Aluffi, *Algebra: Chapter 0*

Danny Nygård Hansen

26th January 2022

I • Preliminaries: Set theory and categories

II • Groups, first encounter

II.1. Definition of group

Exercise 1.4

Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

Solution. The hypothesis implies that $g = g^{-1}$ for all $g \in G$. For $g, h \in G$ we thus have

$$gh = (gh)^{-1} = h^{-1}g^{-1} = hg$$

as desired. □

Exercise 1.8

Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$.

Solution. Every element g in G different from e and f has order greater than two, hence $g \neq g^{-1}$. The product $\prod_{g \in G \setminus \{e,f\}} g$ therefore contains all such elements along with their inverses, and thus equals e. The claim follows. □

Exercise 1.9

Let G be a finite group, of order n, and let m be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if n is even, then G necessarily contains elements of order 2.

SOLUTION. Let G' denote the set of elements in G with order greater than 2. We claim that $|G'|$ is even, and we give two arguments for this fact. First, simply notice that the elements of G' come in pairs $\{g, g^{-1}\}$ with $g \neq g^{-1}$.

For a more precise argument (using group theory language we haven't seen yet), consider the inversion map $g \mapsto g^{-1}$. This restricts to a well-defined map $\iota\colon G' \to G'$, and ι is a permutation of G'. Letting the cyclic group $\langle \iota \rangle \leq S_{G'}$ act on G' splits G' into orbits of size two, and since these orbits determine a partition of G', $|G'|$ must be even.

Now notice that G' contains $n - m - 1$ elements since e has order 1, hence $n - m$ is odd. If n is even, then m must be odd and thus at least 1. □

EXERCISE 1.11

Prove that for all g, h in a group G, $|gh| = |hg|$.

SOLUTION. Let $a, g \in G$, and let $n = |g|$. Then

$$(aga^{-1})^n = ag^n a^{-1} = e,$$

so the order of aga^{-1} divides the order of g. Substituting $g \to aga^{-1}$ and $a \to a^{-1}$ shows that $|g|$ also divides $|aga^{-1}|$, so $|g| = |aga^{-1}|$. Finally substituting $g \to gh$ and $a \to h$ proves the claim.

Alternatively, the conjugation map $g \mapsto aga^{-1}$ is an isomorphism, so it preserves orders. □

EXERCISE 1.13

Give an example showing that $|gh|$ is not necessarily equal to $\operatorname{lcm}(|g|, |h|)$, even if g and h commute.

SOLUTION. In $\mathbb{Z}/4\mathbb{Z}$ we have $|[2]_4| = 2$ and $|[2]_4 + [2]_4| = |[0]_4| = 1$. □

EXERCISE 1.14

Prove that if g and h commute *and* $\gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$.

SOLUTION. First recall that $\operatorname{lcm}(|g|, |h|) = |g||h|$, so Proposition 1.14 implies that $|gh|$ divides $|g||h|$. Conversely, letting $N = |gh|$ we have

$$e = (gh)^{|g|N} = g^{|g|N} h^{|g|N} = h^{|g|N},$$

so $|h|$ divides $|g|N$. But since $|g|$ and $|h|$ are relatively prime, $|h|$ divides N. So does $|g|$, so again using relative primality we find that $|g||h|$ divides N. In total, $|gh| = |g||h|$. □

II.2. Examples of groups

Exercise 2.1

One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$ by letting the entry at[1] $(i, \sigma(i))$ be 1 and letting all other entries be 0. Prove that, with this notation,

$$M_\sigma M_\tau = M_{\tau\sigma}$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices.

Solution. Notice that, for $1 \leq i, j \leq n$,

$$(M_\sigma M_\tau)_{ij} = \sum_{k=1}^{n} (M_\sigma)_{ik} (M_\tau)_{kj},$$

and that the summand $(M_\sigma)_{ik}(M_\tau)_{kj}$ is 1 just when $\sigma(i) = k$ and $\tau\sigma(i) = j$, and 0 otherwise. Thus,

$$(M_\sigma M_\tau)_{ij} = \begin{cases} 1, & \tau\sigma(i) = j, \\ 0, & \text{otherwise}, \end{cases}$$

which is just the definition of the matrix $M_{\tau\sigma}$. □

Exercise 2.5

Describe generators and relations for all dihedral groups D_{2n}.

Solution. Consider a regular n-gon, let x be reflection about a line through its centre and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. Then x and y generate D_{2n} subject to a series of relations. First of all, clearly $x^2 = e$ and $y^n = e$ (more precisely, x and y have order 2 and n respectively). Furthermore, a geometric argument shows that $(xy)^2 = e$, or equivalently that $yx = xy^{n-1}$. By applying this third relation successively, any product $x^{i_1} y^{i_2} x^{i_3} y^{i_4} \cdots$ can be reduced to one on the form $x^i y^j$. Using the other two relations we find that we can choose i and j such that $0 \leq i \leq 1$ and $0 \leq j < n$, which yields $2n$ products on this form.

Next we show that all these products are different. Given two products $x^{i_1} y^{j_1}$ and $x^{i_2} y^{j_2}$, if either $i_1 = i_2$ or $j_1 = j_2$ then this is obvious. So assume that $i_1 \neq i_2$ and $j_1 \neq j_2$. Without loss of generality also assume that $i_1 = 0$ and $i_2 = 1$. Now consider the equation

$$y^{j_2 - j_1} = x.$$

[1] Contrary to Aluffi, we prefer to let permutation act on the left.

It follows from Proposition 1.13 that $j_2 - j_1 = \pm n/2$. But the third relation above then implies that

$$y^{\frac{n}{2}+1} = y^{\frac{n}{2}+n-1},$$

or $e = y^{n-2}$ which is impossible. Hence the equation has no solutions, and all products $x^i y^j$ are distinct. □

EXERCISE 2.13

Prove that if $\gcd(m,n) = 1$, then there exist integers a and b such that

$$am + bn = 1.$$

Conversely, prove that if $am+bn = 1$ for some integers a and b, then $\gcd(m,n) = 1$.

SOLUTION. By Corollary 2.5, the class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. Hence there exists an $a \in \mathbb{Z}$ such that $a[m]_n = [1]_n$. But then $qn = am - 1$ for some $q \in \mathbb{Z}$, i.e. $am + (-q)n = 1$.

Conversely, if $am + bn = 1$ and d divides both m and n, then d also divides 1 and hence $d = \pm 1$. □

II.3. The category **Grp**

EXERCISE 3.3

Show that if G, H are *abelian* groups, then $G \times H$ satisfies the universal property for coproducts in **Ab**.

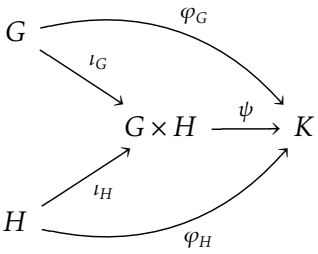
SOLUTION. Let $\varphi_G \colon G \to K$ and $\varphi_H \colon H \to K$ be homomorphisms into an abelian group K. Define a map $\psi \colon G \times H \to K$ by

$$\psi(g,h) = \varphi_G(g)\varphi_H(h).$$

We first show that ψ is a group homomorphism. For $g_1, g_2 \in G$ and $h_1, h_2 \in H$ we have

$$\begin{aligned}\psi((g_1,h_1)(g_2,h_2)) &= \psi(g_1g_2, h_1h_2) = \varphi_G(g_1g_2)\varphi_H(h_1h_2)\\ &= \varphi_G(g_1)\varphi_G(g_2)\varphi_H(h_1)\varphi_H(h_2)\\ &= \varphi_G(g_1)\varphi_H(h_1)\varphi_G(g_2)\varphi_H(h_2)\\ &= \psi(g_1,h_1)\psi(g_2,h_2).\end{aligned}$$

In the fourth equality we used that K is abelian. Next we show that the diagram



commutes, where $\iota_G(g) = (g, e_H)$ and $\iota_H(h) = (e_G, h)$. For the upper triangle we have

$$(\psi \circ \iota_G)(g) = \psi(g, e_G) = \varphi_G(g)\varphi_H(e_G) = \varphi_G(g)e_K = \varphi_G(g),$$

and similarly for the lower triangle. Finally notice that ψ is unique with this property, since if $\chi\colon G \times H \to K$ is any such homomorphism we have

$$\chi(g,h) = \chi(g,e_H)\chi(e_G,h) = (\chi \circ \iota_G)(g)(\chi \circ \iota_H)(h) = \varphi_G(g)\varphi_H(h),$$

so $\chi = \psi$. □

Exercise 3.4

Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial?

Solution. Let H be any nontrivial group, and let $G = \prod_{n\in\mathbb{N}} H$. Then the map $\varphi\colon G \to H \times G$ given by

$$\varphi(h_1, h_2, h_3, \ldots) = \Big(h_1, (h_2, h_3, \ldots)\Big)$$

is an isomorphism. □

Exercise 3.5

Prove that $\mathbb{Q}$ is not the direct product of two nontrivial groups.

Solution. Let G and H be groups such that there is an isomorphism $\varphi\colon \mathbb{Q} \to G \times H$. Assume without loss of generality that G is nontrivial, and consider the map $\varphi_G = \pi_G \circ \varphi$. We claim that φ_G is injective.

First notice that if $g \in G$ has finite order then $g = 0_G$, since $(g, 0_H)$ has finite order in $G \times H$. Let $p, q \in \mathbb{Z}$ with $p, q \neq 0$, and notice that $\varphi_G(p/q) = 0_G$ implies that

$$0_G = q\varphi_G\left(\frac{p}{q}\right) = \varphi_G(p) = p\varphi_G(1).$$

Hence $\varphi_G(1) = 0_G$, and so $\mathbb{Z} \subseteq \ker \varphi_G$. Furthermore, if $a, b \in \mathbb{Z}$ with $b \neq 0$, then

$$b\varphi_G\left(\frac{a}{b}\right) = \varphi_G(a) = 0_G,$$

so $\varphi_G(a/b)$ has finite order and hence equals 0_G. Thus if $\ker \varphi_G$ is nontrivial, then $\ker \varphi_G = \mathbb{Q}$. But since φ_G is surjective and G is nontrivial, this is impossible. Hence φ_G is injective. On the other hand, the kernel of φ_G is clearly $1 \times H$, so H must be trivial. □

EXERCISE 3.6

Consider the product $C_2 \times C_3$ of the cyclic groups C_2, C_3. By Exercise 3.3, this group is a coproduct of C_2 and C_3 in **Ab**. Show that it is *not* a coproduct of C_2 and C_3 in **Grp**.

