Aluffi, *Algebra: Chapter 0*

Danny Nygård Hansen

29th December 2023

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

REMARK II.1: Bezout's identity.
The identity in Exercise 2.13 is known as *Bezout's identity*. Notice that if $a, b, m, n \in \mathbb{Z}$ satisfy

$$am + bn = 1,$$

then the exercise not only shows that m and n are relatively prime, but also that (a, b), (m, b) and (a, n) are pairs of relatively prime integers.

If $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, then there exist $a, b \in \mathbb{Z}$ such that $am + bn = 1$. But this also shows that a and n are relatively prime (so $[a]_n$ is a multiplicative inverse of $[m]_n$), finishing the proof of Proposition 2.6 which says that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group. ⌟

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 $1 \le i, j \le n$,

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

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

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

$x^2 = e$ 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^iy^j. Using the other two relations we find that we can choose i and j such that $0 \le i \le 1$ and $0 \le j < n$, 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

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

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^iy^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**

REMARK II.2: Universal algebra.

Let A be a set and let $n \in \mathbb{N}$. An *operation on* A is a set function $A^n \to A$. The set $A^0 \cong 1$ is a singleton and is only determined up to isomorphism in **Set**. The number n is called the operation's *arity*, and we say that the operation is *n-ary*. A 0-ary operation is also called a *constant*. If $c\colon \{*\} \to A$ is a constant, then instead of $c(*)$ we simply write c.

An *algebra* is a pair $\mathfrak{A} = \langle A, F\rangle$, where A is a set[2] and F is a collection (of arbitrary cardinality) of operations on A. Writing $F = \{f_i \mid i \in I\}$ for some index set I, the *(similarity) type* of $\mathfrak{A}$ is the function $\rho\colon I \to \mathbb{N}$ where $\rho(i)$ is the arity of f_i. If I is a finite set, then writing $I = \{1,\dots,k\}$ we display the type of an algebra by the tuple $\langle \rho(1),\dots,\rho(k)\rangle$, and we also refer to this tuple as the type of the algebra. Notice that if any operation in F is a constant, then A must be nonempty.

A *subalgebra* of $\mathfrak{A}$ is an algebra $\mathfrak{S} = \langle S, F_S\rangle$ such that $S \subseteq A$, and such that for each $g \in F_S$ there is an $f \in F$ with $g = f|_S$. Notice that a subset $S \subseteq A$ induces a subalgebra if $f(S^n) \subseteq S$ for all $f \in F$, where $n = \rho(f)$. We will usually identify the algebra $\mathfrak{S}$ with the underlying set S.

When considering the family of algebras with a particular similarity type, it is common to index the operations on each algebra by a family $\mathcal{F}$ of *operation symbols*. In this case we write $\mathcal{F}^{\mathfrak{A}}$ for the set of operations on $\mathfrak{A}$, and for each $f \in \mathcal{F}$ we write $f^{\mathfrak{A}}$ for the corresponding operation on $\mathfrak{A}$.

Let $\mathfrak{A} = \langle A, \mathcal{F}^{\mathfrak{A}}\rangle$ and $\mathfrak{B} = \langle B, \mathcal{F}^{\mathfrak{B}}\rangle$ be algebras of the same similarity type $\rho\colon \mathcal{F} \to \mathbb{N}$. A set function $\varphi\colon A \to B$ is called a *homomorphism* from $\mathfrak{A}$ to $\mathfrak{B}$ if

$$\varphi\left(f^{\mathfrak{A}}(a_1,\dots,a_n)\right) = f^{\mathfrak{B}}(\varphi(a_1),\dots,\varphi(a_n))$$

with $n = \rho(f)$ for all $f \in \mathcal{F}$ and all $a_1,\dots,a_n \in A$. In this case we write $\varphi\colon \mathfrak{A} \to \mathfrak{B}$. This is equivalent to the diagram (in **Set**)

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi\times\cdots\times\varphi} & B^n \\ {\scriptstyle f^{\mathfrak{A}}}\downarrow & & \downarrow{\scriptstyle f^{\mathfrak{B}}} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

commuting for all $f \in \mathcal{F}$. In the case where $\rho(f) = 0$ we interpret the 0-fold product of φ with itself as the unique map $1 \to 1$, and the above square is equivalent to the triangle

$$\begin{array}{ccc} & 1 & \\ {\scriptstyle f^{\mathfrak{A}}}\swarrow & & \searrow{\scriptstyle f^{\mathfrak{B}}} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

Then $f^{\mathfrak{A}}$ and $f^{\mathfrak{B}}$ are constants, and this diagram means that $\varphi(f^{\mathfrak{A}}) = f^{\mathfrak{B}}$, i.e. that φ preserves the constant corresponding to f.

