Leandro Vendramin

Group theory

Notes

Sunday 2[nd] July, 2023

Preface

The notes correspond to the bachelor course *Ring and Modules* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve or thirteen two-hours lectures.

The material is somewhat standard. Basic texts on abstract algebra are for example [1], [2] and [3]. Lang's book [4] is also a standard reference, but maybe a little bit more advanced. We based the lectures on representation theory of finite groups on [5] and [6].

We also mention a set of great expository papers by Keith Conrad available at https://kconrad.math.uconn.edu/blurbs/. The notes are extremely well-written and are useful at every stage of a mathematical career.

Bibtex information:

```
@misc{rings,
    author={Vendramin, L.},
    title={Rings and modules},
    year={2022},
    note={Available at www.github.com/vendramin/rings},
    pages={106}
}
```

Thanks go to Wouter Appelmans, Arne van Antwerpen, Ilaria Colazzo, Luca Descheemaeker, Łukas Kubat, Lucas Simons and Geoffrey Jassens.

This version was compiled on Sunday 2nd July, 2023 at 17:02. Please send comments and corrections to me at Leandro.Vendramin@vub.be.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Groups

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

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

Note that 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, for example, 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 every $x \in G$ there exists $y \in G$ such that $xy = yx = e$.

The associativity condition implies that all ordered products that we can form with the elements, say, $x_1, x_2, \dots, x_n$ 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. We will provide an alternative proof as an application of Cayley's theorem.

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 $z = z(xy) = (zx)y = ey = y$. $\square$

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 identity 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.

It is a good idea to keep in mind the *group of invertible matrices*. With this, the the following properties 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, the equation $x = ba^{-1}$ 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 $-x$.

Definition 1.7. 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.

Example 1.8. Let us see some 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) $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ 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 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 1.8 are infinite groups.

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) $(g^k)^l = g^{kl}$ for all $k, l \in \mathbb{Z}$.
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 formal 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. Moreover, the set $\cup_{n \geq 1} G_n$ is an abelian group.

Example 1.12. Let X be a 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 elemants. Let $f : X \to X$ be such that $f(a) = b$, $f(b) = c$ and $f(c) = a$ and $g : X \to X$ 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 $f : \{1, \dots, n\} \to \{1, \dots, n\}$. To denote permutations, we can use the following convention. The symbol

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

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

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

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 rather intuitive. Let us decompose the permutation

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

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

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

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

There is a handy way of writing permutations. It is based on *decomposing permutations as a product of disjoint cycles*. In this particular case, the elements of $\mathbb{S}_3$ are

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

where, for example, 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 of this group?

Example 1.15. The set of maps

$$G = \left\{ x, \frac{1}{x}, 1-x, \frac{1}{1-x}, \frac{x}{x-1}, \frac{x-1}{x} \right\}$$

is a non-abelian group with the usual composition of maps. Let $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ (here ∞ is just a symbol) and assume that the following rules hold:

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

Then G is 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:

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

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 units of $\mathbb{Z}/n$ form a group with the usual multiplication modulo n. We will use the following notation:

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

The order of $\mathcal{U}(\mathbb{Z}/n)$ 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 discuss a concrete example. The table of $\mathcal{U}(\mathbb{Z}/8) = \{1,3,5,7\}$ is

$$\begin{array}{r|rrrr} & 1 & 3 & 5 & 7 \\ \hline 1 & 1 & 3 & 5 & 7 \\ 3 & 3 & 1 & 7 & 5 \\ 5 & 5 & 7 & 1 & 3 \\ 7 & 7 & 5 & 3 & 1 \end{array}$$

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

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

Example 2.5. $S^1 = \{z \in \mathbb{C} : |z| = 1\} \leq \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

Example 2.6. 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

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

Exercise 2.7. 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.

Exercise 2.8. Let G be a group and $g \in G$. Prove that the **centralizer**

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

of g in G is a subgroup of G.

One can prove that, if G is a group, then $Z(G) = \cap_{g \in G} C_G(g)$.

Exercise 2.9. 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: ${}^{g}S = gSg^{-1}$.

Exercise 2.10. Prove that $Z(\mathbb{S}_3) = \{\mathrm{id}\}$ and compute $C_{\mathbb{S}_3}((12))$.

The following exercise is useful:

Exercise 2.11. 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 2.12. $\mathbf{SL}_n(\mathbb{R}) = \{a \in \mathbf{GL}_n(\mathbb{R}) : \det(a) = 1\} \leq \mathbf{GL}_n(\mathbb{R})$.

Exercise 2.13. 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 set of elements.

Definition 2.14. Let G be a group and X a subset of G. The **subgroup generated** by X is the smallest subgroup of G that contains X, that is

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

One can indeed check that if $S \leq G$ is such that $X \subseteq S$, then $S \subseteq \langle X \rangle$. 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 in the case of finite sets. 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 2.15. 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 $x_1, \dots, x_n$.

Example 2.16. 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 arbitrary element of $\mathbb{D}_n$ is a word of the form $r^{i_1} s^{j_1} r^{i_2} s^{j_2} \cdots$, where $i_1, i_2, \dots \in \{0, 1, \dots, n-1\}$ 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 $j \in \{0, 1\}$. In particular, $|\mathbb{D}_n| = 2n$.