SOLUTION. Denote by g and h generators of C_2 and C_3 respectively, and define group homomorphisms $\varphi_2 \colon C_2 \to S_3$ and $\varphi_3 \colon C_3 \to S_3$ by

$$\varphi_2(g) = (1\ 2) \quad \text{and} \quad \varphi_3(h) = (1\ 2\ 3).$$

Assume that $C_2 \times C_3$ is a coproduct of C_2 and C_3 in **Grp**. Then there exists a homomorphism $\psi \colon C_2 \times C_3 \to S_3$ such that $\varphi_2 = \psi \circ \iota_2$ and $\varphi_3 = \psi \circ \iota_3$. Since $C_2 \times C_3$ is commutative, it follows that

$$(1\ 2)(1\ 2\ 3) = \psi(\iota_2(g)\iota_3(h)) = \psi(\iota_3(h)\iota_2(g)) = (1\ 2\ 3)(1\ 2).$$

But this is false, so $C_2 \times C_3$ is not a coproduct of C_2 and C_3 in **Grp**. □

EXERCISE 3.8

Define a group G with two generators x, y subject (only) to the relations $x^2 = e_G$, $y^3 = e_G$. Prove that G is a coproduct of C_2 and C_3 in **Grp**.

SOLUTION. Denote the generators of C_2 and C_3 by g and h respectively, and let $\varphi_2 \colon C_2 \to H$ and $\varphi_3 \colon C_3 \to H$ be homomorphisms into a group H. Define a map $\psi \colon G \to H$ by letting $\psi(x) = \varphi_2(g)$ and $\psi(y) = \varphi_3(h)$ and extending to all elements in G by requiring that ψ be a homomorphism. Then $\varphi_2 = \psi \circ \iota_2$ and $\varphi_3 = \psi \circ \iota_3$, and ψ is clearly unique with this property, so G is indeed a coproduct. □

Exercise 4.1

Check that the function π_m^n defined in §4.1 is well-defined and makes the diagram commute. Verify that it is a group homomorphism.

Solution. Recall that $\pi_m^n\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is defined by $\pi_m^n([a]_n) = [a]_m$, assuming that $m \mid n$. To show that this is well-defined, let $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{n}$. This means that $n \mid a - b$, and hence that $m \mid a - b$, i.e. that $a \equiv b \pmod{m}$. In other words, $[a]_n = [b]_n$ implies that $[a]_m = [b]_m$, and thus π_m^n is well-defined. It is also obvious that the diagram

$$\begin{array}{ccc} \mathbb{Z} & & \\ {\scriptstyle \pi_n}\downarrow & \searrow^{\pi_m} & \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\pi_m^n]{} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

commutes, since $\pi_n(a) = [a]_n$ and $\pi_m(a) = [a]_m$.

Finally we show that π_m^n is a homomorphism. For $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} \pi_m^n([a]_n + [b]_n) = \pi_m^n([a+b]_n) = [a+b]_m = [a]_m + [b]_m \\ = \pi_m^n([a]_n) + \pi_m^n([b]_n) \end{aligned}$$

as desired. □

Exercise 4.4

Prove that no two of the groups $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are isomorphic to one another. Can you decide whether $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *are* isomorphic to one another?

Solution. Firstly, $\mathbb{R}$ is uncountable so cannot be isomorphic to $\mathbb{Z}$ or $\mathbb{Q}$. Secondly, $\mathbb{Z}$ is cyclic but $\mathbb{Q}$ is not: This follows since if $p \in \mathbb{Q}^*$, then $p/2 \notin \langle p \rangle$, and hence p is not a generator of $\mathbb{Q}$.

Next we claim that $\mathbb{R}$ and $\mathbb{C}$ are indeed isomorphic. Both $\mathbb{R}$ and $\mathbb{C} \cong \mathbb{R}^2$ are $\mathbb{Q}$-vector spaces, so let $\mathcal{B}$ be a Hamel basis of $\mathbb{R}$ (using the axiom of choice, not sure if the claim holds without it). Then

$$\mathcal{C} = \{(b, 0) \mid b \in \mathcal{B}\} \cup \{(0, b) \mid b \in \mathcal{B}\}$$

is a Hamel basis of $\mathbb{C}$. Again using the axiom of choice we have $|\mathcal{B}| = |\mathcal{B} \times \mathcal{B}|$, and since $|\mathcal{B}| \leq |\mathcal{C}| \leq |\mathcal{B} \times \mathcal{B}|$, $\mathbb{R}$ and $\mathbb{C}$ are equidimensional as $\mathbb{Q}$-vector spaces. They are thus isomorphic as vector spaces, and hence as abelian groups. □

Exercise 4.8

Let G be a group, and let $g \in G$. Prove that the function $\gamma_g \colon G \to G$ defined by $\gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms γ_g are called 'inner' automorphisms of G.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian.

Solution. For $a, b \in G$ we have

$$\gamma_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \gamma_g(a)\gamma_g(b),$$

so γ_g is a homomorphism. It is obviously invertible with $\gamma_g^{-1} = \gamma_{g^{-1}}$, hence an isomorphism.

Now let also $h \in G$. Then

$$(\gamma_{gh})(a) = (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = \gamma_g(hah^{-1}) = (\gamma_g \circ \gamma_h)(a),$$

so $g \mapsto \gamma_g$ is a homomorphism. □

Exercise 4.9

Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$.

Solution. The map $\pi = (\pi_m^{mn}, \pi_n^{mn})$ is a group homomorphism, and since the sets C_{mn} and $C_m \times C_n$ have the same cardinality, it suffices to show that π is injective. Using additive notation, if $\pi([a]_{mn}) = \pi([b]_{mn})$ then $[a]_m = [b]_m$, i.e. $m \mid a - b$. Similarly $n \mid a - b$, and since $\gcd(m, n) = 1$ we have $mn \mid a - b$. It follows that $[a]_{mn} = [b]_{mn}$ as desired. □

II.5. Free groups

Exercise 5.3

Use the universal property of free groups to prove that the map $j \colon A \to F(A)$ is injective, for all sets A.

Solution. This is obvious for sets with less than two elements, so assume that there are elements $a, b \in A$ with $a \neq b$. Define a set function $f \colon A \to \mathbb{Z}$ by letting $f(a) = 1$ and $f(x) = 0$ for $x \neq a$. By the universal property there exists a group homomorphism $\varphi \colon F(A) \to \mathbb{Z}$ such that $f = \varphi \circ j$. Then

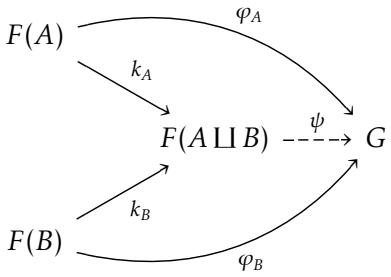
$$\varphi(j(a)) = f(a) \neq f(b) = \varphi(j(b)),$$

so we must have $j(a) \neq j(b)$, and thus j is injective. □

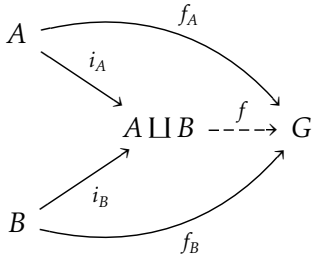
EXERCISE 5.8

Prove that $F(A \amalg B) = F(A) * F(B)$ for all sets A, B.

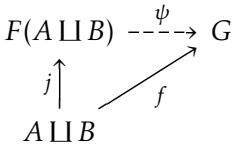
SOLUTION. Given homomorphisms $\varphi_A \colon F(A) \to G$ and $\varphi_B \colon F(B) \to G$ into a group G, we must prove the existence and uniqueness of a homomorphism $\psi \colon F(A \amalg B) \to G$ such that the diagram



commutes, for suitable definitions of k_A and k_B. Denoting the injection from A into $F(A)$ by j_A, we let $f_A = \varphi_A \circ j_A$, and we define f_B analogously. The universal property for coproducts in **Set** yields a unique set function $f \colon A \amalg B \to G$ making the diagram



commute. The universal property for free groups then yields a unique homomorphism $\psi \colon F(A \amalg B) \to G$ such that



commutes. Choose k_A to be the unique homomorphism such that $k_A \circ j_A = j \circ i_A$. Then we have

$$\varphi_A \circ j_A = f_A = f \circ i_A = \psi \circ j \circ i_A = \psi \circ k_A \circ j_A,$$

and since j_A is injective by Exercise 5.3 it follows that $\psi_A = \psi \circ k_A$ as desired.

It remains to be shown that ψ is unique with this property. But any such homomorphism making the first diagram commutes would induce arrows such that the other diagrams also commute, hence induce the same unique arrow ψ in the final diagram. Hence ψ is unique which proves the claim. □

EXERCISE 5.10

Let $F = F^{ab}(A)$.

(a) Define an equivalence relation $\sim$ on F by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$. Prove that $F/\!\sim$ is a finite set if and only if A is finite, and in that case $|F/\!\sim| = 2^{|A|}$.

(b) Assume $F^{ab}(B) \cong F^{ab}(A)$. If A is finite, prove that B is also, and that $A \cong B$ as sets.

SOLUTION. (a) Writing $f = \sum_{a\in A} m_a j(a)$ and $f' = \sum_{a\in A} m'_a j(a)$ in the notation of §5.4, we find that

$$2g = f - f' = \sum_{a\in A} (m_a - m'_a) j(a)$$

for some $g \in F$ if and only if $m_a \equiv m'_a \pmod 2$ for all $a \in A$. That is, the $\sim$-equivalence classes are determined by a choice of sign for each coefficient m_a. If A is finite there are finitely many such choices, namely $2^{|A|}$. Conversely, it is clear that there are at least as many choices as elements in A, so $|F/\!\sim| \geq |A|$. Thus $F/\!\sim$ is finite if and only if A is.

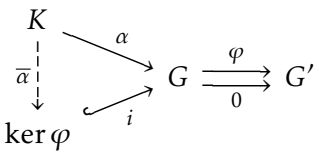
(b) Let $\varphi\colon F^{ab}(A) \to F^{ab}(B)$ be an isomorphism. Let $\sim_A$ and $\sim_B$ denote the above equivalence relations on $F^{ab}(A)$ and $F^{ab}(B)$ respectively, and notice that $f \sim_A f'$ if and only if $\varphi(f) \sim_B \varphi(f')$. Thus the number of $\sim_A$- and $\sim_B$-equivalence classes agree, so (a) implies that A is finite if and only if B is finite. In this case we have

$$2^{|A|} = |F^{ab}(A)/\!\sim_A| = |F^{ab}(B)/\!\sim_B| = 2^{|B|}.$$

It follows that $|A| = |B|$, and thus that $A \cong B$ as sets. □

II.6. Subgroups

REMARK II.1. We restate Proposition 6.6 in more explicitly categorical language: Let $\varphi\colon G \to G'$ be a homomorphism. The inclusion $i\colon \ker\varphi \to G$ is an equaliser of φ and the trivial map $0\colon G \to G'$. In other words, for any group homomorphism $\alpha\colon K \to G$ such that $\varphi \circ \alpha = 0 \circ \alpha$ there is a unique homomorphism $\overline{\alpha}\colon K \to \ker\varphi$ such that the following diagram commutes:



For $k \in K$ we must have $(\varphi \circ \alpha)(k) = e_{G'}$, so $\alpha(k) \in \ker \varphi$. The unique choice of $\overline{\alpha}$ is then just α with codomain restricted to $\ker \varphi$. ⌟

Exercise 6.4

Let G be a group, and let $g \in G$. Verify that the image of the exponential map $\varepsilon_g \colon \mathbb{Z} \to G$ is a cyclic group (in the sense of Definition 4.7).