By pasting together two of the above types of diagrams, it is easy to see that function composition preserves homomorphisms. Since the identity on each algebra is obviously a homomorphism, each similarity type gives rise to a category. ⌟

[2] Many authors require A to be nonempty, e.g. Manzano and Bergman

REMARK II.3: Images and preimages of subalgebras.
Let $\mathfrak{A} = \langle A, \mathcal{F}^{\mathfrak{A}} \rangle$ and $\mathfrak{B} = \langle B, \mathcal{F}^{\mathfrak{B}} \rangle$ be algebras of the same type $\rho\colon \mathcal{F} \to \mathbb{N}$, where $\mathcal{F}$ is a family of operation symbols. Further let $S \subseteq A$ and $T \subseteq B$ be subalgebras, and let $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ a homomorphism.

We first claim that $\varphi(S)$ is a subalgebra of $\mathfrak{B}$. Consider $f \in \mathcal{F}$ and let $n = \rho(f)$. For any $y_1, \dots, y_n \in \varphi(S)$ there exist $x_1, \dots, x_n \in S$ such that $\varphi(x_i) = y_i$ for $i = 1, \dots n$. Then $f^{\mathfrak{A}}(x_1, \dots, x_n) \in S$ since S is a subalgebra, and because φ is a homomorphism we have

$$f^{\mathfrak{B}}(y_1, \dots, y_n) = f^{\mathfrak{B}}\Big(\varphi(x_1), \dots, \varphi(x_n)\Big) = \varphi\Big(f^{\mathfrak{A}}(x_1, \dots, x_n)\Big) \in \varphi(S)$$

as required.

Next we claim that $\varphi^{-1}(T)$ is either empty (if this is not allowed in the definition of an algebra) or a subalgebra of $\mathfrak{A}$. If $x_1, \dots, x_n \in \varphi^{-1}(T)$, then $\varphi(x_1), \dots, \varphi(x_n) \in T$. Hence

$$\varphi\Big(f^{\mathfrak{A}}(x_1, \dots, x_n)\Big) = f^{\mathfrak{B}}\Big(\varphi(x_1), \dots, \varphi(x_n)\Big) \in T$$

since T is a subalgebra. Hence $f^{\mathfrak{A}}(x_1, \dots, x_n) \in \varphi^{-1}(T)$ as claimed. Furthermore, if there is a nullary symbol f in $\mathcal{F}$, then $\varphi^{-1}(T)$ is nonempty since it must contain the image of $f^{\mathfrak{A}}$. ⌟

REMARK II.4: Homomorphisms and generating subalgebras.
If $\mathfrak{A} = \langle A, F \rangle$ is an algebra and $S \subseteq A$, then we denote the smallest subalgebra of $\mathfrak{A}$ containing S by $\langle S \rangle_{\mathfrak{A}}$, or simply $\langle S \rangle$ if $\mathfrak{A}$ is understood.

Let $\mathfrak{A} = \langle A, \mathcal{F}^{\mathfrak{A}} \rangle$ and $\mathfrak{B} = \langle B, \mathcal{F}^{\mathfrak{B}} \rangle$ be algebras of the same type, where $\mathcal{F}$ is a family of operation symbols. If $\varphi\colon \mathfrak{A} \to \mathfrak{B}$ is a homomorphism and $S \subseteq A$ is any subset, then we claim that $\langle \varphi(S) \rangle_{\mathfrak{B}} = \varphi(\langle S \rangle_{\mathfrak{A}})$. The inclusion '$\subseteq$' is obvious since the image of a subalgebra is a subalgebra. For the other inclusion, first define $S_0 = S$ and

