z}/9$ and $\mathbb{Z}/3\times\mathbb{Z}/3$ (up to isomorphism). In particular, groups of order nine are abelian.

Lecture 7. 28/03/2024

§ 7.1. Isomorphism theorems. The following theorem is fundamental. For example, it allows us to recognize quotient groups.

THEOREM 7.1 (First isomorphism theorem). *If $f\colon G\to H$ is group homomorphism, then $G/\ker f\simeq f(G)$.*

PROOF. Let $K=\ker f$ and $\varphi\colon G/K\to f(G)$, $xK\mapsto f(x)$. We need to show that φ is well-defined. This means that we need to show that if $xK=yK$, then $f(x)=f(y)$. If $xK=yK$, then, since $y^{-1}x\in K$,
$$f(y)^{-1}f(x)=f(y^{-1}x)\in f(K)=\{1\}.$$
Thus $f(x)=f(y)$.

We now show that φ is a group homomorphism:
$$\varphi(xKyK)=\varphi(xyK)=f(xy)=f(x)f(y)=\varphi(xK)\varphi(yK).$$
To compute $\ker\varphi$ we proceed as follows:
$$\pi(x)=xK\in\ker\varphi\iff\varphi(xK)=1\iff f(x)=1\iff x\in K.$$
Therefore $\ker\varphi$ is trivial and φ is injective. Since $\varphi\colon G/K\to f(G)$ is surjective, we conclude that $G/K\simeq f(G)$. □

If G is a group, then $G/\{1\}\simeq G$ and $G/G\simeq\{1\}$.

EXAMPLE 7.2. Since $f\colon\mathbb{Z}\to\mathbb{Z}/n$, $x\mapsto x \bmod n$, is a group homomorphism with $\ker f=n\mathbb{Z}$, it follows that $\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/n$.

EXAMPLE 7.3. Let G be an infinite cyclic group, say $G=\langle g\rangle$. The map $f\colon\mathbb{Z}\to G$, $k\mapsto g^k$, is a group isomorphism. Thus $G\simeq\mathbb{Z}$ by the first isomorphism theorem. In particular, $G=\langle g^k\rangle$ if and only if $k\in\{-1,1\}$.

EXAMPLE 7.4. We claim that $\mathbb{Z}/n\mathbb{Z}\simeq G_n$. Let
$$f\colon\mathbb{Z}\to G_n,\quad f(k)=\exp(2i\pi k/n).$$
Then f is a surjective group homomorphism and $\ker f=n\mathbb{Z}$. By the first isomorphism theorem, the claim follows.

EXAMPLE 7.5. Note that $2\mathbb{Z}\simeq3\mathbb{Z}$, as both groups are infinite (alternatively, one can also consider the map $2k\mapsto3k$). Moreover,
$$\mathbb{Z}/2\simeq\mathbb{Z}/2\mathbb{Z}\not\simeq\mathbb{Z}/3\mathbb{Z}\simeq\mathbb{Z}/3.$$

EXAMPLE 7.6. Since
$$f\colon\mathbb{C}^\times\to\mathbb{C}^\times,\quad f(z)=\frac{z}{|z|},$$
is a group homomorphism with $\ker f=\mathbb{R}_{>0}$ and $f(\mathbb{C}^\times)=S^1$, the first isomorphism theorem implies that $\mathbb{C}^\times/\mathbb{R}_{>0}\simeq S^1$.

EXAMPLE 7.7. If we apply the first isomorphism theorem to the map $f\colon S^1\to S^1$, $f(z)=z^2$, we obtain that $S^1/\{\pm1\}\simeq S^1$, as $\ker f=\{-1,1\}$ and $f(S^1)=S^1$.

EXAMPLE 7.8. Let $f\colon\mathbb{C}^\times\to\mathbb{C}^\times$, $f(z)=|z|$. Since $\ker f=S^1$ and $f(\mathbb{C}^\times)=\mathbb{R}_{>0}$, the first isomorphism theorem implies that $\mathbb{C}^\times/S^1\simeq\mathbb{R}_{>0}$.

Example 7.9. We claim that $(\mathbb{Z}\times\mathbb{Z})/\langle(1,3)\rangle \simeq \mathbb{Z}$. We consider the surjective group homomorphism $f\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, $f(x,y)=3x-y$. Since

$$\ker f = \{(x,3x) : x\in\mathbb{Z}\} = \langle(1,3)\rangle,$$

the first isomorphism theorem implies that $(\mathbb{Z}\times\mathbb{Z})/\langle(1,3)\rangle \simeq \mathbb{Z}$.

Exercise 7.10. Prove that $\mathbb{R}/\mathbb{Z}\simeq S^1$.

Exercise 7.11. Prove that $\mathbb{Q}/\mathbb{Z}\simeq \cup_{n\geq 1}G_n$.

Exercise 7.12. Prove that $(\mathbb{Z}\times\mathbb{Z})/\langle(6,3)\rangle \simeq \mathbb{Z}\times(\mathbb{Z}/3)$.

Let us see another application that shows that the first isomorphism theorem is quite familiar.

Example 7.13. Let V be a vector space and W be a subspace of V. In particular, V is an abelian group and W is a normal subgroup of V. The abelian group V/W is then a vector space with

$$\lambda(v+W) = (\lambda v)+W, \quad \lambda\in\mathbb{R}, v\in V,$$

and the canonical homomorphism $\pi\colon V\to V/W$ is also a linear map. As an exercise, the reader needs to show that $\dim(V/W) = \dim V - \dim W$ if $\dim V<\infty$.

If $f\colon V\to U$ is a linear map, then $V/\ker f\simeq f(V)$ as abelian groups (by the first isomorphism theorem). The map realizing this isomorphism is moreover linear, so $V/\ker f\simeq f(V)$ as vector spaces. In particular, if $\dim V<\infty$, then

$$\dim V - \dim\ker f = \dim f(V).$$

Exercise 7.14. Let $f\colon G\to H$ be a group homomorphism and K a normal subgroup of G such that $K\subseteq \ker f$. Prove that there exists a unique group homomorphism $\varphi\colon G/K\to H$ such that the diagram

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

commutes. The commutativity of the diagram means that $\varphi\circ\pi = f$, where $\pi\colon G\to G/K$ is the canonical group homomorphism. Moreover, $\ker\varphi = \pi(\ker f)$ and $\varphi(G/K) = f(G)$. In particular, φ is injective if and only if $\ker f = K$ and φ is surjective if and only if f is surjective.

We now discuss the second isomorphism theorem. As a rule to remember what the theorem is about, one has the following diagram:

$$\begin{tikzcd}[column sep=small] & NT \arrow[dl, dash] \arrow[dr, dash] & \\ N \arrow[dr, dash] & & T \arrow[dl, dash] \\ & N\cap T & \end{tikzcd}$$

Exercise 7.15 (Second isomorphism theorem). If N is a normal subgroup of G and T is a subgroup of G, then $N\cap T$ is normal in T and

$$T/N\cap T \simeq NT/N.$$

Exercise 7.16. Let N be a normal subgroup of G and $\pi\colon G\to G/N$ the canonical homomorphism. Prove that if L is a subgroup of G, then $\pi^{-1}(\pi(L)) = NL$.

The following example uses additive groups.

Example 7.17. Let $G=\mathbb{Z}/24$, $H=\langle 4\rangle$ and $N=\langle 6\rangle$. Since G is abelian, H and K are normal in G. Then $H+N=\langle 2\rangle$ and $H\cap N=\{0,12\}$. Let us compute the left cosets of N in $H+N$:

$$0+N=\{0,6,12,18\},\quad 2+N=\{2,8,14,20\},\quad 4+N=\{4,10,16,22\}.$$

The left cosets of $H\cap N$ in H are

$$0+(H\cap N)=\{0,12\},\quad 4+(H\cap N)=\{4,16\},\quad 8+(H\cap N)=\{8,20\}.$$

By the second isomorphism theorem, $(H+N)/N\simeq H/H\cap N$. The isomorphism is given by $f\colon H/(H\cap N)\to(H+N)/N$, $h+(H\cap N)\mapsto h+N$. In our particular case,

$$\begin{aligned} f(0+(H\cap N)) &= 0+N,\\ f(4+(H\cap N)) &= 4+N,\\ f(8+(H\cap N)) &= 8+N=2+N. \end{aligned}$$

Let us discuss some applications.

Example 7.18. Let $a,b\in\mathbb{Z}\setminus\{0\}$. Then $a\mathbb{Z}+b\mathbb{Z}=\gcd(a,b)\mathbb{Z}$ and $a\mathbb{Z}\cap b\mathbb{Z}=\operatorname{lcm}(a,b)\mathbb{Z}$. By the second isomorphism theorem,

$$\frac{\gcd(a,b)\mathbb{Z}}{b\mathbb{Z}}=\frac{a\mathbb{Z}+b\mathbb{Z}}{b\mathbb{Z}}\simeq\frac{a\mathbb{Z}}{a\mathbb{Z}\cap b\mathbb{Z}}=\frac{a\mathbb{Z}}{\operatorname{lcm}(a,b)\mathbb{Z}}.$$

Since the formula involves finite groups, computing orders yields

$$ab=\gcd(a,b)\operatorname{lcm}(a,b).$$

A group G is said to be **meta-abelian** if it contains an abelian normal subgroup N and G/N is abelian. Abelian groups are meta-abelian. However, the group $\mathbb{S}_3$ is meta-abelian and not abelian. The following exercise present another application of the second isomorphism theorem.

EXERCISE 7.19. Prove that if G is a mete-abelian group and H is a subgroup of G, then H is meta-abelian.

There is a third isomorphism theorem.

EXERCISE 7.20 (Third isomorphism theorem). Let S and T be normal subgroups of G such that $S \subseteq T$. Prove that S is normal in T, T/S is normal in G/S and

$$\frac{G/S}{T/S} \simeq G/T,$$

where $T/S = \{tS : t \in T\}$.

The following example helps to visualize the third isomorphism theorem.

EXAMPLE 7.21. If m divides n, then $n\mathbb{Z} \leq m\mathbb{Z} \leq \mathbb{Z}$. Thus

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/m\mathbb{Z}.$$

The following theorem is known as the *correspondence theorem*. It is powerful and essential. It helps to have in mind the following diagram:

$$\begin{tikzcd}[column sep=small]
 & & G \arrow[dl, dash] \arrow[dr, dash] & \\
 & L \arrow[dl, dash] \arrow[dr, dash] & & f(G) \arrow[dl, dash] \\
N \arrow[dr, dash] & & Y \arrow[dl, dash] & \\
 & \{1\} & &
\end{tikzcd}$$

THEOREM 7.22 (Correspondence theorem). *Let $f\colon G \to H$ be a group homomorphism and $K = \ker f$. There exists a bijective correspondence*

$$\mathscr{A} = \{L : K \leq L \leq G\} \underset{\tau}{\overset{\sigma}{\rightleftarrows}} \{Y : Y \leq f(G)\} = \mathscr{B}$$

The correspondence is given by $\sigma(L) = f(L)$ and $\tau(Y) = f^{-1}(Y)$. Moreover, the following statements hold:

1) *$L_1 \leq L_2$ if and only if $\sigma(L_1) \leq \sigma(L_2)$.*
2) *$L \trianglelefteq G$ if and only if $\sigma(L) \trianglelefteq f(G)$.*

PROOF. Note that σ and τ are well-defined, as $f(L) \leq f(G)$ and $K \leq f^{-1}(Y) \leq G$.

Let us prove that $\tau \circ \sigma = \mathrm{id}_{\mathscr{A}}$. We need to show that $\tau(\sigma(L)) = L$ for all $L \in \mathscr{A}$. If $x \in f^{-1}(f(L))$, then $f(x) \in f(L)$. Thus $f(x) = f(l)$ for some $l \in L$. Hence $xl^{-1} \in K$ and therefore $x \in Kl \subseteq L$, as $K \subseteq L$. Conversely, if $l \in L$, then $f(l) \in f(L)$. Thus $l \in f^{-1}(f(L))$.

We now prove that $\sigma \circ \tau = \mathrm{id}_{\mathscr{B}}$. If $Y \in \mathscr{B}$, then $\sigma(\tau(Y)) = Y$. If $y \in Y \subseteq f(G)$, then $y = f(x)$ for some $x \in G$, that is $x \in f^{-1}(y)$. This implies that $y = f(x) \in f(f^{-1}(Y))$. Conversely, if $y \in f(f^{-1}(Y))$, then $y = f(x)$ for some $x \in f^{-1}(Y)$. This implies that $y = f(x) \in Y$.

It is an exercise to show that $X \leq Y$ if and only if $f(X) \leq f(Y)$.