Solution. If ε_g is injective, then $\mathbb{Z} \cong \varepsilon_g(\mathbb{Z})$. Otherwise $\ker \varepsilon_g$ is nontrivial, so let n be the least positive number in $\ker \varepsilon_g$, and consider the map $\varphi \colon \mathbb{Z}/n\mathbb{Z} \to \varepsilon_g(\mathbb{Z})$ given by $\varphi([a]_n) = g^a$. This is easily seen to be well-defined, bijective and a group homomorphism, hence an isomorphism.

Alternatively, the first isomorphism theorem implies that $\mathbb{Z}/\ker \varepsilon_g \cong \varepsilon_g(\mathbb{Z})$, and $\ker \varepsilon_g = n\mathbb{Z}$ for some $n \in \mathbb{N}$. □

Exercise 6.6

Prove that the union of a family of subgroups of a group G is not necessarily a subgroup of G. In fact:

(a) Let H, H' be subgroups of a group G. Prove that $H \cup H'$ is a subgroup of G only if $H \subseteq H'$ or $H' \subseteq H$.

(b) On the other hand, let $H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots$ be subgroups of a group G. Prove that $\bigcup_{i \geq 0} H_i$ *is* a subgroup of G.

Solution. (a) Assume that $H \cup H'$ is a subgroup of G and let $h \in H$ and $h' \in H'$. Then $hh' \in H \cup H'$, say $hh' \in H$. But then $h' = h^{-1}(hh') \in H$, so $h' \in H$ and hence $H' \subseteq H$. Similarly if $hh' \in H'$.

(b) Write $H = \bigcup_{i \geq 0} H_i$. If $g, h \in H$, then $g \in H_i$ and $h \in H_j$ for some $i, j \in \mathbb{N}$.[2] Hence $g, h \in H_i \cup H_j = H_{i \vee j} \subseteq H$. We furthermore have $g^{-1} \in H_i \subseteq H$. □

Exercise 6.7

Show that *inner* automorphisms (cf. Exercise 4.8) form a subgroup of $\mathrm{Aut}(G)$; this subgroup is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G)$ is trivial if and only if G is abelian. Deduce that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

[2] The natural numbers include zero.

SOLUTION. It is clear that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Assume that $\mathrm{Inn}(G)$ is cyclic, and let $a \in G$ be such that γ_a generates $\mathrm{Inn}(G)$. For $g \in G$ we then have $\gamma_g = \gamma_a^n = \gamma_{a^n}$ for some $n \in \mathbb{Z}$. Hence

$$gag^{-1} = \gamma_g(a) = \gamma_{a^n}(a) = a^n a a^{-n} = a,$$

so a commutes with every $g \in G$. For $b \in G$ we thus have

$$\gamma_g(b) = \gamma_{a^n}(b) = a^n b a^{-n} = b,$$

so γ_g is the identity map for every $g \in G$. Therefore $\mathrm{Inn}(G)$ is trivial, which is obviously equivalent to G being abelian.

Finally, if $\mathrm{Aut}(G)$ is cyclic then Propositions 6.9 and 6.11 imply that $\mathrm{Inn}(G)$ is also cyclic. But then G is abelian. □

EXERCISE 6.8

Prove that an *abelian* group G is finitely generated if and only if there is a surjective homomorphism

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}} \twoheadrightarrow G$$

for some n.

SOLUTION. First notice the general fact that if $\varphi\colon G \to H$ is any group homomorphism and $A \subseteq G$, then $\varphi(\langle A\rangle) = \langle \varphi(A)\rangle$: The inequality $\supseteq$ is obvious, so let $h \in \varphi(\langle A\rangle)$. Then $h = \varphi(g)$ for some $g \in \langle A\rangle$, and g is on the form $g_1 \cdots g_n$ for $g_i \in A$. Hence $h = \varphi(g_1)\cdots\varphi(g_1) \in \langle \varphi(A)\rangle$ as claimed.

If $\varphi\colon \mathbb{Z}^{\oplus n} \to G$ is surjective, then since $\mathbb{Z}^{\oplus n} = \langle A\rangle$ with $A = \{1,\dots,n\}$ we have $G = \langle \varphi(1),\dots,\varphi(n)\rangle$. Conversely, if G is generated by a finite set $\{g_1,\dots,g_n\}$, then we construct a homomorphism $\varphi\colon \mathbb{Z}^{\oplus n} \to G$ as follows: Define a set function $f : A \to G$ by $f(i) = g_i$. Since $\mathbb{Z}^{\oplus n} = F^{ab}(A)$, f induces a homomorphism $\varphi\colon \mathbb{Z}^{\oplus n} \to G$. But the image of φ is a subgroup containing $g_1,\dots,g_n$, hence contains $\langle g_1,\dots,g_n\rangle = G$. Thus φ is surjective. □

EXERCISE 6.9

Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic. Prove that $\mathbb{Q}$ is not finitely generated.

SOLUTION. Let

$$G = \left\langle \frac{p_1}{q_1},\dots,\frac{p_n}{q_n} \right\rangle$$

be a finitely generated subgroup of $\mathbb{Q}$, and let $m = \operatorname{lcm}(q_1, \ldots, q_n)$. Then each p_i/q_i is an integer multiple of $1/m$, and so $G \subseteq \langle 1/m \rangle$. But every subgroup of a cyclic group is cyclic, so G is cyclic.

Since $\mathbb{Q}$ is not cyclic (cf. Exercise 4.4), it is not finitely generated. □

EXERCISE 6.16

The homomorphism $\varphi\colon \mathbb{Z}/3\mathbb{Z} \to S_3$ given by

$$\varphi([0]) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varphi([1]) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \varphi([2]) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

is a monomorphism; show that it has *no* left-inverse in **Grp**.

SOLUTION. Assume towards a contradiction that φ has a left-inverse ψ. Since ψ is neither injective nor trivial, the kernel of ψ must be a proper nontrivial subgroup of S_3. It is also normal, and the only such subgroup is A_3. But A_3 is precisely the image of φ, so ψ cannot be its left-inverse. □

II.7. Quotient groups

REMARK II.2. We elaborate on the condition $H \subseteq \ker\varphi$ in the statement of Theorem 7.12.

If $f\colon X \to Y$ is a set function, then we define the *kernel* of f, written $\ker f$, as the equivalence relation on X given by $x' \sim_f x$ if and only if $f(x) = f(x')$. In **Set** we cannot say much more about this relation, but in **Grp** we recover the usual notion of kernel as follows: If $\varphi\colon G \to G'$ is a group homomorphism and $a, b \in G$, then $a \sim_\varphi b$ if and only if $\varphi(a) = \varphi(b)$. But since φ is a homomorphism, this is equivalent to $\varphi(a^{-1}b) = e_{G'}$, i.e. $a^{-1}b \in \ker\varphi$ in the group-theoretic sense. Thus the equivalence relation generated by the subgroup $\ker\varphi$ is precisely the relation $\ker\varphi$, and in particular the notation $G/\ker\varphi$ for the quotient group is unambiguous.

Given a subgroup H of G we define a left-invariant equivalence relation on G by $a \sim_H b$ if and only if $a^{-1}b \in H$.[3] In this notation we thus have $\sim_\varphi = \sim_{\ker\varphi}$. If K is another subgroup of G, then we claim that $H \subseteq K$ if and only if $\sim_H \subseteq \sim_K$. Assuming that $H \subseteq K$ and $a \sim_H b$ we have $a^{-1}b \in H \subseteq K$, so also $a \sim_K b$. Conversely, if $\sim_H \subseteq \sim_K$ and $g \in H$, then also $e^{-1}g \in H$ so $g \sim_H e$. It follows that $g \sim_K e$, so $g = e^{-1}g \in K$.

We can now understand the condition $H \subseteq \ker\varphi$. This says that $\sim_H \subseteq \sim_{\ker\varphi} = \sim_\varphi$, i.e. that $a \sim_H b$ implies $\varphi(a) = \varphi(b)$. When H is normal, this

[3] We focus on left-invariant relations here, but we could just as well have defined right-invariant relations instead.

is precisely the property that ensures the existence and uniqueness of a homomorphism $\tilde{\varphi}\colon G/{\sim_H} \to G'$ such that $\tilde{\varphi} \circ \pi = \varphi$. ⌟

Exercise 7.10

Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise 6.7, show that H is normal in G if and only if $\gamma(H) \subseteq H$ for all $\gamma \in \mathrm{Inn}(G)$.

Solution. Since H is normal if and only if $gHg^{-1} \subseteq H$ for all $g \in G$, and every inner automorphism is on the form γ_g for some $g \in G$, the claim follows. □

Exercise 7.11

Let G be a group, and let $[G,G]$ be the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$. Prove that $[G,G]$ is normal in G. Prove that $G/[G,G]$ is commutative.

Solution. For $a, b \in G$, write $[a,b] = aba^{-1}b^{-1}$. If $\varphi\colon G \to H$ is any homomorphism into a group H, we have

$$\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = [\varphi(a), \varphi(b)].$$

Thus the homomorphic image of any commutator is itself a commutator, and thus $\varphi([G,G]) \subseteq [H,H]$. It follows from Exercise 7.10 that $[G,G]$ is normal.

To show that $G/[G,G]$ is commutative, let $\pi\colon G \to G/[G,G]$ denote the quotient map and notice that

$$[\pi(a), \pi(b)] = \pi([a,b]) = e$$

for all $a, b \in G$. □

Exercise 7.12

Let $F = F(A)$ be a free group, and let $f : A \to G$ be a set-function from the set A to a *commutative* group G. Prove that f induces a unique homomorphism $F/[F,F] \to G$. Conclude that $F/[F,F] \cong F^{ab}(A)$.

Solution. First f induces a unique homomorphism $\varphi\colon F \to G$. Next notice that if $a, b \in F$, then $\varphi([a,b]) = [\varphi(a), \varphi(b)] = e_G$ since G is commutative, so $[F,F] \subseteq \ker\varphi$. Hence Theorem 7.12 induces a unique homomorphism $\tilde{\varphi}\colon F/[F,F] \to G$. Thus $\tilde{\varphi}$ makes the diagram

$$\begin{array}{ccc} F/[F,F] & \xrightarrow{\tilde{\varphi}} & G \\ {\scriptstyle j'}\uparrow & \nearrow_{f} & \\ A & & \end{array}$$

commute. If $\psi\colon F/[F,F] \to G$ is any such homomorphism and $\pi\colon F \to F/[F,F]$ is the quotient map, the diagram

$$\begin{array}{ccc} F & \xrightarrow{\psi\circ\pi} & G \\ {\scriptstyle j}\uparrow & \nearrow_{f} & \\ A & & \end{array}$$

also commutes. But then $\psi \circ \pi = \varphi$, and so $\psi = \tilde{\varphi}$. Thus $F/[F,F]$ satisfies the universal property of $F^{ab}(A)$, and these are thus isomorphic. □

EXERCISE 7.13

Let A, B be sets and $F(A), F(B)$ the corresponding free groups. Assume $F(A) \cong F(B)$. If A is finite, prove that B is also and $A \cong B$.