To understand better the previous example, we discuss two concrete particular cases. If $n = 3$,

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

and we obtain (another representation of) the group of symmetries of a regular triangule. If $n = 4$,

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

and we obtain (another representation of) the group of symmetries of the square.

Exercise 2.17. The union of subgroups is not, in geenral, a subgroup. Can you give an example?

§3. Subgroups of $\mathbb{Z}$

It is time for the first theorem. What can we say about the subgroups of $\mathbb{Z}$?

Theorem 3.1. *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 this m exists? Since $S \neq \{0\}$, it contains an element $n \in S \setminus \{0\}$. There are then two possible cases: $n > 0$ o bien $-n > 0$. 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 r such that $0 \leq r < m$. Suppose that $r \neq 0$. Since $x, m \in S$, $r \in S$, 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

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

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

Exercise 3.2. 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

$$\begin{aligned} a \text{ y } b \text{ son coprimos} &\Longleftrightarrow \gcd(a, b) = 1 \\ &\Longleftrightarrow \mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \\ &\Longleftrightarrow \text{existen } r, s \in \mathbb{Z} \text{ tales que } ar + bs = 1. \end{aligned}$$

Exercise 3.3. 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 $m = \operatorname{mcm}(a, b)$.

Exercise 3.4. Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $m = \operatorname{mcm}(a, b)$. 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 3.5. Let $a, b \in \mathbb{Z}_{\geq 1}$. Prove that if $d = \gcd(a, b)$ and $m = \operatorname{mcm}(a, b)$, then $ab = dm$.

§4. Commutators

Definition 4.1. The **commutator subgroup** $[G,G]$ of G is the subgroup generated by the commutators of G, that is

$$[G,G] = \langle [x,y] \mid x,y \in G \rangle,$$

where $[x,y] = xyx^{-1}y^{-1}$ is the commutator of x and y.

In the literature, the commutator subgroup of a group G is also called the **derived subgroup** of G.

Example 4.2. In $\mathbb{Z}$, the commutator of $x, y \in \mathbb{Z}$ is the integer

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

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

Exercise 4.3. Prove that $[\mathbb{S}_3,\mathbb{S}_3] = \{\mathrm{id},(123),(132)\}$.

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

Example 4.4. 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.

The following example goes back to Guralnick [**?**]. It was found by hand, when computers were no so popular in group theory as they are now.

Example 4.5. 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. Moreover, G is the smallest group with the property that the set of commutators is not a subgroup.

§5. Cyclic groups

Definition 5.1. 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.

Examples 5.2.

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

Exercise 5.4. Prove that subgroups of a cyclic group are cyclic.

Definition 5.5. 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 5.6. *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 $g = 1$, thens $n = 1$. 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. □

Corollary 5.7. *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 5.8. 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 5.9. 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 5.10. 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.

Exercise 5.11. Prove that every group of odd order contains an element of order two.

Let us see some concrete examples:

Example 5.12. In $\mathbb{S}_3$ we have the following order pattern:

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

Example 5.13. In $\mathbb{Z}$, every non-zero element has infinite order.

Example 5.14. 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 5.15. The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$ has infinite order.

Example 5.16. The group $G_\infty = \bigcup_{n \geq 1} G_n$ is abeliano and infinite. Note that every element of G_∞ has finite order.

We conclude the topic with some exercises.

Exercise 5.17. Compute the orders of the elements of $\mathbb{Z}/6$.

Exercise 5.18. 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 5.19. Compute the order of $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbf{GL}_2(\mathbb{R})$.

Exercise 5.20. Prove that in $\mathbb{D}_n$ one has $|r^j s| = 2$ and $|r^j| = n/\gcd(n, j)$.

Exercise 5.21. Prove that a group with finitely many subgroups is finite.

Lecture 3

§6. 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:

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

Exercise 6.1. Prove that (3.1) is an equivalence relation. This means that the following properties hold:

1) $x \equiv x \bmod H$ for all x.
2) If $x \equiv y \bmod H$, then $y \equiv x \bmod H$.
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.

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

Proposition 6.2. *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** of H in G.

Proposition 6.3. *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

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

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

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

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

Example 6.4. 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 6.5. 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

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

Note that our group decomposes as

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

Example 6.6. 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 $p \in R^2$, the coset $p + L$ is the line parallel to L that passes through p.

Definition 6.7. If H is a subgroup of G, the **índex** of H in G is the number $(G : H)$ of left (or right) cosets of H in G.

The following important theorem will be used extensively.

Theorem 6.8 (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 6.9. *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 6.10. *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 $G = H = \langle g \rangle$. $\square$

Corollary 6.11. *If G is an 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 os 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). $\square$

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

Exercise 6.12 (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 6.13 (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 6.14. Consider the **alternating group**

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

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 6.15. 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.

Some solutions

References

1. M. Artin. *Algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.
2. D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.
3. T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.
4. S. Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.
5. J.-P. Serre. *Linear representations of finite groups*. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.
6. B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.

Index