We now show that $L \trianglelefteq G$ if and only if $f(L) \trianglelefteq f(G)$. If $L \trianglelefteq G$ and $x \in G$, then $xLx^{-1} = L$. This implies that $f(L) = f(xLx^{-1}) = f(x)f(L)f(x)^{-1}$, that is to say that $f(L)$ is normal in $f(G)$. Conversely, if $f(L) \trianglelefteq f(G)$ and $x \in G$, then

$$f(xLx^{-1}) = f(x)f(L)f(x)^{-1} = f(L).$$

This implies that $xLx^{-1} \subseteq LK \subseteq L$. Thus $xLx^{-1} \subseteq L$, which means that L is normal in G. $\square$

Proposition 7.23. *If $f\colon G \to f(G)$ is a surjective group homomorphism and $H \leq G$ is such that $K = \ker f \subseteq H$, then $(G : H) = (f(G) : f(H))$.*

Proof. Let $H \leq G$ be such that $\ker f \subseteq H$ and

$$\alpha\colon G/H \to f(G)/f(H), \quad \alpha(gH) = f(g)f(H).$$

It is an exercise to show that α is well-defined. We need to show that α is bijective, as then

$$(G : H) = |G/H| = |f(G)/f(H)| = (f(G) : f(H)).$$

First, we show that α is surjective. If $yf(H) \in f(G)/f(H)$, then $y = f(g)$ for some $g \in G$ (because f is surjective).Thus

$$yf(H) = f(g)f(H) = f(gH) = \alpha(gH).$$

We now show that α is injective. If $\alpha(gH) = \alpha(g_1H)$, then,

$$f(g)^{-1}f(g_1) = f(h) \in f(H)$$

for some $h \in H$, that is $f(g_1) = f(g)f(h) = f(gh)$ for some $h \in H$. This implies that $g_1 = ghk$ for some $k \in \ker f \subset eqH$ and hence $g_1 = gh_1$ for some $h_1 \in H$, that is $g_1H = gH$. $\square$

In the case of the canonical homomorphism $\pi\colon G \to G/N$, the previous result reads as follows. If N is a normal subgroup of G, then $K \mapsto K/N$ is a bijection between the set of (normal) subgroups of G containing N and the set of (normal) subgroups ofG/N. If H is a subgroup of G, then

$$\pi(H) = HN/N.$$

Example 7.24. Let us show that every subgroup of

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

is normal Q_8. Let $N = \{-1, 1\}$. Then N is normal in Q_8, as $N \subseteq Z(Q_8)$). Since $|Q_8/N| = 4$, Q_8/N is an abelian group.

We claim that N is included in every non-trivial subgroup of Q_8. If K is a non-trivial subgroup of Q_8, then $-1 \in K$ (because, for example, if $-i \in K$, then $-1 = (-i)^2 \in K$). Then every subgroup of Q_8 corresponds to a subgroup of Q_8/N. Since Q_8/N is abelian, every subgroup of Q_8/N is normal. Thus if $S \leq Q_8$, then $\pi(S)$ is normal in Q_8/N. Since $N \subseteq S$, it follows that $S = \pi^{-1}(\pi(S))$. Hence S is normal in Q_8.

Example 7.25. Let $f\colon \mathbb{Z}/12 \to \mathbb{Z}/6$ be the group homomorphism given by $1 \mapsto 1$. Then $K = \ker f = \{0, 6\}$. The subgroups of $\mathbb{Z}/12$ containing K are

$$\langle 1\rangle = \{0, 1, \dots, 11\}, \quad \langle 2\rangle = \{0, 2, 4, 6, 8, 10\}, \quad \langle 3\rangle = \{0, 3, 6, 9\}, \quad \langle 6\rangle = \{0, 6\}.$$

These subgroups correspond via f to the subgroups

$$\langle 1\rangle = \{0, 1, \dots, 5\}, \quad \langle 2\rangle = \{0, 2, 4\}, \quad \langle 3\rangle = \{0, 3\}, \quad \{0\}$$

of $\mathbb{Z}/6$, respectively. For example,

$$\begin{tikzcd}
 & & \mathbb{Z}/12 \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle 2\rangle \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Z}/6 \arrow[dl, dash] \\
\{0,6\} \arrow[dr, dash] & & \langle 2\rangle \arrow[dl, dash] & \\
 & \{0\} & &
\end{tikzcd}$$

The correspondence theorem helps to transport properties from the image of a group homomorphism to the domain. Let us discuss a concrete example.

Example 7.26. Let G be a finite group and N be a normal subgroup of G such that $N \simeq \mathbb{Z}/5$ and $G/N \simeq \mathbb{S}_4$. The following statements hold:

1) $|G| = 120$
2) G contains a normal subgroup of order 20.
3) G contains three subgroups of order 15, none of them normal in G.

To prove the first claim we note that Lagrange's theorem implies that

$$24 = |G/N| = \frac{|G|}{|N|} = |G|/5.$$

We prove the second claim. Let K be the subgroup of G/N isomorphic to the Klein group. Then K is normal in G/N and $|K| = 4$. Since $(G/N : K) = 6$, the subgroup K of G/N corresponds to a normal subgroup H of G such that $(G : H) = 6$. Using Lagrange's theorem and the correspondence theorem, $|H| = 20$, as

$$6 = (G/N : K) = (G : H) = \frac{|G|}{|H|}.$$

For the third claim, note that $G/N \simeq \mathbb{S}_4$ has four subgroups of order 3 (these are the subgroups generated by a 3-cycle), none normal in G/N. By the correspondence theorem, these subgroups correspond with four non-normal subgroups of G, all of order 15.

If G is a group, $\mathbb{S}_G = \{f : G \to G : f \text{ bijective}\}$.

Theorem 7.27 (Cayley). *Every group G is isomorphic to a subgroup of $\mathbb{S}_G$.*

Proof. Let $f : G \to \mathbb{S}_G$, $g \mapsto L_g$, where $L_g : G \to G$, $L_g(x) = gx$. Then f is a group homomorphism, as

$$L_{gh}(x) = (gh)x = g(hx) = L_g(hx) = L_gL_h(x)$$

for all $g,h,x \in G$. Moreover, f is injective (if $f(g) = f(h)$, then $L_g = L_h$, and this implies that $gx = L_g(x) = L_h(x) = hx$ for all $x \in G$, which ultimately implies $g = h$). It follows that $G \simeq f(G)$, which is a subgroup of $\mathbb{S}_G$. $\square$

Every finite group is isomorphic to a subgroup of some $\mathbb{S}_n$. In particular, using permutation matrices, we see that every finite group isomorphic to a subgroup of $\mathbf{GL}_n(\mathbb{Z})$ for some n. Those groups are known as **linear groups**.

Proposition 7.28. *Every finite simple group G is contained in some $\mathbb{A}_n$.*

Proof. If $|G| = 2$, the result is trivial, as $G \simeq \langle (12)(34) \rangle \subseteq \mathbb{A}_2$. Assume that $|G| > 2$. Let $f\colon G \to \mathbb{S}_n$ by the injective group homomorphism given by Cayley's theorem. If $H = f(G)$, then $G \simeq H$ by the first isomorphism theorem. We claim that $H \subseteq \mathbb{A}_n$. If H is not a subgroup of $\mathbb{A}_n$, there exists $h \in H$ such that $h \notin \mathbb{A}_n$. Write $h = f(g)$ for some $g \in G$. Since $h \notin \mathbb{A}_n$, $\operatorname{sign}(f(g)) = \operatorname{sign}(h) = -1$, that is $g \notin \ker(\operatorname{sign} \circ f)$. Let $K = \ker(\operatorname{sign} \circ f)$. Then $K = \{1\}$, as G is simple. Moreover, $\operatorname{sign} \circ f$ is a bijective map, as $\operatorname{sign}(f(1)) = 1$ and $\operatorname{sign}(f(g)) = -1$. Therefore $G \simeq G/K \simeq \mathbb{Z}/2$, by the first isomorphism theorem. In particular, $|G| = 2$, a contradiction. Thus $H \subseteq \mathbb{A}_n$. □

Let us briefly discuss another application of Cayley's theorem. We use the theorem to show that in a group, no product needs parenthesis By Cayley's theorem, a group G is (isomorphic to) a subgroup of $\mathbb{S}_G$. The composition of maps is an associative operation. Moreover, no composition of finitely many maps needs parenthesis. Thus

$$(f_1 \circ \cdots \circ f_n)(g) = f_1(f_2(\cdots f_n(g)) \cdots).$$

Lecture 8. 18/05/2024

§ 8.1. Semi-direct products. We first start with an exercise of **direct products**. Let G be a group and H and K be normal subgroups with trivial intersection, that is $H\cap K=\{1\}$. Then $hk=kh$ for all $h\in H$ and $k\in K$. In fact,

$$[h,k]=hkh^{-1}k^{-1}\in H\cap K=\{1\},$$

since $hkh^{-1}\in K$ because K is normal in G and $kh^{-1}k^{-1}\in H$ because H is normal in G.

Exercise 8.1. Let G be a group and H and K be normal subgroups of G. If $G=HK$ and $H\cap K=\{1\}$, then $G\simeq H\times K$.

Exercise 8.2. Let A be a normal subgroup of H, and B be a normal subgroup of K. Prove that $A\times B$ is a normal subgroup of $H\times K$ and

$$\frac{H\times K}{A\times B}\simeq (H/A)\times(K/B).$$

We say that a group G admits an exact factorization through the subgroups H and K if $G=HK$ and $H\cap K=\{1\}$. By Exercise 8.1, if G admits an exact factorization through two normal subgroups, then it is isomorphic to the direct product of these subgroups.

Exercise 8.3. Let G be a group that admits an exact factorization through the subgroups H and K. Prove that every $g\in G$ can be written uniquely as $g=hk$ for some $h\in H$ and $k\in K$.

Example 8.4. Let $G=\mathbb{S}_3$, $H=\langle(123)\rangle\trianglelefteq G$ and $K=\langle(12)\rangle$. Since K is not normal in G, we cannot apply Exercise 8.1. We do have $G=HK$ and $H\cap K=\{\mathrm{id}\}$, but $H\times K\simeq\mathbb{Z}/3\times\mathbb{Z}/2\not\simeq\mathbb{S}_3$, as $\mathbb{Z}/3\times\mathbb{Z}/2$ is abelian and $\mathbb{S}_3$ is not.

In the next example, we present a group of **affine transformations**.

Example 8.5. Let

$$G=\{f\colon\mathbb{R}\to\mathbb{R}, f(x)=ax+b \text{ for some } a,b\in\mathbb{R} \text{ with } a\neq 0\}.$$

Then G is a group with the usual composition of functions. The identity map is an element of G. If $f\in G$, say $f(x)=ax+b$, then the inverse is an element of G, as $f^{-1}(x)=(1/a)x-b/a$. Finally, compositions of functions of G are elements of G: if $f(x)=ax+b$ and $g(x)=cx+d$, then

$$f(g(x))=f(cx+d)=a(xc+d)+b=(ac)x+(ad+b).$$

Note that $K=\{f\in G: f(x)=x+b \text{ for some } b\in\mathbb{R}\}$ is a normal subgroup of G isomorphic to the additive group $\mathbb{R}$. In fact, let $f(x)=x+b$ be an element of K and $g(x)=cx+d$ be an element of G. Then $gfg^{-1}\in K$, as

$$\begin{aligned}(gfg^{-1})(x)&=g(f((1/c)x-d/c))\\&=g((1/c)x-d/c+b)\\&=c((1/c)x-d/c+b)+d\\&=x+(bc).\end{aligned}$$

Finally, $Q=\{f\in G: f(x)=ax \text{ for some } a\neq 0\}$ is a subgroup of G isomorphic to the multiplicative group $\mathbb{R}^\times$. Then $G=KQ$ and $K\cap Q=\{\mathrm{id}\}$.

Definition 8.6. Let G be a group, K a normal subgroup of G, and Q a subgroup of G. We say that Q **complements** K in G if $K \cap Q = \{1\}$ and $G = KQ$.

Example 8.7. Let $G = \mathbb{S}_3$ and $K = \langle(123)\rangle \trianglelefteq G$. The subgroups $\langle(12)\rangle$, $\langle(13)\rangle$ and $\langle(23)\rangle$ complement K in G.

The previous example shows that complements are not unique. However, complements are unique under isomorphism, as

$$G/K = KQ/K \simeq Q/K \cap Q = Q/\{1\} \simeq Q.$$

We now present a generalization of the (internal) direct product of Exercise 8.1.

Definition 8.8. We say that a group G is a **semi-direct product** of Q and K if K is normal in G and K admits a complement in G isomorphic to Q. Notation: $G = K \rtimes Q$.

The symbol $\rtimes$ is not symmetric, but points to remind us which subgroup is normal.

Let $G = K \rtimes Q$. Then $G = KQ$ with K normal in G. Let $g = ax$ and $g_1 = a_1x_1$ with $a, a_1 \in K$ and $x, x_1 \in Q$. Then

$$gg_1 = (ax)(a_1x_1) = (axa_1x^{-1})(xx_1) \in KQ,$$

because K is normal in G.

Theorem 8.9. *Let K be a normal subgroup of G. The following statements are equivalent:*

1) *K admits a complement in G.*
2) *There exists a subgroup Q of G such that each $g \in G$ can be written uniquely as $g = xy$ for some $x \in K$ and $y \in Q$.*
3) *There is a group homomorphism $s\colon G/K \to G$ such that $\pi \circ s = \mathrm{id}_{G/K}$, where $\pi\colon G \to G/K$, $g \mapsto Kg$, is the canonical homomorphism.*
4) *There exists a group homomorphism $\rho\colon G \to G$ such that $\ker \rho = K$ and the restriction $\rho|_{\rho(G)}$ equals the identity.*

Proof. We first prove that $(1) \implies (2)$. If Q complements K, then $G = KQ$ and $K \cap Q = \{1\}$. In particular, if $g \in G$, then $g = xy$ para $x \in K$ e $y \in Q$. To show that the decomposition is unique, suppose that $g = x_1y_1$ with $x_1 \in K$ and $y_1 \in Q$. Then $x_1^{-1}x = yy_1^{-1} \in K \cap Q = \{1\}$ and hence $x = x_1$ and $y = y_1$.