SOLUTION. First notice that $[F(A),F(A)]$ and $[F(B),F(B)]$ are isomorphic, since homomorphisms send commutators to commutators, so $F(A)/[F(A),F(A)]$ and $F(B)/[F(B),F(B)]$ are also isomorphic. Thus Exercise 7.12 implies that $F^{ab}(A) \cong F^{ab}(B)$. By Exercise 5.10 we then have $A \cong B$ as desired. □

II.8. Canonical decomposition and Lagrange's theorem

REMARK II.3. Given a normal subgroup H of a group G, Proposition 8.9 gives a bijection u from subgroups $K \leq G$ that contain H to subgroups K/H of G/H. If $\pi\colon G \to G/H$ is the quotient map, then $u(K) = \pi(K)$, and Aluffi shows that this has inverse $v(K') = \pi^{-1}(K')$ for $K' \leq G/H$.

We give a slightly different proof of this fact, based on the following concept: Given a set function $f\colon X \to Y$, a subset $A \subseteq X$ is said to be *saturated with respect to* f if $A = f^{-1}(B)$ for some $B \subseteq Y$. The following are then equivalent:[4]

(a) A is saturated.

(b) $A = f^{-1}(f(A))$.

(c) A is a union of fibres.

(d) If $x \in A$, then $f(x) = f(x')$ implies that $x' \in A$, for all $x' \in X$.

We first prove this claim.

[4] This is Exercise 3.59 in Lee's *Introduction to Topological Manifolds*. We shall only need the equivalence of (b) and (c) but include the rest for the sake of exposition.

(a) ⇔ (b): Let $A = f^{-1}(B)$. Then $f(A) \subseteq B$, so $f^{-1}(f(A)) \subseteq f^{-1}(B) = A$, and the opposite inclusion always holds. The opposite implication is obvious.

(a) ⇔ (c): Simply notice that

$$f^{-1}(B) = f^{-1}\left(\bigcup_{y\in B}\{y\}\right) = \bigcup_{y\in B} f^{-1}(y)$$

for any $B \subseteq Y$, so A is on the form $f^{-1}(B)$ if and only if it is a union of fibres.

(c) ⇔ (d): If $f(x) = f(x')$ then x and x' lie in the same fibre, and this fibre is either contained entirely in A or is disjoint from A. Conversely, if $x \in A$ then $f^{-1}(x) \subseteq A$, since $f(x) = f(x')$ for all x' in this preimage.

The application of this concept to the proposition in question is as follows: Given any quotient map $q\colon X \to X/\!\sim$ in **Set** (so in particular in **Grp**), any equivalence class $[x]$, considered as a subset of X, is equal to the fibre $q^{-1}([x])$.

Now we can easily prove that u and v are each other's inverses: Firstly,

$$(u \circ v)(K') = \pi(\pi^{-1}(K')) = K'$$

for subgroups K' of G/H since π is surjective. Secondly, if K is a subgroup of G containing H, then it is a union of all cosets aH for $a \in K$. But these cosets are equivalence classes, so K is a union of fibres. The above then shows that

$$(v \circ u)(K) = \pi^{-1}(\pi(K)) = K$$

as desired. ⌟

Remark II.4. Given a group G and subgroups H and K with H normal, Proposition 8.11 ensures that HK is a subgroup of G, H is normal in HK, and $H \cap K$ is a normal subgroup of K. A part of the lattice of subgroups of G is seen in Figure 1.

In this lattice we see that $HK = H \vee K$ and $H \cap K = H \wedge K$. The latter is obvious, and the former follows since every subgroup containing H and K must contain all elements on the form hk for $h \in H$ and $k \in K$. Recall that for positive integers a, b we have

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

and that $\operatorname{lcm}(a,b) = a \vee b$ and $\gcd(a,b) = a \wedge b$ in the lattice $\mathbb{N}$ ordered by divisibility. Thus we might expect that, in the lattice of subgroups of G, we would have

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

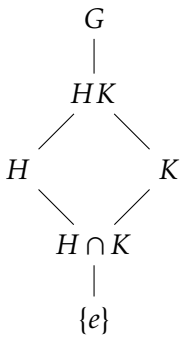


Figure 1: Partial lattice of subgroups of G.

But this is precisely the content of the second isomorphism theorem.

However, while a and b appear symmetrically, H and K do not, since only H is assumed normal. But notice that in **Ab** they do. Also notice that, since H is normal,

$$HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH.$$

In fact, this evidently holds whenever K is *any* subset of G. ⌟

Exercise 8.1

If a group H may be realised as a subgroup of two groups G_1 and G_2, and if

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follow that $G_1 \cong G_2$?

Solution. It does not. Notice that

$$\frac{C_4}{C_2} \cong C_2 \cong \frac{C_2 \times C_2}{C_2},$$

but that $C_4 \ncong C_2 \times C_2$. □

Exercise 8.3

Prove that every finite group is finitely presented.

Solution. Let G be a finite group and consider the free group $F(G)$ on the underlying set of G. If $n = |G|$ we denote the n distinct elements of G by $g_1, \dots, g_n$. For $1 \le i, j \le n$ we let $g_{ij} = g_i g_j$. Let $\mathcal{R}$ be the set of words in $F(G)$ on the form $g_i g_j g_{ij}^{-1}$, and let R be the normal subgroup of $F(G)$ generated by $\mathcal{R}$.

By the univeral property of free groups, the identity map $\iota\colon G \to G$ from the set G to the group G induces a surjective homomorphism $\rho\colon F(G) \to G$. We claim that $\ker\rho = R$. We clearly have $R \subseteq \ker\rho$, so let $h_1 \cdots h_k \in \ker\rho$. By repeatedly applying the relations in $\mathcal{R}$ we may reduce the length of this word and obtain a word $h \in \ker\rho$ of length one. But then h is an element of the underlying set of G, and $h = \iota(h) = \rho(h) = e_G$. This lies in R, and applying the above sequence of relations from $\mathcal{R}$ in reverse order we recover the word $h_1 \cdots h_k$, staying inside of R. Thus $\ker\rho \subseteq R$.

Finally, the first isomorphism theorem implies that $F(G)/R \cong G$, and both G and $\mathcal{R}$ are finite, so this proves the claim. □

EXERCISE 8.8

Prove that $\mathrm{SL}_n(\mathbb{R})$ is a *normal subgroup* of $\mathrm{GL}_n(\mathbb{R})$ and 'compute'

$$\frac{\mathrm{GL}_n(\mathbb{R})}{\mathrm{SL}_n(\mathbb{R})}$$

as a well-known group.

SOLUTION. Consider the determinant

$$\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*.$$

This is a surjective homomorphism with kernel $\mathrm{SL}_n(\mathbb{R})$, and the first isomorphism theorem implies that $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$. □

EXERCISE 8.13

Let G be a finite commutative group, and assume $|G|$ is odd. Prove that every element of G is a square.

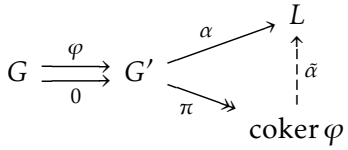
Exercise 8.14 is solved by the same argument.

SOLUTION. We show that the map $g \mapsto g^2$ is surjective, and since G is finite it suffices to show that it is injective. For $g, h \in G$ with $g^2 = h^2$ we have $(g^{-1}h)^2 = e$. But the order of $g^{-1}h$ cannot be even since $|G|$ is odd, so $g^{-1}h = e$, i.e. $g = h$. □

EXERCISE 8.22

Let $\varphi\colon G \to G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\operatorname{im}\varphi$. Prove that G'/N satisfies the universal property of $\operatorname{coker}\varphi$ in **Grp**.

SOLUTION. First we rephrase the universal property of $\operatorname{coker}\varphi$. If $0\colon G \to G'$ is the trivial map, $\operatorname{coker}\varphi$ is the coequaliser of φ and 0. That is, given a homomorphism $\alpha\colon G' \to L$ such that $\alpha\circ\varphi = \alpha\circ 0$ there is a unique homomorphism $\tilde{\alpha}\colon \operatorname{coker}\varphi \to L$ such that the diagram



commutes. The condition $\alpha\circ\varphi = \alpha\circ 0$ implies that $\operatorname{im}\varphi \subseteq \ker\alpha$, and since $\ker\alpha$ is normal it follows that $N \subseteq \ker\alpha$. Theorem 7.12 yields a unique homomorphism $\tilde{\alpha}\colon G'/N \to L$ such that $\tilde{\alpha}\circ\pi = \alpha$. Thus $G'/N \cong \operatorname{coker}\varphi$.

Also notice that the above works in **Ab**, only here $\operatorname{im}\varphi = N$. □

EXERCISE 8.23

Consider the subgroup $H = \{e, (1\ 2)\}$ of S_3. Show that the cokernel of the inclusion $\iota\colon H \hookrightarrow S_3$ is trivial, although ι is not surjective

SOLUTION. In accordance with Exercise 8.22 we compute the smallest normal subgroup N of S_3 containing $\operatorname{im}\iota = H$. The only nontrivial proper normal subgroup of S_3 is A_3, but $(1\ 2) \notin A_3$. Hence $N = S_3$, so $\operatorname{coker}\iota \cong S_3/N$ is trivial. □

EXERCISE 8.24

Show that epimorphisms in **Grp** do not necessarily have right-inverses.

SOLUTION. Consider the homomorphism $\pi_2\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ given by $\pi_2(n) = [n]_2$. This is surjective hence an epimorphism, but the only homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ is the trivial one. □

II.9. Group actions

REMARK II.5. We elaborate on the orbit-stabiliser theorem (Proposition 9.9). Let G be a group with a transitive left-action on a set A, and fix an element $a \in A$. We define an equivalence relation on G by letting $g_1 \sim g_2$ if and only if $g_1 a = g_2 a$. This is the case just when $g_1^{-1} g_2 a = a$, i.e. when $g_1^{-1} g_2 \in \operatorname{Stab}_G(a)$. Since $e_g \in \operatorname{Stab}_G(a)$ we see that $\sim$ agrees with the equivalence relation induced by $\operatorname{Stab}_G(a)$ as a subgroup of G.

Next notice that the map $\varphi\colon G \to A$ given by $\varphi(g) = ga$ has the property that $\varphi(g_1) = \varphi(g_2)$ if and only if $g_1 \sim g_2$. Furthermore, since G acts transitively on A, φ is also surjective. Thus φ induces a bijection $\tilde{\varphi}\colon G/\!\sim \to A$.