$$S_{n+1} = S_n \cup \Big\{ f^{\mathfrak{A}}(a_1, \dots, a_k) \;\Big|\; a_1, \dots, a_k \in S_n \text{ and } f \in \mathcal{F} \Big\}$$

for $n \in \mathbb{N}$. Then clearly $\langle S \rangle_{\mathfrak{A}} = \bigcup_{n \in \mathbb{N}} S_n$. Since function images respect unions, it suffices to show that $\varphi(S_n) \subseteq \langle \varphi(S) \rangle_{\mathfrak{B}}$ for all $n \in \mathbb{N}$. This is obvious for $n = 0$. Next assume that the inclusion holds for some $n \in \mathbb{N}$, let $f \in \mathcal{F}$ have rank k, and let $a_1, \dots, a_k \in S_n$. Then

$$\varphi\Big(f^{\mathfrak{A}}(a_1, \dots, a_k)\Big) = f^{\mathfrak{B}}\Big(\varphi(a_1), \dots, \varphi(a_k)\Big) \in \langle \varphi(S) \rangle_{\mathfrak{B}}$$

by induction, since each $\varphi(a_i)$ lies in $\varphi(S_n)$. ⌟

REMARK II.5. The universal algebra definition of groups is as follows: First, a *semigroup* is an algebra $\langle S, \cdot \rangle$, where $\cdot$ is a binary operation (in infix notation), satisfying the associative law

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

A *monoid* is an algebra $\langle M, \cdot, e\rangle$, where e is a constant, such that $\langle M, \cdot\rangle$ is a semigroup, and which satisfies the identities

$$x \cdot e = x \quad \text{and} \quad e \cdot x = x.$$

Finally, a *group* is an algebra $\langle G, \cdot, \iota, e\rangle$, where ι is a unary operation, such that $\langle G, \cdot, e\rangle$ is a monoid, and which satisfies

$$x \cdot \iota(x) = e = \iota(x) \cdot x.$$

We usually denote the operation $\cdot$ by concatenation, and we write $\iota(x) = x^{-1}$.

For a map $\varphi\colon G \to H$ between groups, it turns out that for φ to be a group homomorphism it is sufficient that φ commutes with the group operation. This is obviously also the case for semigroups, but for monoids we do require it to respect both the group operation and preserve the identity. ⌟

EXERCISE 3.3

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

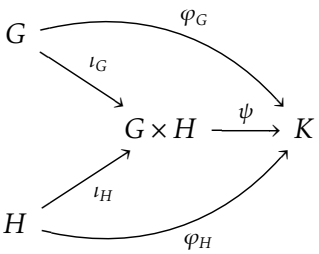
SOLUTION. Let $\varphi_G\colon G \to K$ and $\varphi_H\colon H \to K$ be homomorphisms into an abelian group K. Define a map $\psi\colon G \times H \to K$ by

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

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

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

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. □

II.4. Group homomorphisms

REMARK II.6: Cyclic groups.

We prove that a group G is generated by a single element if and only if it is cyclic. The 'if' part is clear, so assume that G is generated by some element g and consider the exponential map $\varepsilon_g \colon \mathbb{Z} \to G$ given by $\varepsilon_g(n) = g^n$. This is clearly a surjective group homomorphism, so if it is injective then $G \cong \mathbb{Z}$, and if it is trivial then $G \cong 1$.

Otherwise choose $m_1 < m_2$ such that $g^{m_1} = g^{m_2}$. Then $g^{m_2 - m_1} = e$, so let m be the smallest positive integer such that $g^m = e$. It follows that the kernel of ε_g is $m\mathbb{Z}$, so in this case $G \cong \mathbb{Z}/m\mathbb{Z}$. ⌟

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. □

EXERCISE 4.14

Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r < n$ that are relatively prime to n. (This is called *Euler's φ-function*; cf. Exercise 6.14.)