We now prove that $(2) \implies (3)$. Let $s\colon G/K \to G$, $s(Kg) = y$ if $g = xy$ with $x \in K$ and $y \in Q$. (Note that here we use right cosets, as it is more convenient.) Let us check that s is well-defined. For that purpose, we must show that $Kg = Kg_1$ implies $s(Kg) = s(Kg_1)$. Let $g = xy$ and $g_1 = x_1y_1$ with $x, x_1 \in K$ and $y, y_1 \in Q$, then, since $Kg = Kg_1$, $xyy_1^{-1}x_1^{-1} = gg_1^{-1} \in K$, that is $yy_1^{-1} \in x^{-1}Kx_1 = K$ because $x, x_1 \in K$. Hence $yy_1^{-1} \in K \cap Q = \{1\}$ and thus $y = y_1$.

We now show that $\pi \circ s = \mathrm{id}_{G/K}$:

$$(\pi \circ s)(Kg) = \pi(y) = Ky = Kxy = Kg.$$

Finally, the map s is a group homomorphism, as

$$s((Kg)(Kg_1)) = s(Kgg_1) = s(Kx(yx_1y^{-1})yy_1) = yy_1 = s(Kg)s(Kg_1),$$

since $yx_1y^{-1} \in K$.

We now prove that $(3) \implies (4)$. Let $\rho = s \circ \pi$. Then ρ is a group homomorphism (because it is the composition of homomorphisms). To prove that $\rho|_{\rho(G)} = \mathrm{id}$, we need to show that $\rho(\rho(g)) = \rho(g)$ for all $g \in G$. We compute:

$$\rho(\rho(g)) = (s \circ (\pi \circ s) \circ \pi)(g) = (s \circ \pi)(g) = \rho(g).$$

We now compute $\ker\rho$. If $g\in\ker\rho$, then $s(\pi(g))=\rho(g)=1$. Thus

$$\pi(g)=\pi(s(\pi(g)))=\pi(1)=1_{G/K},$$

that is $g\in\ker\pi=K$. Conversely, if $x\in K$, then

$$\rho(x)=\rho(s(Kx))=\rho(s(K))=\rho(1)=1$$

and hence $x\in\ker\rho$.

Finally, we prove that (4) $\implies$ (1). We claim that $Q=\rho(G)$ complements K in G. We first show that $K\cap Q=\{1\}$: if $x\in K\cap Q$, then $x=\rho(g)$ for some $g\in G$. Moreover,

$$1=\rho(x)=\rho(\rho(g))=\rho(g).$$

Hence $g\in\ker\rho=K$ and $x=1$. We now prove that $G=KQ$. For the inclusion $G\subseteq KQ$,

$$g=(g\rho(g^{-1}))\rho(g)$$

and $g\rho(g^{-1})\in K=\ker\rho$, as $\rho(g\rho(g^{-1}))=\rho(g)\rho(g^{-1})=1$. □

Example 8.10. $\mathbb{S}_n=\mathbb{A}_n\rtimes\langle(12)\rangle$, as $Q=\langle(12)\rangle\simeq\mathbb{Z}/2$ complements $\mathbb{A}_n$ in $\mathbb{S}_n$.

For a group G, the set

$$\mathrm{Aut}(G)=\{f\colon G\to G : f\text{ bijective group homomorphism}\}$$

is a group with the composition of maps. It is called the **automorphism group** of G. Examples of automorphism groups are the identity map and conjugations homomorphisms.

Example 8.11. $\mathrm{Aut}(\mathbb{Z})\simeq\mathbb{Z}/2$, as $\mathrm{Aut}(\mathbb{Z})=\{\mathrm{id},-\mathrm{id}\}$.

Example 8.12. Let G be a group and $g\in G$. The conjugation map $\gamma_g\colon G\to G$, $x\mapsto gxg^{-1}$, is an automorphism of G, as

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

Moreover, $\gamma\colon G\to\mathrm{Aut}(G)$, $g\mapsto\gamma_g$, is a group homomorphism:

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

The group of **inner automorphisms** of G is the group $\mathrm{Inn}(G)=\gamma(G)$. Note that $\ker\gamma=Z(G)$, as if $g\in G$ is such that $\gamma_g=\mathrm{id}$, then

$$\gamma_g(x)=gxg^{-1}=x$$

for all $x\in G$. By the first isomorphism theorem,

$$G/Z(G)\simeq\gamma(G)=\mathrm{Inn}(G).$$

Exercise 8.13. Prove that $\mathrm{Aut}(\mathbb{S}_3)\simeq\mathbb{S}_3$.

Exercise 8.14. Let G be a group. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

For a group G, the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of **outer automorphisms** of G. Note that

$$\mathrm{Inn}(G)\text{ is cyclic}\iff|\mathrm{Inn}(G)|=1\iff G\text{ is abelian}.$$

Exercise 8.15. Let G be a group. Prove that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

EXERCISE 8.16. Prove that if G is finite, then $\mathrm{Aut}(G)$ is finite.

Let us discuss how groups acts on groups. An action of a group on a group is a group homomorphism $\theta\colon Q \to \mathrm{Aut}(K)$, $x \mapsto \theta_x$. This is nothing but a way in which Q permutes the elements of K in a way that is compatible with both group structures. Typically, in this setting, one says that Q acts on K by automorphisms.

What does it mean that θ is a group homomorphism? For $x \in Q$, write $\theta_x\colon K \to K$, $a \mapsto x \cdot a$. Then θ is a well-defined group homomorphism if and only if the following properties hold:

1) $1 \cdot a = a$ for all $a \in K$.
2) $x \cdot (y \cdot a) = (xy) \cdot a$ for all $x, y \in Q$ and $a \in K$.
3) $x \cdot 1 = 1$ for all $x \in Q$.
4) $x \cdot (ab) = (x \cdot a)(x \cdot b)$ for all $x \in Q$ and $a, b \in K$.

EXAMPLE 8.17. The group $\mathbf{GL}_2(\mathbb{R})$ acts on the additive group $\mathbb{R}^{2\times 1}$ by automorphisms via the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}. \tag{8.1}$$

Before doing calculations, note that this formula is nothing but the usual left multiplication of matrices by vectors! In fact $\alpha \in \mathbf{GL}_2(\mathbb{R})$ and $v \in \mathbb{R}^{2\times 1}$, the action of (8.1) is just

$$\alpha \cdot v = \alpha v.$$

To show that we have an action by automorphisms, there are four properties to verify. First, it is trivial to check the first property, as

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

For the second property, a direct calculation shows that

$$\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$$

for all $\alpha, \beta \in \mathbf{GL}_2(\mathbb{R})$ and $v \in \mathbb{R}^{2\times 1}$. The third property is trivial:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Finally, the fourth property is just the left distributivity:

$$\alpha \cdot (v+w) = x(v+w) = \alpha v + \alpha w = \alpha \cdot v + \alpha \cdot w$$

for all $\alpha \in \mathbf{GL}_2(\mathbb{R})$ and $v, w \in \mathbb{R}^{2\times 1}$.

EXERCISE 8.18. Let K and Q be groups and $\theta\colon Q \to \mathrm{Aut}(K)$, $x \mapsto \theta_x$, a group homomorphism. Prove that $K \times Q$ with

$$(a,x)(b,y) = (a\theta_x(b), xy)$$

is a group. This group will be written as $K \rtimes_\theta Q$.

The group of Exercise 8.18 is the semi-direct product of the subgroups

$$K \times \{1\} = \{(a,1) : a \in K\} \simeq K, \qquad \{1\} \times Q = \{(1,x) : x \in Q\} \simeq Q$$

of $K \rtimes_\theta Q$. Note that $K \times \{1\}$ is normal in $K \rtimes_\theta Q$. We can identity $K \rtimes \{1\}$ with K and $\{1\} \rtimes Q$ with Q. This means that for $a \in K$ and $x \in Q$, instead of writing $(a,1)$ one simply writes a and $(1,x)$ is replaced by x. Moreover,

$$ax = (a,1)(1,x) = (a,x)$$

and

$$xa = (1,x)(a,1) = (\theta_x(a),x) = (\theta_x(a),1)(1,x) = \theta_x(a)x.$$

Thus we can write

$$\theta_x(a) = xax^{-1}$$

for all $x \in Q$ and $a \in K$, that is

$$\theta_x(a) = (\theta_x(a),1) = (1,x)(a,1)(1,x)^{-1} = xax^{-1}.$$

EXERCISE 8.19. Prove that if G is a semi-direct product of the normal subgroup K with the subgroup Q, there exists a group homomorphism $\theta\colon Q \to \mathrm{Aut}(K)$ such that $G \simeq K \rtimes_\theta Q$.

Let us discuss some examples.

EXAMPLE 8.20. The multiplicative group $Q = \mathbb{R}^\times$ acts on the additive group $K = \mathbb{R}$ by multiplication: If $x \in Q$ and $a \in K$, then $x \cdot a = xa$. This is an action by automorphisms, as

$$1 \cdot a = a, \quad x \cdot (y \cdot a) = x(ya) = (xy)a = (xy) \cdot a, \quad x \cdot 0 = 0, \quad x \cdot (a+b) = xa + xb$$

for all $a,b \in \mathbb{R}$ and $x,y \in \mathbb{R}^\times$.

Hence one can construct the semi-direct product $K \rtimes Q$. The operation of this group is

$$(d,c)(b,a) = (cb+d, ca).$$

This group is isomorphic to the group of affine transformations of Example 8.5. In fact, one can easily show that

$$K \rtimes Q \to \{f\colon \mathbb{R} \to \mathbb{R} : f(x) = ax+b \text{ for some } a \in \mathbb{R}^\times \text{ and } b \in \mathbb{R}\}, \quad (b,a) \mapsto f(x) = ax+b,$$

is a bijective group homomorphism.

EXAMPLE 8.21. Let $N \simeq \mathbb{Z}/n$ and $H \simeq \mathbb{Z}/2 = \{0,1\}$. The map $\theta\colon H \to \mathrm{Aut}(N)$, $1 \mapsto (x \mapsto x^{-1})$, is a group homomorphism. Let $G = N \rtimes_\theta H$. Then $G \simeq \mathbb{D}_n$, the dihedral group of order $2n$.

Recall that

$$\mathbb{D}_n = \langle r,s : r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Assume that $N = \langle x \rangle$ and $H = \langle y \rangle$. Then $|(x,1)| = n$ and $|(1,y)| = 2$. Moreover,

$$\begin{aligned}(1,y)(x,1)(1,y)^{-1} &= (\theta_y(x),y)(1,y)\\ &= (\theta_y(x),y^2)\\ &= (\theta_y(x),1)\\ &= (x^{-1},1)\\ &= (x,1)^{-1}.\end{aligned}$$

If $u = (x,1)$ and $v = (1,y)$, then $u^n = v^2 = (1,1)$ and $vuv^{-1} = u^{-1}$. Thus there exists a surjective group homomorphism $\mathbb{D}_n \to G$ (because G is generated by u and v). Moreover, $|G| = |N||H| = 2n$. Hence G has order $2n$ and therefore $G \simeq \mathbb{D}_n$.

EXAMPLE 8.22. Let $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Then K is normal in $\mathbb{A}_4$. Let $H = \langle (123) \rangle \simeq \mathbb{Z}/3$. Since $K \cap H$ is a subgroup of H and K and, moreover, K and H have coprime orders, $H \cap K = \{\mathrm{id}\}$. Hence $\mathbb{A}_4 = K \rtimes H$.

EXAMPLE 8.23. Let

$$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}, \quad H = \{\sigma \in \mathbb{S}_4 : \sigma(4) = 4\}.$$

Note that H is a subgroup of $\mathbb{S}_4$ isomorphic to $\mathbb{S}_3$. Then $H \cap K = \{\mathrm{id}\}$ and hence $\mathbb{S}_4 = K \rtimes H$.

Let $n \geq 5$. Using the fact that $\mathbb{A}_n$ is a simple group, one proves that $\mathbb{A}_n$ cannot be written as a semi-direct product of proper subgroups.

EXAMPLE 8.24. Let $K = \mathbb{Z}/3$ and $Q = \mathbb{Z}/4$. Since $\mathrm{Hom}(Q, \mathrm{Aut}(K)) = \{1, \tau\}$, where

$$\tau \colon \mathbb{Z}/4 \to \mathrm{Aut}(\mathbb{Z}/3) = \{\mathrm{id}, \rho\} \simeq \mathbb{Z}/2, \quad 1 \mapsto \rho,$$

the semi-direct product $T = K \rtimes_\tau Q$ is a non-abelian group of order 12. Moreover, $T \not\simeq \mathbb{A}_4$ as $|(2,2)| = 6$ and $\mathbb{A}_4$ has no elements of order six.

EXERCISE 8.25. Prove that the group of Exercise 6.20 is a semi-direct product.

Lecture 9. 25/04/2024

§ 9.1. Actions of groups on sets.

DEFINITION 9.1. Let G be a group and X a set. A (left) **action** of G on X is a map $G \times X \to X$, $(g,x) \mapsto g \cdot x$, such that

1) $1 \cdot x = x$ for all $x \in X$, and
2) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g,h \in G$ and $x \in X$.

If a group G acts on a set X, we also say that X is a G-set.