Letting $H = \mathrm{Stab}_G(a)$, since we have $G/\!\sim = G/H$ we let G act on G/H by left-multiplication. We easily see that $\tilde{\varphi}$ is equivariant:

$$\varphi(g'(gH)) = \varphi(g'gH) = (g'g)a = g'(ga) = g'\varphi(gH)$$

for $g, g' \in G$.

We can understand the theorem more informally as follows: Fixing an element of $a \in A$ introduces a sort of 'origin' in A. Since A is just a set, the choice of origin is arbitrary. Next we group the elements of G based on where they send a when acting on A. It turns out that two elements send a to the same point if and only if they lie in the same $\mathrm{Stab}_G(a)$-coset. But this makes sense, since quotienting out by $\mathrm{Stab}_G(a)$ means that we force every element in G that fixes a to 'do nothing'. So if $g_1H = g_2H$ with $H = \mathrm{Stab}_G(a)$, then this means that g_1 and g_2 are the same up to 'doing nothing'.

Finally, the equivariance of $\tilde{\varphi}$: Left-multiplication in G/H is basically just composition of transformations, since $g'(gH) = (g'g)H = (g'H)(gH)$. And because composition of functions in general is defined pointwise, it makes sense that the same should be true in this case. ⌟

Exercise 9.7

Prove that stabilisers are indeed subgroups.

Solution. Let G be a group acting on a set A, and let $a \in A$. Clearly $e_G \in \mathrm{Stab}_G(a)$, and if $g, h \in \mathrm{Stab}_G(a)$ then also $gh \in \mathrm{Stab}_G(a)$. Finally we also have

$$g^{-1}a = g^{-1}(ga) = (g^{-1}g)a = a,$$

so $g^{-1} \in \mathrm{Stab}_G(a)$. □

Exercise 9.8

For G a group, verify that G-**Set** is indeed a category, and verify that the isomorphisms in G-**Set** are precisely the equivariant bijections.

Solution. Let $\varphi\colon (\rho, A) \to (\sigma, B)$ and $\psi\colon (\sigma, B) \to (\tau, C)$ be equivariant maps. For $g \in G$ and $a \in A$ we have

$$(\psi \circ \varphi)(ga) = \psi(\varphi(ga)) = \psi(g\varphi(a)) = g(\psi \circ \varphi)(a),$$

so $\psi \circ \varphi$ is also equivariant. The identity map on a set is clearly also equivariant, so G-**Set** is indeed a category.

Now assume that the set function φ is bijective and consider its inverse φ^{-1}. Let $b \in B$ and put $a = \varphi^{-1}(b)$. Since $\varphi(ga) = g\varphi(a)$, applying φ^{-1} to both sides yields

$$g\varphi^{-1}(b) = ga = \varphi^{-1}(g\varphi(a)) = \varphi^{-1}(gb),$$

so φ^{-1} is equivariant. It is already the inverse of φ in **Set**, so it is also the inverse of φ in G-**Set**. □

EXERCISE 9.9

Prove that G-**Set** has products and coproducts and that every finite object of G-**Set** is a coproduct of objects of the type G/H, where H is a subgroup of G and G acts on G/H by left-multiplication.

SOLUTION. *Products*: Let A and A' be sets, and let $\sigma\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A)$ and $\sigma'\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A')$ be actions of G on A and A'. These induce a homomorphism

$$\langle\sigma,\sigma'\rangle\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A)\times\mathrm{Aut}_{\mathbf{Set}}(A') \subseteq \mathrm{Aut}_{\mathbf{Set}}(A\times A').$$

The inclusion is understood as follows: A pair of maps $\varphi \in \mathrm{Aut}_{\mathbf{Set}}(A)$ and $\varphi' \in \mathrm{Aut}_{\mathbf{Set}}(A')$ determine a map $\varphi\times\varphi' \in \mathrm{Aut}_{\mathbf{Set}}(A\times A')$ given by

$$(\varphi\times\varphi')(a,a') = (\varphi(a),\varphi'(a')).$$

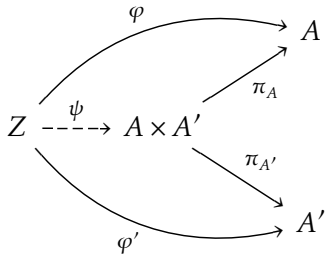
This is clearly also an automorphism. Thus $\langle\sigma,\sigma'\rangle$ is an action of G on $A\times A'$. For $g \in G$ we thus have $\langle\sigma,\sigma'\rangle(g) = \sigma(g)\times\sigma'(g)$, so $a \in A$ and $a' \in A'$ this is given explicitly by

$$\langle\sigma,\sigma'\rangle(g)(a,a') = \Big(\sigma(g)(a),\sigma'(g)(a')\Big),$$

or more simply by

$$g(a,a') = (ga,ga').$$

Let Z be another object in G-**Set**, and let $\varphi\colon Z \to A$ and $\varphi'\colon Z \to A'$ be equivariant maps. There is then a unique set map $\psi\colon Z \to A\times A'$ such that the diagram



commutes. It thus suffices to show that ψ, π_A and $\pi_{A'}$ are equivariant. For π_A we have

$$\pi_A(g(a,a')) = \pi_A(ga,ga') = ga = g\pi_A(a,a'),$$

and for ψ,

$$\psi(gz) = (\varphi(gz),\varphi'(gz)) = (g\varphi(z),g\varphi'(z)) = g(\varphi(z),\varphi'(z)) = g\psi(z).$$

Thus $A\times A'$ equipped with the action $\langle\sigma,\sigma'\rangle$ is a product of A and A' in G-**Set** as claimed.

Coproducts: For $g \in G$ we have automorphisms $\sigma(g)\colon A \to A$ and $\sigma'(g)\colon A' \to A'$. These induce an automorphism

$$\sigma(g) \oplus \sigma'(g)\colon A \amalg A' \to A \amalg A'$$

given by $a \mapsto \sigma(g)(a)$ if $a \in A$, and $a \mapsto \sigma'(g)(a)$ if $a \in A'$. This in turn gives rise to a map $\sigma \oplus \sigma'\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A \amalg A')$ given by $(\sigma \oplus \sigma')(g) = \sigma(g) \oplus \sigma'(g)$, and we claim that this is an action of G on $A \amalg A'$. Let $g, h \in G$, and assume that $a \in A$. Then

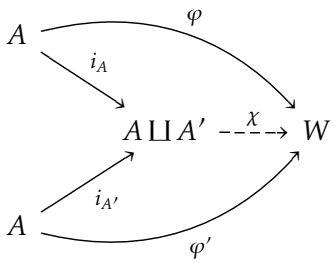
$$\begin{aligned}(\sigma \oplus \sigma')(gh)(a) &= \Big(\sigma(gh) \oplus \sigma'(gh)\Big)(a) = \sigma(gh)(a) = \sigma(g) \circ \sigma(h)(a) \\ &= \Big(\sigma(g) \oplus \sigma'(g)\Big) \circ \Big(\sigma(h) \oplus \sigma'(h)\Big)(a) \\ &= (\sigma \oplus \sigma')(g) \circ (\sigma \oplus \sigma')(h)(a),\end{aligned}$$

and similarly if $a \in A'$. Thus

$$(\sigma \oplus \sigma')(gh) = (\sigma \oplus \sigma')(g) \circ (\sigma \oplus \sigma')(h),$$

so $\sigma \oplus \sigma'$ is a group homomorphism, hence an action of G on $A \amalg A'$.

Now let W be another object in G-**Set**, and let $\varphi\colon A \to W$ and $\varphi'\colon A' \to W$ be equivariant maps. There is then a unique set map $\chi\colon A \amalg A' \to W$ such that the diagram



commutes. It thus suffices to show that χ, i_A and $i_{A'}$ are equivariant. For i_A we simply have $i_A(ga) = ga = g i_A(a)$ for $a \in A$. For χ we have

$$\chi(ga) = \varphi(ga) = g\varphi(a) = g\chi(a)$$

if $a \in A$, and similarly if $a \in A'$.

Finite objects: Let A be a finite set equipped with an action σ, and let Ω be the set of distinct orbits of elements in A under σ, and let σ_ω denote the restriction of σ to $\omega \in \Omega$. Since A is finite so is Ω, and it is obvious that

$$\bigoplus_{\omega \in \Omega} \sigma_\omega = \sigma.$$

Furthermore, every σ_ω is transitive, so Proposition 9.9 yields isomorphisms $\omega \cong G/H_\omega$ in G-**Set**, where H_ω is the stabiliser of some element of ω. It follows that

$$A \cong \coprod_{\omega\in\Omega} \omega \cong \coprod_{\omega\in\Omega} G/H_\omega.$$

This proves the claim. □

III • Rings and modules

III.1. Definition of ring

EXERCISE 1.5

Let R be a ring. If a, b are zero-divisors in R, is $a+b$ necessarily a zero-divisor?

SOLUTION. We give a counterexample. Let

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

in the matrix ring $\mathcal{M}_n(\mathbb{R})$. Then $ab = ba = 0$, so both a and b are zero-divisors, but $a+b$ is the identity matrix.

However, if R is commutative, then $a+b$ is in fact a zero-divisor: For if $ac = 0$ and $bd = 0$ for some $c, d \in R$, then

$$(a+b)cd = acd + bdc = 0 \cdot d + 0 \cdot c = 0.$$ □

EXERCISE 1.6

An element a of a ring R is *nilpotent* if $a^n = 0$ for some n.

(a) Prove that if a and b are nilpotent in R and $ab = ba$, then $a+b$ is also nilpotent.

(b) Is the hypothesis $ab = ba$ in the previous statement necessary for its conclusion to hold?

SOLUTION. (a) Since $ab = ba$, the binomial theorem implies that

$$(a+b)^N = \sum_{i=0}^{N} \binom{N}{i} a^i b^{N-i}.$$

Choose $m, n \in \mathbb{N}$ such that $a^m = 0$ and $b^n = 0$, and let $N = m+n$. Then if $i < m$ we have $N - i \geq n$, so it follows that $(a+b)^N = 0$.

(b) It is necessary. Consider the matrices

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

in $\mathcal{M}_2(\mathbb{R})$. Then $a^2 = b^2 = 0$, but $(a+b)^2$ is the identity matrix, so $a+b$ is not nilpotent. □

III.2. The category **Ring**

REMARK III.1. Let S be a ring and $s \in S$. According to Example 2.2 there exists a unique ring homomorphism $\iota\colon \mathbb{Z}[x] \to S$ that sends x to s. This is guaranteed by the proof of Proposition 2.1 as long as s commutes with every element in $\iota(\mathbb{Z})$. We claim that this is in fact the case:

Clearly s commutes with $\iota(1) = 1_S$, so assume that it commutes with $\iota(n)$ for some $n \in \mathbb{N}$. It follows that

$$s\iota(n+1) = s(\iota(n) + 1_S) = (\iota(n) + 1_S)s = \iota(n+1).$$

The extension to $n \in \mathbb{Z}$ is obvious.

We can also give a more structural argument: Let A be a subset of a ring R, and let $\langle A \rangle$ denote the smallest subring of R that contains A. Explicitly, this is the collection of finite sums of finite products of elements in A or their additive inverses, including the empty sum 0_R and the empty product 1_R.

If $\varphi\colon R \to S$ is a ring homomorphism, then we claim that $\varphi(\langle A \rangle) = \langle \varphi(A) \rangle$. The inclusion $\supseteq$ is obvious, so consider the other inclusion. If $s \in \varphi(\langle A \rangle)$, then $s = \varphi(r)$ for some $r \in \langle A \rangle$. Hence

$$r = \sum_{i=1}^{n} a_{i1} \cdots a_{ik_i},$$

where the a_{ij} are either elements in A or their additive inverses, and n and k_i are positive integers. It follows that

$$s = \varphi(r) = \sum_{i=1}^{n} \varphi(a_{i1}) \cdots \varphi(a_{ik_i}).$$

If $a_{ij} \in A$, then $\varphi(a_{ij}) \in \varphi(A)$. Otherwise $-a_{ij} \in A$ so $\varphi(a_{ij}) = -\varphi(-a_{ij}) \in \langle \varphi(A) \rangle$. In total, $s \in \langle \varphi(A) \rangle$ as claimed.

Now we apply this to the above situation. As mentioned, s commutes with $\iota(1)$. The set of elements of S with which s commute (i.e. the centraliser of s, cf. Exercise 2.10) is a subring containing $\iota(1)$, hence it contains $\langle \iota(1) \rangle = \iota(\langle 1 \rangle) = \iota(\mathbb{Z})$ as desired. ⌟

EXERCISE 2.2

Let R and S be rings, and let $\varphi\colon R \to S$ be a function preserving both operations $+, \cdot$.

(a) Prove that if φ is surjective, then necessarily $\varphi(1_R) = 1_S$.

(b) Prove that if $\varphi \neq 0$ and S is an integral domain, then $\varphi(1_R) = 1_S$.

SOLUTION. (a) Assume that φ is surjective, and choose $r \in R$ such that $\varphi(r) = 1_S$. Then

$$1_S = \varphi(r) = \varphi(1_R r) = \varphi(1_R)\varphi(r) = \varphi(1_R)$$

as desired.

(b) Assume that $\varphi \neq 0$ and that S is an integral domain. First notice that $\varphi(1_R) \neq 0_S$, since otherwise $\varphi = 0$. Also notice that φ is a group homomorphism between the underlying additive groups of R and S, so $\varphi(0_R) = 0_S$. It follows that

$$0_S = \varphi(0_R) = \varphi(1_R^2 - 1_R) = \varphi(1_R)(\varphi(1_R) - 1_S),$$

and since S is an integral domain we obtain $\varphi(1_R) - 1_S = 0$ as claimed. □

EXERCISE 2.6

Verify the 'extension property' of polynomial rings, stated in Example 2.3.

SOLUTION. If $\alpha\colon R \to S$ is a ring homomorphism, and $s \in S$ commutes with $\alpha(r)$ for all $r \in R$, then we must construct a unique ring homomorphism $\overline{\alpha}\colon R[x] \to S$ which extends α and sends x to s.

Similar to the proof of Proposition 2.1, since $\overline{\alpha}$ has to be a homomorphism, we require that

$$\overline{\alpha}\left(\sum_{i\in\mathbb{N}} r_i x^i\right) = \sum_{i\in\mathbb{N}} \alpha(r_i)s^i,$$

where finitely many $r_i \in R$ are nonzero. This clearly preserves addition. As for multiplication:

$$\begin{aligned}\overline{\alpha}\left(\sum_{i\in\mathbb{N}} r_i x^i \sum_{j\in\mathbb{N}} t_j x^j\right) &= \overline{\alpha}\left(\sum_{k\in\mathbb{N}}\sum_{i+j=k} r_i t_j x^{i+j}\right) = \sum_{k\in\mathbb{N}}\sum_{i+j=k} \alpha(r_i)\alpha(t_j)s^{i+j} \\ &= \sum_{k\in\mathbb{N}}\sum_{i+j=k} \alpha(r_i)s^i\alpha(t_j)s^j = \sum_{i\in\mathbb{N}} \alpha(r_i)s^i \sum_{j\in\mathbb{N}} \alpha(t_j)s^j \\ &= \overline{\alpha}\left(\sum_{i\in\mathbb{N}} r_i x^i \sum_{j\in\mathbb{N}} t_j x^j\right).\end{aligned}$$

Thus $\overline{\alpha}$ is a homomorphism, and it is clearly unique with the required properties. □

Exercise 2.8

Prove that every subring of a field is an integral domain.

Solution. Let R be a subring of a field F. We need only show that the only zero-divisor in R is zero. But this is obvious, since if $a, b \in R$ are such that $ab = 0$ in R, then this equality also holds in F, so either $a = 0$ or $b = 0$. □

Exercise 2.9

The *centre* of a ring R consists of the elements a such that $ar = ra$ for all $r \in R$.

(a) Prove that the centre is a subring of R.

(b) Prove that the centre of a division ring is a field.

Solution. (a) Let C denote the centre of R. Clearly $\pm 1_R \in C$. If $a, b \in C$ and $r \in R$, then

$$(a + b)r = ar + br = ra + rb = r(a + b)$$

by the distributive property, and

$$(ab)r = arb = r(ab)$$

by associativity. Thus $a + b \in C$ and $ab \in C$, so is a subring of R.

(b) Let C be the centre of a division ring R. Since the elements of C commute with all elements in R, in particular all elements in C, it follows that C is commutative. It remains to be shown that all nonzero elements of C have an inverse in C, so let $a \in C$. This has an inverse a^{-1} in R, and we claim that $a^{-1} \in C$. For

$$a^{-1}r = a^{-1}r(aa^{-1}) = a^{-1}(ra)a^{-1} = a^{-1}(ar)a^{-1} = (a^{-1}a)ra^{-1} = ra^{-1}.$$ □

Exercise 2.10

The *centraliser* of an element a of a ring R consists of the elements $r \in R$ such that $ar = ra$.

(a) Prove that the centraliser of a is a subring of R, for every $a \in R$.

(b) Prove that the centre of R is the intersection of all its centralisers.

(c) Prove that every centraliser in a division ring is a division ring.

SOLUTION. (a) Denote the centraliser of $a \in R$ by C_a. If $r, s \in C_a$, then

$$(r+s)a = ra + sa = ar + as = a(r+s)$$

and

$$(rs)a = ras = a(rs),$$

so $r+s \in C_a$ and $rs \in C_a$. Thus C_a is a subring of R.

(b) Let C denote the centre of R. Then $r \in C$ if and only if $ar = ra$ for all $a \in R$. But this is the case just when $r \in C_a$ for all $a \in R$. Thus $C = \bigcap_{a \in R} C_a$. (Incidentally, this also shows that C is a subring, since an arbitrary intersection of subrings is a subring.)

(c) Assume that R is a division ring, and let $a \in R$. Given $r \in C_a$ we must show that $r^{-1} \in C_a$. But we have

$$r^{-1}a = r^{-1}a(rr^{-1}) = r^{-1}(ar)r^{-1} = r^{-1}(ra)r^{-1} = (r^{-1}r)ar^{-1} = ar^{-1},$$

which proves the claim. □

III.3. Ideals and quotient rings

EXERCISE 3.2

Let $\varphi\colon R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J)$ is an ideal of R.

SOLUTION. We may of course prove this by verifying directly that $\varphi^{-1}(J)$ satisfies the definition of an ideal. Alternatively, notice that I is the kernel of the composition

$$R \xrightarrow{\varphi} S \xrightarrow{\pi} S/J.$$

□

EXERCISE 3.3

Let $\varphi\colon R \to S$ be a ring homomorphism, and let J be an ideal of R.

(a) Show that $\varphi(J)$ need not be an ideal of S.

(b) Assume that φ is surjective; then prove that $\varphi(J)$ *is* an ideal of S.

(c) Assume that φ is surjective, and let $I = \ker\varphi$; thus we may identify S

with R/I. Let $\overline{J} = \varphi(J)$, an ideal of R/I by the previous point. Prove that

$$\frac{R/I}{\overline{J}} \cong \frac{R}{I+J}.$$

SOLUTION. (a) x

(b) Since J is a subgroup of $(R,+)$, $\varphi(J)$ is also a subgroup of $(S,+)$. If $b \in \varphi(J)$ and $s \in S$, then there exist $a \in J$ and $r \in R$ such that $b = \varphi(a)$ and $s = \varphi(r)$. But then

$$bs = \varphi(a)\varphi(r) = \varphi(ar) \in \varphi(J),$$

since $ar \in J$. We similarly find that $sb \in \varphi(J)$, so $\varphi(J)$ is an ideal.

(c) Notice that $\varphi(I+J) = \varphi(J) = \overline{J}$. Substituting $J \to I+J$ in Proposition 3.11 then yields the claim, since $I+J$ is an ideal containing I. □

EXERCISE 3.8

Prove that a nonzero ring R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R.

In particular, a nonzero commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.

We have added the assumption that R be nonzero since the zero ring is not a field, yet (0) and (1) are its only ideals (indeed they both coincide with the ring itself). Furthermore, Aluffi does not require division rings to be nonzero (cf. Definition 1.13), but he seems to assume this elsewhere so we do so as well.

SOLUTION. Assume that R is a division ring, and let $I \neq (0)$ be a left-ideal of R. If $a \in I$ then also $1 = a^{-1}a \in I$, so $I = R$. Similarly for right-ideals.

Conversely, assume that $\{0\}$ and R are the only left-ideals and right-ideals of R. If $a \in R$ is nonzero, then Ra and aR are left- and right-ideals of R different from $\{0\}$. But then we must have $Ra = aR = R$, so 1 lies in both ideals. Thus there are elements $r_1, r_2 \in R$ such that $r_1 a = 1 = ar_2$, hence a is a unit (and in fact $r_1 = r_2$). □

EXERCISE 3.10

Let $\varphi\colon k \to R$ be a ring homomorphism, where k is a field and R is a nonzero ring. Prove that φ is *injective*.

SOLUTION. Let $a \in k$ be nonzero. Then it is a unit, so $\varphi(a)$ is a unit in R. Since R is nonzero, we must have $\varphi(a) \neq 0_R$. It follows that $a \notin \ker\varphi$, so φ is injective. □

EXERCISE 3.12

Let R be a *commutative* ring. Prove that the set of nilpotent elements of R is an ideal of R. (Cf. Exercise 1.6. This ideal is called the *nilradical* of R.)

SOLUTION. Denote the nilradical of R by N. Exercise 1.6 implies that N is a subgroup, so let $a \in N$ and $r \in R$, and choose $n \in \mathbb{N}$ such that $a^n = 0$. Since a and r commute, it follows that $(ar)^n = a^n r^n = 0$, so $ar \in N$. Thus N is an ideal. □

EXERCISE 3.13

Let R be a commutative ring, and let N be its nilradical (cf. Exercise 3.12). Prove that R/N contains no nonzero nilpotent elements. (Such a ring is said to be *reduced*.)