EXAMPLE 9.2. Recall the action of Example 8.17. The group $\mathbf{GL}_2(\mathbb{R})$ acts on $\mathbb{R}^{2\times 1}$ by left multiplication: if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ and $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^{2\times 1}$, then

$$A \cdot v = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

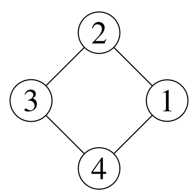
EXAMPLE 9.3. The group

$$G = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$$

acts on the plane $\mathbb{R}^{2\times 1}$ by left multiplication. For example, with $\theta = \pi/2$,

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}.$$

EXAMPLE 9.4. The dihedral group $\mathbb{D}_8 = \langle r,s : r^4 = s^2, srs = r^{-1} \rangle$ of eight elements acts on the vertices of the square:



The element r is a rotation by 90° counterclockwise and s is a reflection across the line joining vertices 1 and 3. Thus r can be identified with the permutation (1234) and s with (24). The rest of the elements of $\mathbb{D}_8$ as permutations on the vertices appear in the following table:

1	r	r^2	r^3	s	rs	r^2s	r^3s
id	(1234)	$(13)(24)$	(1423)	(24)	$(12)(34)$	(13)	$(14)(23)$

In the previous example, a relabelling of the vertices will turn $\mathbb{D}_8$ into a different subgroup of $\mathbb{S}_4$. Do you remember what conjugate subgroups are?

EXAMPLE 9.5. The multiplicative group $\mathbb{R}^\times$ acts on the plane $\mathbb{R}^2$ by multiplication:

$$\lambda \cdot (x,y) = (\lambda x, \lambda y), \quad \lambda \in \mathbb{R}^\times, (x,y) \in \mathbb{R}^2.$$

EXAMPLE 9.6. Every group G acts on G trivially: $g \cdot h = h$ for all $g,h \in G$.

EXAMPLE 9.7. Every group G acts on G by left multiplication, that is $g \cdot h = gh$ for all $g,h \in G$.

EXAMPLE 9.8. Every group G acts on G by conjugation, that is $g \cdot h = ghg^{-1}$ for all $g, h \in G$. More generally, if N is a normal subgroup of G, then G acts on N by conjugation: $g \cdot x = gxg^{-1}$ for all $g \in G$ and $x \in N$.

EXAMPLE 9.9. Let G be a group H be a subgroup of G. Then G acts on the set of left cosets G/H by left multiplication, that is $g \cdot (xH) = (gx)H$ for all $g, x \in G$.

For sets X and Y, let $\mathrm{Fun}(X,Y)$ be the set of maps $X \to Y$.

EXERCISE 9.10. Let G be a group and X and Y be sets. Assume that G acts on X. Prove that G acts on $\mathrm{Fun}(X,Y)$ by

$$(g \cdot f)(x) = f(g^{-1} \cdot x), \quad g \in G,\ f \in \mathrm{Fun}(X,Y),\ x \in X.$$

There is a bijective correspondence between left actions of a group G on a set X and group homomorphisms $\rho \colon G \to \mathbb{S}_X$. The correspondence is given by the formula

$$\rho(g)(x) = g \cdot x, \quad g \in G, x \in X.$$

We will write $\rho_g = \rho(g)$.

As an example, if $G \times X \to X$, $(g,x) \mapsto x$, is an action of G on X, then each $\rho_g \colon X \to X$ is a bijective map with inverse $(\rho_g)^{-1} = \rho_{g^{-1}}$. Moreover, ρ is a group homomorphism, as

$$\rho(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \rho_g(h \cdot x) = \rho_g(\rho_h(x))$$

for all $g, h \in G$ and $x \in X$.

EXAMPLE 9.11. Let $G = \mathbb{S}_3$ and

$$H = \langle (123) \rangle = \{\mathrm{id}, (123), (132)\}.$$

Let G act on the set $X = G/H = \{H, (12)H\}$ of left cosets of H by left multiplication. Write $x_1 = H$ and $x_2 = (12)H$. Then

$$(12) \cdot x_1 = x_2, \qquad (12) \cdot x_2 = x_1, \qquad (123) \cdot x_1 = x_1, \qquad (123) \cdot x_2 = x_2.$$

Since $G = \langle (12), (123) \rangle$, one has the group homomorphism $\rho \colon G \to \mathbb{S}_X$ given by $(12) \mapsto (x_1 x_2)$, $(123) \mapsto \mathrm{id}$.

EXAMPLE 9.12. As before, let $G = \mathbb{S}_3$ and $H = \langle (12) \rangle = \{\mathrm{id}, (12)\}$. Let G act on the set $X = G/H = \{H, (123)H, (132)H\}$ of left cosets of H by left multiplication. Write $x_1 = H$, $x_2 = (123)H$ and $x_3 = (132)H$. Then

$$\begin{aligned} &(12) \cdot x_1 = x_1, && (12) \cdot x_2 = x_3, && (12) \cdot x_3 = x_2, \\ &(123) \cdot x_1 = x_2, && (123) \cdot x_2 = x_3, && (123) \cdot x_3 = x_1. \end{aligned}$$

Since $G = \langle (12), (123) \rangle$, one has the group homomorphism $\rho \colon G \to \mathbb{S}_X$ given by $(12) \mapsto (x_2 x_3)$, $(123) \mapsto (x_1 x_2 x_3)$.

EXAMPLE 9.13. Let $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and $N = \{1, -1, i, -i\}$. Since N is normal in G, G acts by conjugation on $X = N$. If $x_1 = 1$, $x_2 = -1$, $x_3 = i$ and $x_4 = -i$, then $i \cdot x = x$ for all $x \in N$. Moreover,

$$j \cdot x_1 = x_1, \qquad j \cdot x_2 = x_2, \qquad j \cdot x_3 = x_4, \qquad j \cdot x_4 = x_3.$$

Since $G = \langle i, j \rangle$, a group homomorphism $\rho \colon G \to \mathbb{S}_X \simeq \mathbb{S}_4$ is determined by $\rho_i = \mathrm{id}$ and $\rho_j = (34)$.

The following example is important.

EXAMPLE 9.14. The group $\mathbb{S}_n$ acts on $\mathbb{R}^n$ by

$$\sigma\cdot(x_1,\dots,x_n)=(x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(n)}).$$

It is very important to use σ^{-1} and not σ, as we need to permute the elements of the standard basis of $\mathbb{R}^3$.

As a concrete example, let us see that the operation

$$\sigma\cdot(x_1,x_2,x_3)=(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)})$$

is not an action of $\mathbb{S}_3$ on $\mathbb{R}^3$. If $\sigma=(12)$ and $\tau=(23)$, then $\sigma\tau=(123)$. Since

$$\begin{aligned}&(123)\cdot(5,6,7)=(6,7,5),\\&(12)\cdot((23)\cdot(5,6,7))=(1,2)\cdot(5,7,6)=(7,5,6),\end{aligned}$$

this does not define an action. If we compute

$$\sigma\cdot(\tau\cdot(x_1,\dots,x_n))=\sigma\cdot(x_{\tau(1)},\dots,x_{\tau(n)})$$

and for each $i\in\{1,\dots,n\}$ we set $y_i=x_{\tau(i)}$, then

$$\sigma\cdot(\tau\cdot(x_1,\dots,x_n))=\sigma\cdot(y_1,\dots,y_n)=(y_{\sigma(1)},\dots,y_{\sigma(n)})=(x_{\tau\sigma(1)},\dots,x_{\tau\sigma(n)}),$$

even if σ and τ do not commute.

Now we show that by using inverses, we do have an action. For $j\in\{1,\dots,n\}$, let $y_j=x_{\tau(j)}$, that is

$$(y_1,y_2,\dots,y_n)=\tau\cdot(x_1,x_2,\cdots,x_n)=(x_{\tau^{-1}(1)},x_{\tau^{-1}(2)},\dots,x_{\tau^{-1}(n)}).$$

Then

$$\begin{aligned}\sigma\cdot(\tau\cdot(x_1,x_2,\dots,x_n))&=\sigma\cdot(y_1,y_2,\dots,y_n)\\&=\left(y_{\sigma^{-1}(1)},y_{\sigma^{-1}(2)},\dots,y_{\sigma^{-1}(n)}\right)\\&=\left(x_{\tau^{-1}(\sigma^{-1}(1))},x_{\tau^{-1}(\sigma^{-1}(2))},\dots,x_{\tau^{-1}(\sigma^{-1}(n))}\right)\\&=\left(x_{(\sigma\tau)^{-1}(1))},x_{(\sigma\tau)^{-1}(2))},\dots,x_{(\sigma\tau)^{-1}(n))}\right).\end{aligned}$$

The following example is also important:

EXAMPLE 9.15. The group $\mathbb{S}_n$ acts on the set of polynomials on n variables $X_1,\dots,X_n$ by permitting the variables. For example, for three variables, if $\sigma=(123)$ and

$$f=X_2X_3-X_1+5X_2X_3^2X_1,$$

then

$$\sigma\cdot f=X_2^2X_3-X_1+5X_2X_3^2X_1.$$

Restricting the action, we see that $\mathbb{S}_n$ acts on the set

$$\{\lambda_1X_1+\cdots\lambda_nX_n:\lambda_1,\dots,\lambda_n\in\mathbb{R}\}.$$

Then

$$\sigma\cdot(\lambda_1X_1+\cdots+\lambda_nX_n)=(\lambda_1X_{\sigma(1)}+\cdots+\lambda_nX_{\sigma(n)})=(\lambda_{\sigma(1)}X_1+\cdots+\lambda_{\sigma(n)}X_n).$$

It is relevant to compute the kernel of the action homomorphism.

EXAMPLE 9.16. Let G be a group and H be a subgroup of G. Then G acts on G/H by left multiplication, that is $g \cdot (xH) = (gx)H$ for all $g, x \in G$. Let $\rho \colon G \to \mathbb{S}_{G/H}$ be the group homomorphism induced by the action.

We claim that $\ker \rho = \cap_{x \in G} xHx^{-1}$. We first prove $\supseteq$. If $g \in xHx^{-1}$ for all $x \in G$, then, for a fixed $x \in G$,

$$\rho(g)(xH) = g \cdot (xH) = (gx)H = (xhx^{-1})xH = (xh)H = xH$$

because $g = xhx^{-1}$ for some $h \in H$. Thus $\rho(g) = \mathrm{id}$ and hence $g \in \ker \rho$. We now prove $\subseteq$. If $g \in \ker \rho$, then $\rho(g) = \mathrm{id}$. So for all $x \in G$,

$$\rho(g)(xH) = xH \iff (gx)H = xH \iff x^{-1}gx \in H \iff g \in xHx^{-1}.$$

The subgroup $\ker \rho$ is called the **core** of H in G.

EXERCISE 9.17. Let G be a group and H be a subgroup of G. Prove that the core of H in G is the largest normal subgroup of G contained in H.

With these results, we can provide a third solution to Exercise 5.24 of page 26. We let G act on G/H by left multiplication. The induced group homomorphism $\rho \colon G \to \mathbb{S}_p$ has kernel

$$K = \ker \rho = \bigcap_{x \in G} xHx^{-1} \subseteq H.$$

By the first isomorphism theorem, $G/K \simeq \rho(G) \lesssim \mathbb{S}_p$ (this means that $\rho(G)$ is isomorphic to a subgroup of $\mathbb{S}_p$). Thus $|G/K|$ divides $p!$. Let $m = (H:K)$. By Lagrange's theorem,

$$(G:K) = (G:H)(H:K) = pm$$

and hence pm divides $p!$. This implies that m divides $(p-1)!$. If q a prime number dividing m, then $q \geq p$, by the minimality of p. Moreover, every prime factor of $(p-1)!$ is $< p$. Hence $m = 1$ and therefore $H = K$.

EXERCISE 9.18. Let a group G act on a set X. On X, we define the following relation: $x \sim y$ if and only if there exists $g \in G$ such that $g \cdot x = y$. Prove that this is an equivalence relation on X.

DEFINITION 9.19. Let G be a group acting on a set X. If $x \in X$, the orbit of x is the set

$$G \cdot x = \{g \cdot x : g \in G\}.$$

The orbits of the action of G on X are the equivalence classes of the equivalence relation induced by the action.

EXERCISE 9.20. Let a group G acts on a set X. Prove that every two orbits will be either disjoint or equal. Moreover, X decomposes as a disjoint union of orbits.

DEFINITION 9.21. Let G be a group that acts on X. If $x \in X$, the **stabilizer** of x in G is the set

$$G_x = \{g \in G : g \cdot x = x\}.$$

The reader must prove that the stabilizer is a subgroup.

DEFINITION 9.22. We say that an action of a group G on a set X is **transitive** if for any $x, y \in X$ there exists $g \in G$ such that $g \cdot x = y$.

EXAMPLE 9.23. Let G be a group and H a subgroup of G. Let G act on G/H by left multiplication. The action is transitive: if $xH, yH \in G/H$, there exists $g \in G$ such that $(gx)H = yH$ (take for example $g = yx^{-1}$).

EXAMPLE 9.24. The symmetric group $\mathbb{S}_n$ acts (by evaluation) transitively on $\{1, \dots, n\}$.

In the definition of a transitive action, there is no assumption on the number of elements g such that $g \cdot x = y$.

DEFINITION 9.25. We say that an action of a group G on a set X is **faithful** if

$$\{g \in G : g \cdot x = x \text{ for all } x \in X\} = \{1\}.$$

The definition is equivalent to the injectivity of the group homomorphism induced by the action.

THEOREM 9.26 (Fundamental counting principle). *Let G be a finite group acting on a finite set X. If $x \in X$, then $|G \cdot x| = (G : G_x)$.*

PROOF. Let $\varphi \colon G/G_x \to G \cdot x$, $gG_x \mapsto g \cdot x$. Then φ is well-defined, as

$$gG_x = hG_x \implies h^{-1}g \in G_x \implies h^{-1}g \cdot x = x \implies g \cdot x = h \cdot x.$$

Moreover, φ is injective:

$$\varphi(gG_x) = \varphi(hG_x) \implies g \cdot x = h \cdot x \implies h^{-1}g \in G_x \implies gG_x = hG_x.$$

Finally, φ is surjective. Hence $|G/G_x| = |G \cdot x|$. $\square$

Theorem 9.26 is also known as the orbit–stabilizer theorem.