SOLUTION. Let $a + N \in R/N$ be nilpotent. Then there is an $n \in \mathbb{N}$ such that

$$0 + N = (a + N)^n = a^n + N,$$

from which it follows that $a^n \in N$, i.e. that a^n is nilpotent. But then a is also nilpotent, so $a \in N$. □

EXERCISE 3.14

Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1?

SOLUTION. Let R be an integral domain, and let $f : \mathbb{Z} \to R$ be the unique homomorphism. Notice that $\operatorname{im} f$ is also an integral domain. The canonical decomposition of f implies that $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{im} f$. But $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is either 0 (in which case this ring is just $\mathbb{Z}$) or a prime integer.

The zero ring has characteristic 1, since it is isomorphic to $\mathbb{Z}/1\mathbb{Z}$. □

III.4. Ideals and quotients: Remarks and examples. Prime and maximal ideals

EXERCISE 4.1

Let R be a ring, and let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals in R. We let

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{\alpha \in A} r_\alpha \;\middle|\; r_\alpha \in I_\alpha \text{ and } r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Prove that $\sum_{\alpha \in A} I_\alpha$ is an ideal of R and that it is the smallest ideal containing

all of the ideals I_α.

SOLUTION. It is clearly an ideal. Let J be an ideal containing all I_α, and let $\sum_{\alpha\in A} r_\alpha$ be an element of $\sum_{\alpha\in A} I_\alpha$. Then $r_\alpha \in I_\alpha \subseteq J$ for all α, and since J is a subgroup of R we have $\sum_{\alpha\in A} r_\alpha \in J$. This proves the claim. □

EXERCISE 4.2

Prove that the homomorphic image of a Noetherian ring is Noetherian.

SOLUTION. We begin with a lemma: If R is a ring and $A \subseteq R$, then we denote by (A) the ideal generated by A, i.e. the intersection of all ideals of R containing A. If $\varphi\colon R \to S$ is a ring homomorphism, then we claim that $\varphi((A)) = (\varphi(A))$, analogously to the situation for groups.

The inclusion $\supseteq$ is obvious, so let $b \in \varphi((A))$. Then $b = \varphi(a)$ for some $a \in (A)$, and

$$a = r_1 a_1 + \cdots + r_n a_n$$

for some $r_i \in R$ and $a_i \in A$. It follows that

$$b = \varphi(r_1)\varphi(a_1) + \cdots + \varphi(r_n)\varphi(a_n).$$

Hence $b \in (\varphi(A))$.

Now let $\varphi\colon R \to S$ be a surjective ring homomorphism with R Noetherian, and let $J \subseteq S$ be an ideal. Then $I = \varphi^{-1}(J)$ is an ideal in R, hence generated by a finite set $A \subseteq R$. Since φ is surjective we have $\varphi(I) = J$, so by the lemma above $J = \varphi((A)) = (\varphi(A))$. Since $\varphi(A)$ is finite, the claim follows. □

EXERCISE 4.3

Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

SOLUTION. Let I be a principal ideal of $\mathbb{Z}[x]$ containing $(2, x)$. Then there is some $f(x) \in \mathbb{Z}[x]$ such that $I = (f(x))$, and in particular $2 = p(x)f(x)$ and $x = q(x)f(x)$ for appropriate $p(x), q(x) \in \mathbb{Z}[x]$. The first equality implies that $\deg f(x) = 0$, and the second that $f(x)$ is monic. Hence $f(x) = 1$, but $1 \notin (2, x)$ so $(2, x) \neq I$. The claim follows. □

EXERCISE 4.4

Prove that if k is a field, then $k[x]$ is a PID.

SOLUTION. Let $I \subseteq k[x]$ be an ideal. If $I = (0)$ then I is principal, so assume that $I \neq (0)$. Let $f(x)$ be a nonzero polynomial in I with minimal degree. By multiplying by the reciprocal of the leading coefficient we may assume that $f(x)$ is monic. Let $g(x) \in I$. By division with remainder there exist $q(x), r(x) \in k[x]$ such that

$$g(x) = f(x)q(x) + r(x),$$

and such that $\deg r(x) < \deg f(x)$. Then $r(x) \in I$, but since $\deg f(x)$ was assumed to be minimal in I, we must have $\deg r(x) = -\infty$, i.e. $r(x) = 0$. Thus $g(x) \in (f(x))$, so $I = (f(x))$. □

EXERCISE 4.5

Let I, J be ideals in a commutative ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$.

SOLUTION. There exist $i \in I$ and $j \in J$ such that $i + j = 1$. For $a \in I \cap J$ it follows that

$$a = a(i + j) = ai + aj = ia + aj.$$

Since a lies in both I and J, this shows that $a \in IJ$. □

EXERCISE 4.10

Let d be an integer that is not the square of an integer, and consider the subset of $\mathbb{C}$ defined by

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

(a) Prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.

(b) Define a function $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(a + b\sqrt{d}) := a^2 - b^2 d$. Prove that $N(zw) = N(z)N(w)$ and that $N(z) \neq 0$ if $z \in \mathbb{Q}(\sqrt{d})$, $z \neq 0$.

(c) Prove that $\mathbb{Q}(\sqrt{d})$ is a field and in fact the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$.

(d) Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$.

SOLUTION. (a) For $a, b, c, e \in \mathbb{Q}$ we have

$$(a + b\sqrt{d}) + (c + e\sqrt{d}) = (a + b) + (b + e)\sqrt{d}$$

and

$$(a + b\sqrt{d})(c + e\sqrt{d}) = (ac + bed) + (ae + bc)\sqrt{d}.$$

Furthermore, $\mathbb{Q}(\sqrt{d})$ clearly contains additive inverses of all its elements.

(b) Writing $z = a + b\sqrt{d}$ and $w = c + e\sqrt{d}$ we find that

$$\begin{aligned} N(zw) &= N\Big((ac + bed) + (ae + bc)\sqrt{d}\Big) \\ &= (ac + bed)^2 - (ae + bc)^2 d \\ &= (ac)^2 - (ae)^2 d - (bc)^2 d + (bed)^2 \\ &= (a^2 - b^2 d)(c^2 - e^2 d) \\ &= N(z)N(w) \end{aligned}$$

as desired. Now assume that $N(z) = 0$. It follows that $a^2 = b^2 d$. For the prime factorisations of each side to agree, since d is not a square, we must have $a = b = 0$. Hence $z = 0$ as claimed.

(c) We prove that $\mathbb{Q}(\sqrt{d})$ is a field, so let $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Define $z^* = a - b\sqrt{d}$ and notice that $N(z) = zz^*$. If $z \neq 0$ then $N(z) \neq 0$, so it follows that $z^*/N(z)$ is the multiplicative inverse of z.

As for minimality, a subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt{d}$ must contain combinations on the form $a + b\sqrt{d}$ in order to be closed under addition and multiplication. Hence $\mathbb{Q}(\sqrt{d})$ is the smallest such subfield.

(d) We have a pair of isomorphisms

$$\frac{\mathbb{Q}[t]}{(t^2 - d)} \cong \mathbb{Q} \oplus \mathbb{Q} \cong \mathbb{Q}(\sqrt{d})$$

of abelian groups, where the first comes from Proposition 4.6 and the second is clear from the constraints on d. To see that this is also an isomorphism of rings, we simply take two elements in the quotient ring and see that the multiplication matches the multiplication on $\mathbb{Q}(\sqrt{d})$. □

EXERCISE 4.11

Let R be a commutative ring, $a \in R$, and $f_1(x), \ldots, f_r(x) \in R[x]$.

(a) Prove the equality of ideals

$$(f_1(x), \ldots, f_r(x), x - a) = (f_1(a), \ldots, f_r(a), x - a).$$

(b) Prove the useful substitution trick

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \ldots, f_r(a))}.$$

SOLUTION. (a) By division with remainder we have

$$f_i(x) = (x - a)q(x) + r$$

for some $q(x) \in R[x]$ and $r \in R$. Evaluating in $x = a$ we find that $r = f_i(a)$, so the claim follows.

(b) Consider the evaluation map $\varphi\colon R[x] \to R$ given by $f(x) \mapsto f(a)$. This is surjective (since it is constant on constant polynomials) with $\ker\varphi = (x-a)$, so the first isomorphism theorem implies that

$$\frac{R[x]}{(x-a)} \cong R.$$

Also notice that the image of $(f_1(x),\dots,f_r(x))$ under φ is $(f_1(a),\dots,f_r(a))$. Since

$$(f_1(a),\dots,f_r(a),x-a) = (f_1(a),\dots,f_r(a)) + (x-a),$$

it follows from Exercise 3.3 that

$$\frac{R[x]}{(f_1(x),\dots,f_r(x),x-a)} \cong \frac{R[x]/(x-a)}{(f_1(a),\dots,f_r(a))} \cong \frac{R}{(f_1(a),\dots,f_r(a))}$$

as desired. □

EXERCISE 4.17

Let K be a compact topological space, and let R be the ring of continuous real-valued functions on K, with addition and multiplication defined pointwise.

(i) For $p \in K$, let $M_p = \{f \in R \mid f(p) = 0\}$. Prove that M_p is a maximal ideal in R.

(ii) Prove that if $f_1,\dots,f_r \in R$ have no common zeros, then $(f_1,\dots,f_r) = (1)$.

(iii) Prove that every maximal ideal M in R is of the form M_p for some $p \in K$.

If further K is Hausdorff, prove that $p \mapsto M_p$ defines a bijection from K to the set of maximal ideals of R.

SOLUTION. (i) Let $p \in K$ and consider the map $\varphi\colon R \to \mathbb{R}$ given by $\varphi(f) = f(p)$. This is easily seen to be a surjective ring homomorphism with kernel M_p, so the first isomorphism theorem implies that $R/M_p \cong \mathbb{R}$. Hence R/M_p is a field, so M_p is a maximal ideal.

(ii) Let $f = f_1^2 + \cdots + f_r^2 \in (f_1,\dots,f_r)$. Then f is strictly positive everywhere, so $1/f$ is well-defined and continuous, i.e. an element of R. But then $1 = (1/f)f \in (f_1,\dots,f_r)$.

(iii) Let I be an ideal in R not contained in any M_p. (Every maximal ideal not on the form M_p must have this property.) For every $p \in K$ there is then

a function $f_p \in I$ such that $f_p(p) \neq 0$. Since f_p is continuous, there is an open neighbourhood $U_p \subseteq K$ of p such that $0 \notin f_p(U_p)$. The collection $\{U_p\}_{p\in K}$ is an open cover of K, so by compactness it has a finite subcover $U_{p_1}, \dots, U_{p_r}$. Every $p \in K$ lies in some U_{p_i}, so $f_{p_i}(p) \neq 0$. Thus $f_{p_1}, \dots, f_{p_r}$ have no common zeros, so $(f_{p_1}, \dots, f_{p_r}) = (1)$. It follows that $I = R$.