If G is a group and X and Y are G-sets, we say that a map $\varphi \colon X \to Y$ is a **homomorphism** of G-sets if $\varphi(g \cdot x) = g \cdot \varphi(x)$ for all $g \in G$ and $x \in X$. The bijection φ constructed in the proof of Theorem 9.26 is a homomorphism of G-sets, where G acts on G/G_x by left multiplication:

$$\varphi(g \cdot hG_x) = \varphi((gh)G_x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot \varphi(hG_x).$$

Thus $G \cdot x \simeq G/G_x$ as G-sets.

EXAMPLE 9.27. If G acts on G by conjugation, that is $g \cdot x = gxg^{-1}$, the orbits of this action are called the **conjugacy classes** of G. They are sets of the form

$$G \cdot x = \{gxg^{-1} : g \in G\}.$$

In particular, G decomposes as a disjoint union of conjugacy classes. Moreover, the stabilizers are the centralizers:

$$G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = C_G(x).$$

In particular, $|G \cdot x| = (G : C_G(x))$.

EXAMPLE 9.28. Let H be a subgroup of G and X the set of subsets of G. Let G act on X by conjugation, that is $S \in X$. Then $g \cdot S = gSg^{-1}$. The orbit of H is

$$G \cdot H = \{g \cdot H : g \in G\} = \{gHg^{-1} : g \in G\},$$

the set of conjugates of H. The stabilizer of H in G is

$$G_H = \{g \in G : g \cdot H = H\} = \{g \in G : gHg^{-1} = H\} = N_G(H),$$

the normalizer of H in G. It follows that H has exactly $(G : N_G(H))$ conjugates in G. In particular, if G is finite, the number of conjugates of H divides $|G|$.

As an application, we provide an alternative proof of Theorem 6.5.

EXAMPLE 9.29. Let G be a group and H and K be subgroups of G. The group $L = H \times K$ acts on $X = HK$ by

$$(h,k)\cdot x = hxk^{-1}, \quad x \in X, h \in H, k \in K.$$

Note that $1 \in HK$ and the action of L on X is transitive, as $(h,k^{-1})\cdot 1 = hk$. Since

$$L_1 = \{(h,k) \in H \times K : (h,k)\cdot 1 = 1\} = \{(h,k) \in H \times K : h = k\},$$

it follows that $|L_1| = |H \cap K|$ because there exists a bijection between L_1 and $H \cap K$. By the fundamental counting principle,

$$|HK| = (L : L_1) = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}.$$

Lecture 10. 02/05/2024

The idea used in Example 9.29 can be generalized.

EXAMPLE 10.1. Let G be a group and H and K be subgroups of G. Let the group $L = H \times K$ act on G by

$$(h,k)\cdot g = hgk^{-1}.$$

The orbtis are sets of the form

$$HgK = \{hgk : h \in H, k \in K\}.$$

These sets are called **double** (H,K)**-coset**. In particular, two double cosets are either disjoint or equal. Moreover, G admits a decomposition as a disjoint union of double cosets, that is

$$G = \bigcup_{i\in I} Hg_iK,$$

for some set I. Now we compute

$$L_g = \{(h,k) \in H \times K : hgk^{-1} = g\} = \{(h, g^{-1}hg) \in H \times K\}.$$

Then $|L_g| = |H \cap gKg^{-1}|$, because there is a bijection between L_g and $H \cap gKg^{-1}$. By the fundamental counting principle (Theorem 9.26),

$$|HgK| = (L : L_g) = \frac{|H \times K|}{|H \cap gKg^{-1}|} = \frac{|H||K|}{|H \cap gKg^{-1}|}.$$

As another application, we compute the order of the group $\mathbf{GL}_n(p)$ para $n \geq 1$ and a prime number p. The argument also works for the group $\mathbf{GL}_n(q)$ in the case where q is a power of the prime number p.

EXAMPLE 10.2. Let p be a prime number and $K = \mathbb{Z}/p$. We claim that

$$|\mathbf{GL}_n(p)| = (p^n - 1)p^{n-1}|\mathbf{GL}_{n-1}(p)|,$$

and hence

$$|\mathbf{GL}_n(p)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

The formula is valid if $n \in \{1,2\}$. Assume that it holds for $n-1 \geq 1$. The group $G = \mathbf{GL}_n(p)$ acts on $K^{n\times 1}$ by left multiplication. How are the orbits? Since for every non-zero $v, w \in K^{n\times 1}$, then there exists $g \in G$ such that $gv = w$. Thus there are only two orbits. One orbit is the one-element orbit of the zero column vector of $K^{n\times 1}$, and the other orbit is the set $\mathscr{O}$ of non-zero vectors of $K^{n\times 1}$. By the fundamental counting principle,

$$p^{n+1} - 1 = |\mathscr{O}| = (G : G_v),$$

for every $v \in \mathscr{O}$, that is every $v \in K^{n\times 1}$.

To compute the stabilizer G_v easily, take

$$v = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathscr{O}.$$

If $g=(g_{ij})\in G$ is such that $gv=v$, then

$$g=\begin{pmatrix}1 & g_{12} & \cdots & g_{1n}\\ 0 & g_{22} & \cdots & g_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & g_{n1} & \cdots & g_{nn}\end{pmatrix}.$$

Therefore $|G_v|=p^{n-1}|\mathbf{GL}_{n-1}(p)|$, as the submatrix $(g_{ij})_{2\leq i,j\leq n}$ is invertible and the g_{1j}'s can be chosen arbitrarily for all $j\in\{2,\dots,n\}$. Hence

$$p^n-1=\frac{|G|}{|G_v|}=\frac{|\mathbf{GL}_n(p)|}{p^{n-1}|\mathbf{GL}_{n-1}(p)|},$$

which implies the formula we wanted to prove.

§ 10.1. ***p*-groups.** Let G be a finite group acting on a finite set X. Let

$$\mathrm{Fix}(X)=\{x\in X:g\cdot x=x\text{ for all }g\in G\}$$

be the set of **fixed points** of X, that is the set of one-elements orbits. We know that X decomposes as a disjoint union of orbits. In particular,

$$X=\mathrm{Fix}(X)\cup\mathscr{O}_1\cup\cdots\mathscr{O}_k,$$

where $\mathscr{O}_1,\dots,\mathscr{O}_k$ are orbits such that $|\mathscr{O}_j|\geq 2$ for all $j\in\{1,\dots,k\}$. If we apply cardinality and use the fundamental counting principle,

$$|X|=|\mathrm{Fix}(X)|+\sum_{i=1}^{k}|\mathscr{O}_i|=|\mathrm{Fix}(X)|+\sum_{i=1}^{k}(G:G_{x_i}), \tag{10.1}$$

where $x_j\in\mathscr{O}_j$ and $(G:G_{x_i})\geq 2$ for all $j\in\{1,\dots,k\}$. Equality (10.1) is extremely useful and is called the **class equation**.

Example 10.3. Let a finite group G act on G by conjugation. Then $\mathrm{Fix}(G)=Z(G)$ and

$$|G|=|Z(G)|+\sum_{i=1}^{k}(G:C_G(x_i)),$$

for some $x_1,\dots,x_k\in G$ such that $(G:C_G(x_i))\geq 2$ for all $i\in\{1,\dots,k\}$.

Definition 10.4. Let p be a prime number. We say that G is a p**-group** if $|G|=p^m$ for some $m\geq 0$.

Theorem 10.5. *Let p be a prime number and G be a p-group. If N is a non-trivial normal subgroup of G, then $N\cap Z(G)\neq\{1\}$.*

Proof. Since N is normal in G, G acts on N by conjugation. By the fundamental counting principle, each orbit has prime-power size. Write

$$N=\underbrace{\mathscr{O}_1\cup\cdots\cup\mathscr{O}_k}_{\text{one-element orbits}}\cup\underbrace{\mathscr{O}_{k+1}\cup\cdots\cup\mathscr{O}_m}_{\text{orbits of size }>1},$$

Since $N\cap Z(G)=\mathscr{O}_1\cup\cdots\cup\mathscr{O}_k$, the integers $k=|N\cap Z(G)|$ and $|N\setminus(N\cap Z(G))|$ are divisible by p. Thus

$$|N|\equiv|N\cap Z(G)|\bmod p.$$

Since $1\in N\cap Z(G)$, then $|N\cap Z(G)|>1$. In particular, $N\cap Z(G)\neq\{1\}$. $\square$

The following corollary follows immediately:

COROLLARY 10.6. *Let p be a prime number and G a p-group. Then $Z(G) \neq \{1\}$.*

In Exercises 6.43 and 6.45 we proved that groups of order four and nine are always abelian.

COROLLARY 10.7. *Let p be a prime number. If G is a group of order p^2, then G is abelian.*

PROOF. By Lagrange's theorem, $|Z(G)| \in \{1, p, p^2\}$. Since G is a p-group, $Z(G) \neq \{1\}$. If $|Z(G)| = p$, then $G/Z(G)$ is cyclic. By Exercise 5.20, G is abelian, a contradiction. Thus $|Z(G)| = p^2$ and hence $G = Z(G)$. □

§ 10.2. Cauchy's theorem.

THEOREM 10.8 (Cauchy). *Let G be a finite group, and p be a prime number that divides $|G|$. Then there exists $g \in G$ of order p.*

PROOF. Let $C = \mathbb{Z}/p$ and

$$X = \{(x_1, \dots, x_p) \in G \times \cdots \times G : x_1 \cdots x_p = 1\}.$$

Then C acts on X by $k \cdot (x_1, \dots, x_p) = (x_{k+1}, \dots, x_{k+p})$, where the indices are taken modulo p. To see that this is an action, note that

$$x_{i_1} \cdots x_{i_p} = 1 \implies (x_{i_1}^{-1} x_{i_1}) x_{i_2} \cdots x_{i_p} = x_{i_1}^{-1} \implies x_{i_2} \cdots x_{i_p} x_{i_1} = 1.$$

If $x_1, \dots, x_{p-1}$ are fixed, then $x_p = x_{p-1}^{-1} \cdots x_1^{-1}$. Thus $|X| = |G|^{p-1}$. Each C-orbit has either one or p elements, as $|C| = p$. Write

$$X = \underbrace{\mathscr{O}_1 \cup \cdots \cup \mathscr{O}_k}_{\text{one-element orbits}} \cup \underbrace{\mathscr{O}_{k+1} \cup \cdots \cup \mathscr{O}_m}_{\text{orbits of size } p}.$$

Hence $0 \equiv |G|^{p-1} = |X| \equiv k \bmod p$, that is p divides k. Since $(1, 1, \dots, 1) \in X$, $k \geq 1$. Therefore $p \leq k$. In particular, there exists $x \in G \setminus \{1\}$ such that $(x, x, \dots, x) \in X$. Hence $|x| = p$. □

EXERCISE 10.9. Let p be a prime number and G be a finite group. Then G is a p-group if and only if every element of G has order a power of p.

COROLLARY 10.10. *Let $p > 2$ be a prime number and G be a group of order $2p$. Then either $G \simeq \mathbb{Z}/2p$ or $G \simeq \mathbb{D}_p$.*

PROOF. By Cauchy's theorem, there exist $r, s \in G$ such that $|r| = p$ and $|s| = 2$. Let $H = \langle r \rangle$. Then $(G : H) = 2$ and $H \trianglelefteq G$. We can decompose G as $G = H \cup Hs$ (disjoint union), as $s \notin H$. In particular,

$$G = \{1, r, \dots, r^{p-1}, s, rs, \dots, r^{p-1}s\}.$$

Since $srs^{-1} \in H$, it follows that $srs^{-1} = r^k$ for some $k \in \{0, 1, \dots, p-1\}$. Since $s^2 = 1$,

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = sr^k s^{-1} = r^{k^2}.$$

Thus $k^2 \equiv 1 \bmod p$ and either $k \equiv 1 \bmod p$ or $k \equiv -1 \bmod p$. If $k \equiv -1 \bmod p$, then $srs^{-1} = r^{-1}$ and hence $G \simeq \mathbb{D}_p$. If $k \equiv 1 \bmod p$, then $rs = sr$ and hence, since G is abelian, $G \simeq \mathbb{Z}/2p$. □

THEOREM 10.11. *Let p be a prime number. A group of order p^m has a normal subgroup of order p^n for every $n \leq m$.*

PROOF. We proceed by induction on m. The case where $m = 1$ is trivial. So let $m \geq 1$ and assume the result holds for groups of order p^m. Let G be a group of order p^{m+1}. We claim that if $n \leq m$, G contains a normal subgroup of order p^n. Since $Z(G) \neq \{1\}$, there exists $g \in Z(G) \setminus \{1\}$ of order p. Let $N = \langle g \rangle \trianglelefteq G$. The quotient group G/N has order p^m. By the inductive hypothesis, there exists a normal subgroup Y of G/N of order p^n. Let $\pi\colon G \to G/N$ be the canonical map. By the correspondence theorem, G contains a normal subgroup K of G that contains N, that is $N \leq K \leq G$. In fact, $Y = \pi(K)$ and $(G : K) = (\pi(G) : \pi(K)) = p^{m-n}$. Hence $|K| = p^{n+1}$. $\square$

Lecture 11. 16/05/2024

§ 11.1. Sylow's theorems.

Definition 11.1. Let G be a group of $p^\alpha m$, where p is a prime number coprime with m. A subgroup S of G is said to be a **Sylow p-subgroup** of G if $|S| = p^\alpha$.

A subgroup S of G is a Sylow p-subgroup of G if and only if S is a p-group and the prime p does not divide $(G:S)$.

Example 11.2.

1) If p does not divide $|G|$, then $\{1\}$ is a Sylow p-subgroup of G.
2) If G is a p-group, then G is a Sylow p-subgroup of G.

Example 11.3. Let $G = \mathbb{S}_3$. Then $\langle (12) \rangle$, $\langle (13) \rangle$ and $\langle (23) \rangle$ are the Sylow 2-subgroups of G. Moreover, $\langle (123) \rangle$ is the only Sylow 3-subgroup of G.

Example 11.4. Let $G = \mathbb{S}_4$. The subgroup $\langle (1234), (13) \rangle$ is a Sylow 2-subgroup of G and $\langle (123) \rangle$ is a Sylow 3-subgroup of G.

Example 11.5. Let $G = \mathbb{Z}/18$. The subgroup $\langle 2 \rangle = \{0,2,4,6,8,10,12,14,16\}$ is the only Sylow 3-subgroup of G and $\langle 9 \rangle = \{0,9\}$ is the only Sylow 2-subgroup of G.

Example 11.6. Let p be a prime number and $G = \mathbf{GL}_n(p)$. Since

$$\begin{aligned} |\mathbf{GL}_n(p)| &= (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) \\ &= p^{1+2+\cdots+n}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1), \end{aligned}$$

we can write $|\mathbf{GL}_n(p)| = p^\alpha m$, where $\alpha = 1 + 2 + \cdots + n$ and m is an integer not divisible by p. The subgroup of matrices of the form

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

that is the set of matrices (g_{ij}) with

$$g_{ij} = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i > j, \end{cases}$$

has order p^α. Thus it is a Sylow p-subgroup of $\mathbf{GL}_n(p)$.

We will prove three crucial theorems that go back to Sylow. The first one guarantees the existence of Sylow subgroups. We shall need a lemma.

Lemma 11.7. *If p is a prime number, $\alpha \geq 0$ and $m \geq 1$, then*

$$\binom{p^\alpha m}{p^\alpha} \equiv m \bmod p.$$

Proof. By the binomial theorem,

$$(1+X)^p = \sum_{j=0}^{p} \binom{p}{j} X^{p-j} \equiv 1 + X^p \bmod p,$$

because $\binom{p}{j}$ is divisible by p for all $j \in \{1,\dots,p-1\}$. By using induction, one proves that

$$(1+X)^{p^j} \equiv 1+X^{p^j} \bmod p$$

holds for all j. Thus

$$(1+X)^{p^\alpha m} \equiv (1+X^{p^\alpha})^m \bmod p.$$

Comparing the coefficient of X^{p^α} in the previous formula, we get the result we wanted to prove. □

THEOREM 11.8 (Sylow's first theorem). *Let G be a finite group and p a prime number. Then there exists a Sylow p-subgroup of G.*

PROOF. Write $|G| = p^\alpha m$ with $\gcd(p,m) = 1$ and $\alpha \geq 1$. Let

$$X = \{S : S \subseteq G \text{ subsets of size } p^\alpha\}.$$

Let G act on X by left multiplication, as $|g\cdot S| = |gS| = |S|$ for all $g \in G$ and $S \in X$. Decompose X into G-orbits and note that the previous lemma implies that

$$|X| = \binom{p^\alpha m}{p^\alpha} \equiv m \not\equiv 0 \bmod p.$$

Thus there exists an orbit $\mathscr{O}$ of size not divisible by p. If $S \in \mathscr{O}$, let G_S be the stabilizer of S in G. Since $|\mathscr{O}| = (G : G_S)$ and $|\mathscr{O}|$ is not divisible by p, we obtain that p^α divide a $|G_S|$. In particular, $p^\alpha \leq |G_S|$. If $g \in G_S$, then $gS = S$. If $x \in S$, then $G_S x \subseteq S$. Thus

$$|G_S| = |G_S x| \leq |S| = p^\alpha$$

as $S \in X$. Therefore G_S is a Sylow p-subgroup of G. □

If G is a finite group and p is a prime divisor of $|G|$, let

$$\mathrm{Syl}_p(G) = \{\text{Sylow } p\text{-subgroups of } G\}.$$

The first Sylow's theorem states that $\mathrm{Syl}_p(G)$ is non-empty.

Before proving Sylow's second theorem, we state and prove a slightly more technical result.

THEOREM 11.9. *Let G be a finite group. If P is a p-subgroup of G and $S \in \mathrm{Syl}_p(G)$, then $P \subseteq gSg^{-1}$ for some $g \in G$.*

PROOF. Let $X = \{xS : x \in G\}$ be the set of left cosets of S in G. Then $|X| = (G : S)$ is not divisible by p. Let G act on X by left multiplication. In particular, P also acts on X by left multiplication. Decompose X into P-orbits. There exists a P-orbit $\mathscr{O}$ of size not divisible by p, as $|X|$ is not divisible by p. Since $|\mathscr{O}|$ divides $|P|$ and p does not divide $|\mathscr{O}|$, it follows that $|\mathscr{O}| = 1$, that is $\mathscr{O} = \{gS\}$ for some $g \in G$. Since $P(gS) = gS$, in particular, $xg \in gS$ for all $x \in P$. This means that if $x \in P$, then $x \in gSg^{-1}$. Hence $P \subseteq gSg^{-1}$. □

An application:

COROLLARY 11.10. *Let p be a prime number. If G is a finite group and P is a p-subgroup of G, then P is contained in some Sylow p-subgroup of G.*

PROOF. If $S \in \mathrm{Syl}_p(G)$, then $gSg^{-1} \in \mathrm{Syl}_p(G)$, as $|gSg^{-1}| = |S|$. By the previous theorem, $P \subseteq gSg^{-1}$ for some $g \in G$. Thus the claim follows. □

Theorem 11.11 states that any two Sylow p-subgroups are conjugate, that is, G acts transitively by conjugation on $\mathrm{Syl}_p(G)$.

THEOREM 11.11 (Sylow's second theorem). *Let G be a finite group and p a prime number. If $S,T \in \mathrm{Syl}_p(G)$, then there exists $g \in G$ such that $gSg^{-1} = T$.*

PROOF. Use the previous theorem with $P = T$. Then $T \subseteq gSg^{-1}$ for some $g \in G$. Since $|S| = |T|$ and $|T| \leq |gSg^{-1}| = |S|$, we conclude that $T = gSg^{-1}$. □

COROLLARY 11.12. *Let G be a finite group, p a prime number and $S \in \mathrm{Syl}_p(G)$. If S is normal in G, then $\mathrm{Syl}_p(G) = \{S\}$.*

PROOF. If $T \in \mathrm{Syl}_p(G)$, then $T = gSg^{-1} = S$ for some $g \in G$. □

For the next theorem, we need some notation. If p is a prime number and G is a finite group of order $p^\alpha m$ with $\gcd(p,m) = 1$, then $n_p(G) = |\mathrm{Syl}_p(G)|$. Note that

$$n_p(G) = (G : N_G(P))$$

for all $P \in \mathrm{Syl}_p(G)$. We will prove that $n_p(G)$ divides m.

THEOREM 11.13 (Sylow's third theorem). *Let G be a finite group and p a prime number. Then $n_p(G) \equiv 1 \bmod p$.*

PROOF. Assume that $|G| = p^\alpha m$ with m not divisible by p. By Sylow's first theorem, $\mathrm{Syl}_p(G)$ is non-empty. Let $P \in \mathrm{Syl}_p(G)$ and $n = n_p(G)$. We consider the set

$$X = \{gPg^{-1} : g \in G\} = \{P = P_1, P_2, \dots, P_n\}.$$

By Sylow's second theorem, $|X| = n$.

Let G act on X by conjugation. Then P also acts on X by conjugation. Each P-orbit has size a power of p.

We claim that $\{P\}$ is the only P-orbit of size one. Since $xPx^{-1} = P$ if $x \in P$, it follows that $\{P\}$ is a P-orbit. Let $\{P_i\}$ be a P-orbit of size one. Then $xP_ix^{-1} = P_i$ for all $x \in P$. Thus $P \subseteq N_G(P_i)$. The group $N_G(P_i)/P_i$ has order not divisible by p, as $P_i \in \mathrm{Syl}_p(G)$. If $xP_i \in N_G(P_i)/P_i$ con $x \in P$, then $xP_i = P_i$. That is $x \in P_i$, since

$$(xP_i)^{p^\alpha} = x^{p^\alpha} P_i = P_i$$

implies that the order of the element $xP_i \in N_G(P_i)/P_i$ divides p^α. Hence xP_i is an element of order one, as $N_G(P_i)/P_i$ has order coprime with p. Therefore $x \in P_i$. This implies that $P \subseteq P_i$. Hence $P = P_i$, as both sets have size p^α. Now

$$X = \{P\} \cup \underbrace{\mathscr{O}_1 \cup \mathscr{O}_2 \cup \dots \cup \mathscr{O}_k}_{\text{of size } > 1 \text{ divisible by } p}.$$

Thus $n_p(G) = |X| \equiv 1 \bmod p$. □

We now discuss some applications of Sylow's theorems.

EXAMPLE 11.14. If G is a group of order 15, then G is cyclic.

Let $n_3 = n_3(G)$ and $n_5 = n_5(G)$. Then $n_3 \equiv 1 \bmod 3$ and n_3 divides 5. Thus $n_3 = 1$ and hence there exists a unique $H \in \mathrm{Syl}_3(G)$. This group is then normal in G and isomorphic to $\mathbb{Z}/3$. Similarly, $n_5 = 1$ and there is a unique subgroup $K \in \mathrm{Syl}_5(G)$ such that $K \trianglelefteq G$ and $K \simeq \mathbb{Z}/5$. Since $H \cap K = \{1\}$ by Lagrange's theorem,

$$|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = 15 = |G|.$$

Hence $G = HK \simeq H \times K \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \simeq \mathbb{Z}/15$.

EXAMPLE 11.15. If G is a group of order 455, then G is cyclic.

For every prime p dividing $|G|$, let $n_p = n_p(G)$. Since n_5 divides 7×13 and $n_5 \equiv 1 \bmod 5$, then $n_5 \in \{1.91\}$. A direct calculation shows that $n_7 = n_{13} = 1$. Let $P \in \mathrm{Syl}_7(G)$ and $Q \in \mathrm{Syl}_{13}(G)$, both normal subgroups of G. Since P and Q have coprime orders, Lagrange's theorem implies that $P \cap Q = \{1\}$. We now apply Sylow's theorems to the quotients G/P and G/Q. Let $m_5 = n_5(G/P)$ and $m_{13} = n_{13}(G/P)$. Since m_5 divides 13 and $m_5 \equiv 1 \bmod 5$, it follows that $m_5 = 1$. Similarly, $m_{13} = 1$ and hence $G/P \simeq \mathbb{Z}/5 \times \mathbb{Z}/13$. The same argument shows that $G/Q \simeq \mathbb{Z}/5 \times \mathbb{Z}/7$. Thus both G/P and G/Q are abelian. This means that $[G,G] \subseteq P \cap Q = \{1\}$. Hence G is also abelian. In particular, $n_5 = 1$ and

$$G \simeq \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/13 \simeq \mathbb{Z}/455.$$

EXAMPLE 11.16. If G is a group of order 21, then either

$$G \simeq \mathbb{Z}/21 \quad \text{or} \quad G \simeq \langle x, y : x^7 = y^3 = 1, yx = x^2 y\rangle.$$

Let $n_3 = n_3(G)$ and $n_7 = n_7(G)$. Since $n_7 \equiv 1 \bmod 7$ and n_3 divides 3, it follows that $n_7 = 1$. There is a unique $H \in \mathrm{Syl}_7(G)$. This subgroup H is such that $H \trianglelefteq G$ and $H \simeq \mathbb{Z}/7$. Thus $H = \langle x \rangle$, where $x^7 = 1$. Let $K \in \mathrm{Syl}_3(G)$. Since n_3 divides 7 and $n_3 \equiv 1 \bmod 3$, it follows that $n_3 \in \{1,7\}$. Hence $K \simeq \mathbb{Z}/3$ and thus $K = \langle y \rangle$ where $y^3 = 1$. By Lagrange's theorem, $H \cap K = \{1\}$ and $G = HK$. In particular,

$$G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2\}.$$

Since H is normal in G, $yxy^{-1} \in H$. That is $yxy^{-1} = x^i$ for some $i \in \{1,\dots,6\}$. Therefore $x^7 = y^3 = 1$ and $yx = x^i y$ for some $i \in \{1,\dots,6\}$. What can we say about this i? We note that

$$x = y^3 x y^{-3} = y^2 (yxy^{-1}) y^{-2} = y^2 x^i y^{-2} = y(x^i)^2 y^{-1} = (x^i)^3.$$

Then $i^3 \equiv 1 \bmod 7$, that is $i \in \{1,2,4\}$. There are three cases:

(a) If $yxy^{-1} = x$, then $xy = yx$. Thus $K \trianglelefteq G$ and $G \simeq H \times K \simeq \mathbb{Z}/21$.

(b) If $yxy^{-1} = x^2$, then we can compute the table of G. In particular, G can be obtained as a certain subgroup of $\mathbf{GL}_2(\mathbb{Z}/7)$, that is

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad G \simeq \langle x, y \rangle \leq \mathbf{GL}_2(\mathbb{Z}/7).$$

(c) If $yxy^{-1} = x^4$, then $y^2 x y^{-2} = x^2$. Since $|y^2| = |y| = 3$, if $z = y^2$, then $H = \langle y \rangle = \langle z \rangle$. So we are in the previous case.

EXAMPLE 11.17. If G is a group of order $5 \cdot 7 \cdot 17$, then G is cyclic.