Finally, also assume that K is Hausdorff. It suffices to show that the map $p \mapsto M_p$ is injective. If $p \neq q$ are points in K, then Urysohn's lemma furnishes a function $f \in R$ such that $f(p) = 0$ and $f(q) = 1$. But then $f \in M_p$ and $f \notin M_q$, so the claim follows.

In fact, notice that the map $p \mapsto M_p$ is surjective if K is compact and injective if K is locally compact Hausdorff. □

Exercise 4.18

Let R be a commutative ring, and let N be its nilradical (cf. Exercise 3.12). Prove that N is contained in every prime ideal in R.

Solution. Let P be a prime ideal in R, and consider $a \in N$. Then there is an $n \in \mathbb{N}$ such that $a^n = 0$, and this lies in P since P is a subgroup of R. But since P is prime, it follows that either $a \in P$ or $a^{n-1} \in P$. Continuing this process yields $a \in P$, so $N \subseteq P$. □

Exercise 4.19

Let R be a commutative ring, let P be a prime ideal in R, and let I_j be ideals in R.

(i) Assume that $I_1 \cdots I_r \subseteq P$; prove that $I_j \subseteq P$ for some j.

(ii) By (i), if $P \supseteq \bigcap_{j=1}^{r} I_j$, then P contains one of the ideals I_j. Prove or disprove: if $P \supseteq \bigcap_{i=1}^{\infty} I_j$, then P contains one of the ideals I_j.

Solution. (i) If at least one of the ideals $I_2, \dots, I_r$ are contained in P, then we are done, so assume that neither of them are. Thus there exist $i_2 \in I_2, \dots, i_r \in I_r$, none of which lie in P. Now let $i_1 \in I_1$. Then $i_1 \cdots i_r \in P$ and since P is prime at least one of $i_1, \dots, i_r$ lie in P. But none of the elements $i_2, \dots, i_r$ do, so we must have $i_1 \in P$. Hence $I_1 \subseteq P$.

(ii) We give a counterexample. Notice that

$$\bigcap_{n=3}^{\infty} n\mathbb{Z} = (0) \subseteq 2\mathbb{Z},$$

but none of the $n\mathbb{Z}$ are contained in $2\mathbb{Z}$. □

EXERCISE 4.21

Let k be an algebraically closed field, and let $I \subseteq k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$.

SOLUTION. First assume that $I = (x - c)$ for some $c \in k$, and let J be an ideal in $k[x]$ that properly contains I. Consider a polynomial $f(x) \in J \setminus I$. If $f(x)$ is constant it is a unit, hence $J = k[x]$. If $\deg f(x) = 1$ we may assume that $f(x)$ is monic, i.e. that $f(x) = x - b$ for some $b \in k$. It follows that $b \neq c$, hence J contains the constant polynomial $(x - b) - (x - c) = c - b \neq 0$, so again $J = k[x]$. Finally assume that $\deg f(x) \geq 2$. By division with remainder there exist $q(x) \in k[x]$ and $r \in k$ such that

$$f(x) = q(x)(x - c) + r.$$

It follows that $r \in J$ since J contains I. We must also have $r \neq 0$, since otherwise $f(x) \in I$, so again we have $J = k[x]$.

Conversely, let I be a maximal ideal in $k[x]$, and let $f(x) \in I$ be nonconstant. Since k is algebraically closed, there exists an $r \in k$ such that $f(r) = 0$. Division with remainder then yields $q(x) \in k[x]$ and $s \in k$ such that

$$f(x) = q(x)(x - r) + s.$$

We find that $s = f(r) = 0$, so $f(x) \in (x - r)$. Thus $I \subseteq (x - r)$, and since I is maximal the opposite inclusion also holds. This proves the claim. □

EXERCISE 4.22

Prove that $(x^2 + 1)$ is maximal in $\mathbb{R}[x]$.

SOLUTION. Let I be an ideal in $\mathbb{R}[x]$ that properly contains $(x^2 + 1)$. Since $\mathbb{R}[x]$ is a PID by Exercise 4.4, there is a polynomial $f(x) \in \mathbb{R}[x]$ such that $I = (f(x))$. Then $x^2 + 1 = q(x)f(x)$ for some $q(x) \in \mathbb{R}[x]$. If $q(x) \in \mathbb{R}$, then $f(x) \in (x^2 + 1)$ which is impossible, so we must have $0 < \deg q(x) \leq 2$. If $\deg q(x) = 1$, then $q(x)$ has a root in $\mathbb{R}$. This is then also a root of $x^2 + 1$, which is also impossible. Hence $\deg q(x) = 2$, which implies that $f(x) \in \mathbb{R}$. Thus $I = \mathbb{R}[x]$. □

III.5. Modules over a ring

REMARK III.2. We elaborate on Example 5.6 and the definition of an R-algebra in Definition 5.7. Given a ring S, left multiplication $\lambda\colon S \to \mathrm{End}_{\mathbf{Ab}}(S)$ is a ring homomorphism by Proposition 2.7. If $\alpha\colon R \to S$ is a ring homomorphism, we can equip S with the R-module structure

$$\sigma\colon R \to \mathrm{End}_{\mathbf{Ab}}(S)$$

given by $\sigma = \lambda \circ \alpha$. That is, $\sigma(r) = \lambda_{\alpha(r)}$ is multiplication in S by $\alpha(r)$. Hence

$$\rho(r,s) = \sigma(r)(s) = \lambda_{\alpha(r)}(s) = \alpha(r)s,$$

as seen in Example 5.6.

In the case where R is *commutative*, Aluffi defines an R-algebra as a ring homomorphism $\alpha\colon R \to S$ such that $\alpha(R)$ lies in the centre of S. In this case we can also make S into a module using the construction above, and multiplication in S is furthermore R-bilinear: it is in this sense that the module structure σ and the multiplication in S are compatible.

We can thus construct R-algebras by taking rings and equipping them with a compatible R-module structure, taking advantage of the ring structure to do so.

In general we can think of an (associative) R-algebra S as a ring that is also an R-module such that the ring and module structures are compatible. By this we mean that the ring addition and the module addition coincide, and that

$$(rs)s' = r(ss') = s(rs') \tag{III.1}$$

for all $r \in R$ and $s, s' \in S$. To recover the definition in terms of ring homomorphisms, define a map $\alpha\colon R \to S$ by $\alpha(r) = r1_S$, where 1_S is the ring identity in S. We easily see that α is a ring homomorphism. The map $\sigma\colon R \to \mathrm{End}_{\mathbf{Ab}}(S)$ given by $\sigma = \lambda \circ \alpha$ is thus also a ring homomorphism, and it thus defines an R-module structure on S. This is more explicitly given by

$$\rho(r,s) = \sigma(r)(s) = \lambda_{\alpha(r)}(s) = \alpha(r)s = (r1_S)s = r(1_S s) = rs,$$

which agrees with the original module structure on S. This uses the first equality in (III.1). Finally we show that $\alpha(R)$ lies in the centre of S. For $r \in R$ and $s \in S$ we have

$$\alpha(r)s = (r1_S)s = r(1_S s) = rs$$

using the first equality in (III.1), and the second equality yields

$$s\alpha(r) = s(r1_S) = r(s1_S) = rs.$$

Thus $\alpha(r)$ and s commute as claimed. ⌟

EXERCISE 5.5

Let R be a ring, viewed as an R-module over itself, and let M be an R-module. Prove that $\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(R, M) \cong M$ as R-modules

SOLUTION. Define a map $\alpha\colon \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(R,M) \to M$ by $\alpha(\varphi) = \varphi(1_R)$. This is easily seen to be a module homomorphism. For $m \in M$ define a map $\beta_m\colon R \to M$ by $\beta_m(r) = rm$, which is clearly a module homomorphism, and further define $\beta\colon M \to \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(R,M)$ by $\beta(m) = \beta_m$. For $\varphi \in \mathrm{Hom}_{R\text{-}\mathbf{Mod}}(R,M)$ and $r \in R$ we have

$$\beta_{\varphi(1_R)}(r) = r\varphi(1_R) = \varphi(r),$$

so $\beta(\varphi(1)) = \varphi$. It follows that

$$(\beta \circ \alpha)(\varphi) = \beta(\varphi(1)) = \varphi.$$

Conversely, for $m \in M$ we have

$$(\alpha \circ \beta)(m) = \alpha(\beta_m) = \beta_m(1_R) = 1_R m = m.$$

Thus β is the inverse (in **Set**) of α, hence a module homomorphism. In total, α is an isomorphism in R-**Mod**. □

EXERCISE 5.6

Let G be an abelian group. Prove that if G has a structure of $\mathbb{Q}$-vector space, then it has only one such structure.

SOLUTION. A $\mathbb{Q}$-vector space structure on G is a ring homomorphism

$$\mathbb{Q} \to \mathrm{End}_{\mathbf{Ab}}(G).$$

Let σ and τ be two such structures, and let $\iota\colon \mathbb{Z} \to \mathbb{Q}$ be the unique ring homomorphism. Since there is also a unique ring homomorphism $\mathbb{Z} \to \mathrm{End}_{\mathbf{Ab}}(G)$, we must have $\sigma \circ \iota = \tau \circ \iota$. But ι is an epimorphism, so this implies that $\sigma = \tau$.□

EXERCISE 5.7

Let K be a field, and let $k \subseteq K$ be a subfield of K. Show that K is a vector space over k (and in fact a k-algebra) in a natural way.

SOLUTION. Let $\iota\colon k \to K$ be the inclusion map. If $\mu\colon K \to \mathrm{End}_{\mathbf{Ab}}(K)$ is multiplication on K, then $\sigma = \mu \circ \iota$ is a k-module structure on K. Explicitly, this induces an action $\rho\colon k \times K \to K$ given by

$$\rho(c,a) = \mu_{\iota(c)}(a) = \iota(c)a = ca.$$

Since K is a field, the image of ι obviously lies in the centre of K, so K is a k-algebra. □

EXERCISE 5.9

Let R be a commutative ring, and let M be an R-module.

(a) Prove that the operation of composition on the R-module $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$ makes the latter into an R-algebra in a natural way.

(b) Prove that $\mathcal{M}_n(R)$ is an R-algebra, in a natural way.

SOLUTION. (a) Recall that composition makes $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M) \subseteq \mathrm{End}_{\mathbf{Ab}}(M)$ into a ring, since composition preserves module homomorphisms. We equip $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$ with R-module structure using the method in Example 5.6: Define a map $\lambda\colon R \to \mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$ given by $\lambda(r) = \lambda_r$, where $\lambda_r(m) = rm$ for $r \in R$ and $m \in M$. This is clearly a ring homomorphism. This induces an action $\rho\colon R \times \mathrm{End}_{R\text{-}\mathbf{Mod}}(M) \to \mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$ given by

$$\rho(r, \varphi) = \lambda(r) \circ \varphi = \lambda_r \circ \varphi = r\varphi$$

for $r \in R$ and $\varphi \in \mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$. Furthermore, since φ is a module homomorphism we also have $\lambda_r \circ \varphi = \varphi \circ \lambda_r$, so the image of λ lies in the centre of $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$. □