For $p \in \{5,7,17\}$, let $n_p = n_p(G)$. Since $n_5 \equiv 1 \bmod 5$ and n_5 divides $7 \cdot 17$, it follows that $n_5 = 1$. Let $H \in \mathrm{Syl}_5(G)$. This is the only Sylow 5-subgrop of G, so H is normal in G. Let $K \in \mathrm{Syl}_7(G)$ and $L \in \mathrm{Syl}_{17}(G)$. Since H is normal in G, HK is a subgroup of G. By Lagrange's theorem, $H \cap K = \{1\}$ because H and K have coprime orders. Thus $|HK| = 5 \cdot 7$. We now apply Sylow's theorems to the group HK. If $m_7 = n_7(HK)$, then $m_7 = 1$. In particular, $K \in \mathrm{Syl}_7(HK)$ and K is normal in HK. Thus $HK \subseteq N_G(K)$ and $|HK| \leq |N_G(K)|$. Since

$$n_7 = (G : N_G(K)) = \frac{|G|}{|N_G(K)|} \leq \frac{|G|}{|HK|} = \frac{5 \cdot 7 \cdot 17}{5 \cdot 7} = 17$$

and $n_7 \in \{1, 5 \cdot 17\}$, we conclude that $n_7 = 1$. The same argument shows that $n_{17} = 1$. Therefore both K and L are normal in G. By Lagrange's theorem,

$$L \cap H = H \cap K = L \cap K = \{1\}$$

It follows that

$$L \cap (HK) = H \cap (LK) = K \cap (LH) = \{1\}.$$

Hence $G = HKL \simeq \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/17 \simeq \mathbb{Z}/(5 \cdot 7 \cdot 17)$.

EXAMPLE 11.18. If G is a group of order 12 such that $n_3(G) \neq 1$, then $G \simeq \mathbb{A}_4$.

Let $P \in \mathrm{Syl}_3(G)$ and $n_3 = n_3(G) = 4$. Then P is not normal in G. Let G act on the set G/P by left multiplication. This induces a group homomorphism

$$\rho \colon G \to \mathbb{S}_{G/P} \simeq \mathbb{S}_4.$$

We claim that ρ is injective. Note that $\ker \rho \subseteq P$, as

$$x \in \ker \rho \implies \rho_x = \mathrm{id} \implies xP \subseteq P \implies x \in P.$$

Since P is not normal in G, $P \neq \ker \rho$. Thus $\ker \rho$ is a proper subgroup of P. Hence $\ker \rho = \{1\}$ since $|P| = 3$. Let $S, T \in \mathrm{Syl}_3(G)$. Since $S \simeq T \simeq \mathbb{Z}/3$, Lagrange's theorem implies that $S \cap T = \{1\}$. Thus G contains exactly eight elements of order three. Since the elements of order three of $\mathbb{S}_4$ belong to $\mathbb{A}_4$, the subgroup $\rho(G) \cap \mathbb{A}_4$ of $\mathbb{S}_4$ contains at least eight elements. Therefore $G \simeq \rho(G) \simeq \mathbb{A}_4$.

Sylow's theorems can be used to detect non-simple groups.

EXAMPLE 11.19. If G is a group of order 36, then G is not simple.

Assume that G is simple. Then $n_3 = n_3(G) = 4$. Let $P \in \mathrm{Syl}_3(G)$ and let G act on $X = \{gPg^{-1} : g \in G\}$ by conjugation. This induces a group homomorphism

$$\rho \colon G \to \mathbb{S}_X \simeq \mathbb{S}_4.$$

Since G is simple, either $\ker \rho = \{1\}$ or $\ker \rho = G$. If $\ker \rho = G$, P is normal in G, a contradiction. Thus $\ker \rho = \{1\}$ and hence ρ is injective. In particular, by the first isomorphism theorem,

$$G \simeq G/\ker \rho \simeq \rho(G) \lesssim \mathbb{S}_4.$$

This implies that 36 divides 24, a contradiction.

EXAMPLE 11.20. If G is a group of order 30, then G is not simple.

For every prime number p dividing 30, let $n_p = n_p(G)$. Assume that $n_2 > 1$, $n_3 > 1$ and $n_5 > 1$. Then $n_3 = 10$. There are ten Sylow 3-subgroups, any two of them with trivial intersection. In fact, if $P, Q \in \mathrm{Syl}_3(G)$ are such that $P \neq Q$, then $P \cap Q \leq P$ and hence $|P \cap Q| \in \{1, 3\}$. If $|P \cap Q| = 3$, then $P \cap Q = P$ and $P = Q$, a contradiction. Similarly, there are six Sylow 5-subgroups of G, any two of them with trivial intersection. In conclusion,

$$|G| \geq 1 + 10 \times 2 + 6 \times 4 > 30,$$

a contradiction.

Lecture 12. 23/05/2024

§ 12.1. More about Sylow's theorems.

THEOREM 12.1. *Let N be a normal subgroup of a finite group G and $P \in \mathrm{Syl}_p(G)$. Then $P \cap N \in \mathrm{Syl}_p(N)$. Moreover, every Sylow p-subgroup of N can be obtained this way.*

PROOF. Since N is normal, by Theorem 11.9 applied to the group N, there exists $g \in G$ such that

$$g(P\cap N)g^{-1} = gPg^{-1} \cap gNg^{-1} = gPg^{-1} \cap N \in \mathrm{Syl}_p(N).$$

Then $P \cap N$ is a Sylow p-subgroup of $g^{-1}Ng = N$.

Let $Q \in \mathrm{Syl}_p N$ and $P \in \mathrm{Syl}_p(G)$ be such that $Q \subseteq P$. Then $Q \subseteq P \cap N$. Hence $Q = P \cap N$, as $P \cap N$ is a Sylow p-subgroup of N. □

As a corollary, if G is a finite group and N is a normal subgroup of G, then $n_p(N) \leq n_p(G)$.

THEOREM 12.2. *Let p be a prime number, G be a finite group, $P \in \mathrm{Syl}_p(G)$, and N be a normal subgroup of G. Let $\pi\colon G \to G/N$ be the canonical homomorphism. Then $\pi(P) \in \mathrm{Syl}_p(G/N)$ and every Sylow p-subgroup of G/N can be obtained this way.*

PROOF. Since $\pi(P) = (\pi|_P)(P) \simeq P/N \cap P$, the second isomorphism theorem implies that $\pi(P)$ is a p-group. Since $|PN| = |P||N|/|P \cap N|$,

$$(G/N : \pi(P)) = (G : PN)$$

is not divisible by p. Thus $\pi(P) \in \mathrm{Syl}_p(G/N)$.

If $Q \in \mathrm{Syl}_p(G/N)$, then $Q = \pi(H)$ for some subgroup H of G with $N \subseteq H$. In particular,

$$|Q| = |\pi(H)| = \frac{|H|}{|H \cap N|} = \frac{|H|}{|N|}.$$

Thus

$$(G : H) = \frac{|G|/|N|}{|H|/|N|} = (G/N : Q)$$

is not divisible by p.

Let $X \in \mathrm{Syl}_p(H)$. Since $(G : H)$ is not divisible by p, $X \in \mathrm{Syl}_p(G)$. Hence

$$\pi(X) \subseteq \pi(H) = Q.$$

Thus $\pi(X) = Q$, as $\pi(X) \in \mathrm{Syl}_p(G/N)$. □

As a corollary, if G is a finite group and N is a normal subgroup of G, then $n_p(G/N) \leq n_p(G)$.

COROLLARY 12.3. *Let G be a finite group. Assume that G contains only one Sylow p-subgroup. Then every subgroup and every quotient of G contains only one Sylow p-subgroup.*

PROOF. If H is a subgroup of G, then $n_p(H) \leq n_p(G) = 1$. If N is a normal subgroup of G, then $n_p(G/N) \leq n_p(G) = 1$. □

§ 12.2. Abelian groups. Let A be an abelian group, written additively, and $x_1,\dots,x_k \in A$. The subgroup $\langle x_1,\dots,x_k\rangle$ generated by $\{x_1,\dots,x_k\}$ is the set of integer linear combinations of the elements $x_1,\dots,x_k$, that is

$$\langle x_1,\dots,x_k\rangle = \left\{\sum_{i=1}^{k} m_i x_i : m_1,\dots,m_k \in \mathbb{Z}\right\}.$$

We say that $\{x_1,\dots,x_k\}$ **generates** A if $A = \langle x_1,\dots,x_k\rangle$. And we say that the set $\{x_1,\dots,x_k\}$ is **linearly independent** if

$$\sum_{i=1}^{k} m_i x_i = 0 \implies m_1x_1 = \cdots = m_kx_k = 0.$$

Note that our definition of linearly independence for abelian groups is slightly different from that of linear algebra. For example, in the group $\mathbb{Z}/5$, one has $5x = 0$ for all x. Thus there will be no linearly independent sets with the standard linear algebra definition.

Exercise 12.4. Let A be an abelian group and X and Y be subgroups of A. We say that A is the **direct sum** of X and Y if $A = X+Y$ and $X\cap Y = \{0\}$. In this case, we write $A = X\oplus Y$. Prove that every element $a \in X\oplus Y$ can be written uniquely as $a = x+y$ for $x\in X$ and $y \in Y$.

A subset $\{x_1,\dots,x_k\}$ is a **basis** of A if $A = \langle x_1\rangle \oplus\cdots\oplus\langle x_k\rangle$, that is if $\{x_1,\dots,x_k\}$ is a linearly independent set of generators of A.

Theorem 12.5. *Every finitely generated abelian group has a basis. In particular, it is a finite direct sum of cyclic groups.*

Before proving the theorem, we need a lemma.

Lemma 12.6. *Let $A = \langle x_1,\dots,x_n\rangle$ be a finitely generated abelian group and $c_1,\dots,c_n \in \mathbb{Z}_{>0}$ be such that* $\gcd(c_1,\dots,c_n) = 1$. *Then there exist $y_1,\dots,y_n \in A$ such that $A = \langle y_1,\dots,y_n\rangle$ and*

$$y_1 = c_1x_1+\cdots+c_nx_n.$$

Proof. We proceed by induction on $s = c_1+\cdots+c_n$. The case $s = 1$ is trivial. So assume that $s \geq 2$. Without loss of generality, we may assume that $c_1 \geq c_2 > 0$. Then

$$(c_1-c_2)+c_2+c_3+\cdots+c_n = c_1+c_3+\cdots+c_n < s.$$

Moreover, $\gcd(c_1-c_2,c_2,\dots,c_n) = 1$. Since $A = \langle x_1,x_1+x_2,x_3,\dots,x_n\rangle$, the inductive hypothesis implies that there exist $y_1,\dots,y_n \in A$ such that $A = \langle y_1,\dots,y_n\rangle$ and

$$y_1 = (c_1-c_2)x_1+c_2(x_1+x_2)+c_3x_3+\cdots+c_nx_n = c_1x_1+c_2x_2+\cdots+c_nx_n. \qquad \square$$

Now we are ready to prove the main theorem of this section.

Proof of Theorem 12.5. We proceed by induction on the number n of generators. The case $n = 1$ is trivial. So assume that the result holds for $n-1$ generators. Among the generating sets $\{x_1,\dots,x_n\}$ with n elements, there is one for which the order $|x_1|$ of x_1 is the smallest possible. By the inductive hypothesis, the theorem will be proved if we can show that

$$A = \langle x_1\rangle \oplus \langle x_2,\dots,x_n\rangle \tag{12.1}$$

holds. Assume that (12.1) does not hold. Note that $A = \langle x_1\rangle + \langle x_2,\dots,x_n\rangle$, as $\{x_1,\dots,x_n\}$ is a generating set of A. Since the decomposition (12.1) does not hold, $\langle x_1\rangle \cap \langle x_2,\dots,x_n\rangle \neq \{0\}$. Let

$\xi \in \langle x_1 \rangle \cap \langle x_2, \dots, x_n \rangle$ be a non-zero element. Then $\xi = m_1x_1 = m_2x_2 + \cdots + m_nx_n$ for some integer $m_1x_1 \neq 0$ and $m_2, \dots, m_n \in \mathbb{Z}$ not all zero. Thus

$$(-m_1)x_1 + m_2 + \cdots + m_nx_n = 0.$$

After changing the sign of some of the generators, we produce a generating set $\{z_1, \dots, z_k\}$ of A such that our linear combination becomes

$$\lambda_1 z_1 + \lambda_2 z_2 + \cdots + \lambda_n z_n = 0,$$

where $\lambda_1, \dots, \lambda_n \in \mathbb{Z}_{\geq 0}$ and $0 < \lambda_1 < |z_1|$. Let $d = \gcd(\lambda_1, \dots, \lambda_n)$ and for each $i \in \{1, \dots, n\}$, let $c_i = \lambda_i / d$. By Lemma 12.6, there exist $y_1, \dots, y_n \in A$ such that $A = \langle y_1, \dots, y_n \rangle$ and

$$y_1 = c_1 z_1 + \cdots + c_n z_n.$$

But $dy_1 = \lambda_1 z_1 + \cdots + \lambda_n z_n = 0$ and $d \leq \lambda_1 < |x_1|$. We have found a generating set $\{y_1, \dots, y_n\}$ in which the element y_1 has order smaller than $|x_1|$, a contradiction. □

The previous theorem translates into the following result.

Theorem 12.7. *Let A be a non-zero finitely generated abelian group. Then*

$$A \simeq (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_k) \times \mathbb{Z}^r,$$

for integers $n_1, \dots, n_k \geq 2$ and $r \geq 0$. The integers $n_1, \dots, n_k$ can be chosen so that $n_1 \geq 2$ and n_j divides n_{j+1} for all $j \in \{1, \dots, k-1\}$.

The integer r in Theorem 12.7 is uniquely determined by A and is called the **rank** of A. The integers $n_1, \dots, n_k$ in Theorem 12.7 are called the **invariant factors** of A and are uniquely determined by A.

In these notes, we will not prove that the rank and the invariant factors are uniquely determined by the group. Additionally, we will not prove the existence of the invariant factors. Instead, we will explain how to obtain them with some concrete examples.

Example 12.8. Let $A = (\mathbb{Z}/6) \times (\mathbb{Z}/100) \times (\mathbb{Z}/45)$. We use the fact that $(\mathbb{Z}/a) \times (\mathbb{Z}/b) \simeq \mathbb{Z}/ab$ whenever $\gcd(a,b) = 1$ to decompose A as follows:

$$A \simeq (\mathbb{Z}/2 \times \mathbb{Z}/3) \times (\mathbb{Z}/4 \times \mathbb{Z}/25) \times (\mathbb{Z}/5 \times \mathbb{Z}/9).$$

Let us order the prime powers: 2, 4, 3, 9, 5, 25. Now we collect the highest prime powers appearing in our decomposition: 4 is the highest power of 2, 9 is the highest power of 3, and 25 is the highest power of 5. Thus $s_2 = 4 \times 9 \times 25 = 900$ is the highest invariant factor. Now 2 is the highest remaining power of 2, 3 is the highest power of 3 and 5 is the highest power of 5. Thus $s_1 = 2 \times 3 \times 5 = 30$ is the second invariant factor. Thus

$$A \simeq (\mathbb{Z}/30) \times (\mathbb{Z}/900).$$

Example 12.9. Let $A = (\mathbb{Z}/10) \times (\mathbb{Z}/15) \times (\mathbb{Z}/20) \times (\mathbb{Z}/25)$. As we did in the previous example, we decompose each factor:

$$A \simeq (\mathbb{Z}/2) \times (\mathbb{Z}/5) \times (\mathbb{Z}/3) \times (\mathbb{Z}/5) \times (\mathbb{Z}/4) \times (\mathbb{Z}/5) \times (\mathbb{Z}/25).$$

The numbers we see are 2, 4, 3, 5, 5, 25. The invariant factors are then $s_3 = 4 \times 3 \times 25 = 300$, $s_2 = 10$, $s_3 = 5$ and $s_4 = 5$. Hence

$$A \simeq (\mathbb{Z}/5) \times (\mathbb{Z}/5) \times (\mathbb{Z}/10) \times (\mathbb{Z}/300).$$

Exercise 12.10. Find the invariant factors of the group $(\mathbb{Z}/4) \times (\mathbb{Z}/6) \times (\mathbb{Z}/8) \times (\mathbb{Z}/12)$.

Some solutions

1.3. If e and e_1 are both neutral elements, then $e = ee_1 = e_1$.

1.5. If $ax = b$, after multiplying on the left by a^{-1} we obtain that $x = a^{-1}b$. Similarly, the equation $xa = b$ has $x = ba^{-1}$ as its unique solution.

1.9. For $g \in G$, the map $L_g \colon G \to G$, $x \mapsto gx$, is invertible with inverse $L_{g^{-1}}$, as

$$(L_g \circ L_{g^{-1}})(x) = g(g^{-1}x) = (gg^{-1})x = x$$

for all $x \in G$. Similarly, $L_{g^{-1}} \circ L_g)(x) = x$ for all $x \in G$.

In the same way, we prove that for each $g \in G$, the map $R_{g^{-1}}$ is the inverse of R_g.

1.17. The neutral element of $G \times H$ is $(1,1)$, as $(1,1)(g,h) = (g,h) = (g,h)(1,1)$. The inverse of (g,h) is $(g,h)^{-1} = (g^{-1},h^{-1})$, as

$$(g,h)(g,h)^{-1} = (g,h)(g^{-1},h^{-1}) = (gg^{-1},hh^{-1}) = (1,1),$$
$$(g,h)^{-1}(g,h) = (g^{-1},h^{-1})(g,h) = (g^{-1}g,h^{-1}h) = (1,1).$$

To prove the associativity, let $g,g_1,g_2 \in G$ and $h,h_1,h_2 \in H$. Since G and H are groups, their multiplications are associative. Then

$$\begin{aligned}((g,h)(g_1,h_1))(g_2,h_2) &= (gg_1,hh_1)(g_2,h_2) = ((gg_1)g_2,(hh_1)h_2)\\ &= (g(g_1g_2),h(h_1h_2)) = (g,h)(g_1g_2,h_1h_2) = (g,h)((g_1,h_1)(g_2,h_2)).\end{aligned}$$

2.6. Clearly $1 \in Z(G)$. If $x \in Z(G)$, then $xg = gx$ for all $g \in G$. Multiplying by x^{-1} on the left and on the right, we get that $gx^{-1} = x^{-1}$ holds for all $g \in G$. Finally, if $x,y \in Z(G)$. Then

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

for all $g \in G$. Hence $xy \in Z(G)$.

2.7. Since S is a subgroup, $1 \in S$ and if $x,y \in S$, then $x^{-1} \in S$ and $xy \in S$. Now $1 \in gSg^{-1}$, as $1 \in S$ and $1 = g1g^{-1}$. If $x \in gSg^{-1}$, then $x = gsg^{-1}$ for some $s \in S$. Thus

$$x^{-1} = (gsg^{-1})^{-1} = gs^{-1}g^{-1} \in gSg^{-1},$$

as $s^{-1} \in S$. Finally, if $x = gsg^{-1} \in gSg^{-1}$ and $y = gtg^{-1} \in gSg^{-1}$ for some $s,t \in S$, then

$$xy = (gsg^{-1})(gtg^{-1}) = g(st)g^{-1} \in gSg^{-1},$$

as $st \in S$.

2.8. If $\sigma \in Z(\mathbb{S}_3)$ and $\sigma \neq \mathrm{id}$, there exists $i \in \{1,2,3\}$ such that $\sigma(i) \neq i$. Let $j = \sigma(i)$ and $k \in \{1,2,3\} \setminus \{i,j\}$. Then $(jk)\sigma$ is a permutation such that $i \mapsto k$, while $\sigma(jk)$ is such that $i \mapsto j$. In particular, $(jk)\sigma \neq \sigma(jk)$, a contradiction.

The group $\mathbb{S}_3$ has six elements: id, (12), (13), (23). (123) and (132). First note that $\mathrm{id} \in C_{\mathbb{S}_3}((12))$ and $(12) \in C_{\mathbb{S}_3}((12))$. However, the permutations (23), (13), (123) and (132) do not commute with (12). For example,

$$(23)(12) = (132) \neq (123) = (12)(23).$$

2.9. Let us prove $\implies$. Since $1 \in S$, then $S \neq \emptyset$. If $u, v \in S$, then $v^{-1} \in S$ and $uv^{-1} \in S$.

Let us prove now $\impliedby$. If $S \neq \emptyset$, let $u \in S$. Then $1 = uu^{-1} \in S$. The assumption Let $u, v \in S$. The assumption with $x = 1 \in S$ and $y = v$ yields $v^{-1} \in S$. The assumption with $x = u$ and $y = v^{-1}$ yields $uv \in S$.

2.10. The identity matrix belongs to $\mathbf{SL}_n(\mathbb{R})$. If $a, b \in \mathbf{SL}_n(\mathbb{R})$, then $ab^{-1} \in \mathbf{SL}_n(\mathbb{R})$, as

$$\det(ab^{-1}) = \det(a)\det(b^{-1}) = \det(a)\det(b)^{-1} = 1.$$

By Exercise 2.9, $\mathbf{SL}_n(\mathbb{R})$ is a subgroup of $\mathbf{GL}_n(\mathbb{R})$.

2.11. Let $\{H_\lambda : \lambda \in \Lambda\}$ be a collection of subgroups of a group G and $H = \cap_{\lambda\in\Lambda} H_\lambda$. We claim that H is a subgroup of G. Since $1 \in H_\lambda$ for all λ, H is non-empty. If $x, y \in H$, then $x, y \in H_\lambda$ for all λ. Since each H_λ is a subgroup of G, $xy^{-1} \in H_\lambda$ for all λ. Thus $xy^{-1} \in H$.

2.13. Let

$$H = \{x_1^{n_1} \cdots x_k^{n_k} : k \geq 0, x_1, \dots, x_k \in X, -1 \leq n_1, \dots, n_k \leq 1\}.$$

To prove that $H \subseteq \langle X \rangle$, let $h = x_1^{n_1} \cdots x_k^{n_k} \in H$. If S is a subgroup of G containing X, then $x_j \in S$ for all j. This implies that $h = x_1^{n_1} \cdots x_k^{n_k} \in S$. Thus

$$h \in \bigcap_{\substack{S \leq G \\ X \subseteq S}} S.$$

To prove that $H \supseteq \langle X \rangle$ we first claim that H is a subgroup of G. Note that $H \neq \emptyset$, as $1 \in H$ (this is the empty word). If $u = x_1^{n_1} \cdots x_k^{n_k} \in H$ and $v = x_{k+1}^{n_{k+1}} \cdots x_l^{n_l} \in H$, then

$$uv^{-1} = x_1^{n_1} \cdots x_k^{n_k} x_l^{-n_l} \cdots x_{k+1}^{-n_{k+1}} \in H.$$

Now note that H is a subgroup of G containing X. Thus

$$\langle X \rangle = \bigcap_{\substack{S \leq G \\ X \subseteq S}} S \subseteq H.$$

2.16. Let $G = \mathbb{S}_3$. Then $H = \{\mathrm{id}, (12)\}$ and $K = \{\mathrm{id}, (23)\}$ are subgroups of G. However, $H \cup K = \{\mathrm{id}, (12), (23)\}$ is not a subgroup, as $(12)(23) = (123) \notin H \cup K$.

4.5. Let $\{e_1, \dots, e_n\}$ be the standard basis of $\mathbb{R}^n$. To prove this formula note that

$$E_{i,j} e_k = \begin{cases} e_i & \text{if } j = k, \\ 0 & \text{if } j \neq k. \end{cases}$$

and verify that $P_\sigma e_k = \sum_{i=1}^n E_{\sigma(i),i} e_k$ for all $k \in \{1, \dots, n\}$. Since P_σ and $\sum_{i=1}^n E_{\sigma(i),i}$ coincide in a basis of $\mathbb{R}^n$, they are equal.

5.16. Since N is normal in G, the operation is well-defined. Routine calculations show that the operation is associative, that N is the neutral element of G/N and that the inverse of an element xN is $(xN)^{-1} = x^{-1}N$. For example, for the associativity, we note that for $x, y, z \in G$ one has

$$((xN)(yN))(zN) = ((xy)N)zN = (xy)zN,$$

equals

$$(xN)((yN)(zN)) = (xN)((yz)N) = x(yz)N.$$

since $x(yz) = (xy)z$.

5.18. For $x,y \in G$,

$$(xH)(yH) = (yH)(xH) \iff (xy)H = (yx)H \iff x^{-1}y^{-1}xy \in H.$$

Thus G/H is abelian if and only if $[x,y] = xyx^{-1}y^{-1} \in H$ for all $x,y \in G$.

5.20. Assume that $G/Z(G)$ is generated by $gZ(G)$. Let $x,y \in G$. Then $xZ(G) = g^kZ(G)$ and $yZ(G) = g^lZ(G)$ for some $k,l \in \mathbb{Z}$, that is $x = g^kz_1$ and $y = g^lz_2$ for some $k,l \in \mathbb{Z}$ y $z_1,z_2 \in Z(G)$. Thus $xy = yx$.

5.24. If $g \in G \setminus H$, then $g^n = 1 \in H$, where $n = |G|$. Since p is prime, n has no prime divisors $< p$. By Exercise 5.23, H is normal in G.

6.2. We need to show that $HK = KH$. We first prove that $HK \subseteq KH$. If $x = hk \in HK$, then $x = k(k^{-1}hk) \in KH$, as $k^{-1}hk \in H$. To prove that $HK \supseteq KH$, let $y = kh \in KH$. Then $y = (khk^{-1})k \in HK$, as $khk^{-1} \in H$.

6.36. Just note that $\mathscr{U}(\mathbb{Z}/12)$ has no elements of order four.

10.9. If G is a p-group, then, by Lagrange's theorem, every element has order a power of p. Conversely, if q is a prime divisor of $|G|$, by Cauchy's theorem, there exists $g \in G$ of order q. Thus $q = p$.

12.10. Decompose A as $(\mathbb{Z}/4) \times (\mathbb{Z}/2) \times (\mathbb{Z}/3) \times (\mathbb{Z}/8) \times (\mathbb{Z}/4) \times (\mathbb{Z}/3)$. We list the highest powers appearing in our decomposition of A:

$$\begin{array}{cc} 8 & 3 \\ 4 & 3 \\ 4 & \\ 2 & \end{array}$$

Then $s_1 = 2$, $s_2 = 4$, $s_3 = 12$ and $s_4 = 24$. Hence $A \simeq (\mathbb{Z}/24) \times (\mathbb{Z}/12) \times (\mathbb{Z}/4) \times (\mathbb{Z}/2)$.

References

[1] M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[2] R. D. Carmichael. *Introduction to the theory of groups of finite order*. Dover Publications, Inc., New York, 1956.

[3] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[4] R. M. Guralnick. Commutators and commutator subgroups. *Adv. in Math.*, 45(3):319–330, 1982.

[5] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[6] S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.

Index