SOLUTION. We use additive notation. Let $\varphi \in \mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}/n\mathbb{Z})$ be an automorphism, and let $k \in \mathbb{Z}$. Then

$$\varphi([k]) = k\varphi([1]),$$

so every automorphism (indeed every *endo*morphism) is given by multiplication by some element $\varphi([1])$. Next notice that since φ is injective, we must

have $\varphi([1]) \in (\mathbb{Z}/n\mathbb{Z})^*$, otherwise we would have $\varphi([k]) = [0]$ for some $k \neq 0$. Hence the map

$$\begin{aligned} \mu\colon (\mathbb{Z}/n\mathbb{Z})^* &\to \mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}/n\mathbb{Z}), \\ k &\mapsto \mu_k, \end{aligned}$$

where μ_k is multiplication by k, is surjective if it is well-defined. But it is, since $\mu_k^{-1} = \mu_{k^{-1}}$. It is also clearly injective, which proves the desired claim.

In fact μ is a group homomorphism, since

$$\mu_{k+l}(x) = (k+l)x = kx + lx = \mu_k(x) + \mu_l(x),$$

hence a group isomorphism. □

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

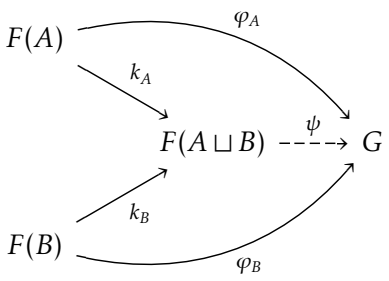
$$\varphi(j(a)) = f(a) \neq f(b) = \varphi(j(b)),$$

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

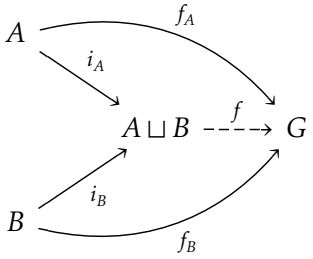
Exercise 5.8

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

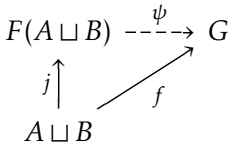
Solution. Given homomorphisms $\varphi_A\colon F(A) \to G$ and $\varphi_B\colon F(B) \to G$ into a group G, we must prove the existence and uniqueness of a homomorphism $\psi\colon F(A \sqcup B) \to G$ such that the diagram



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 $f\colon A \sqcup B \to G$ making the diagram



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

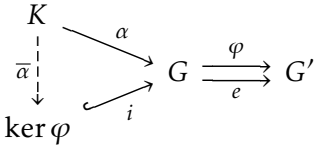
(b) Let $\varphi\colon F^{ab}(A) \to F^{ab}(B)$ be an isomorphism. Let $\sim_A$ and $\sim_B$ denote the above equivalence relations on $F^{ab}(A)$ and $F^{ab}(B)$ respectively, and notice that $f \sim_A f'$ if and only if $\varphi(f) \sim_B \varphi(f')$. Thus the number of $\sim_A$- and $\sim_B$-equivalence 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.7. 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 $e\colon G \to G'$. In other words, for any group homomorphism $\alpha\colon K \to G$ such that $\varphi \circ \alpha = e \circ \alpha$ 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 $\ker\varphi$. ⌟

Remark II.8: Equaliser subgroups.
A subgroup H of a group G is called an *equaliser subgroup* if it is the equaliser of two parallel homomorphisms $\varphi, \psi\colon G \to G'$, i.e. if $H = \{g \in G \mid \varphi(g) = \psi(g)\}$. The above remark shows that kernels (and hence normal subgroups) are equaliser subgroups.

In fact, every subgroup of any group is an equaliser subgroup, a fact we return to in [TODO epi surjection]. To show this, let H be a subgroup of G, let $\mathbf{1} = \{*\}$ be a one-element set, and let K be the permutation group of the disjoint union $G/H \sqcup \mathbf{1}$. Let $\rho \in S$ be the permutation that exchanges eH and the element $*$ of $\mathbf{1}$ and leaves the rest of the set fixed. Then define the maps

$\varphi, \psi\colon G \to S$ by $\varphi(g) = \lambda_g \sqcup \mathrm{id}_{\mathbf{1}}$, where λ_g is left multiplication by g, and define further $\psi(g) = \rho \circ \varphi(g) \circ \rho^{-1}$. For $g, g' \in G$ we have

$$\begin{aligned}\varphi(gg') &= \lambda_{gg'} \sqcup \mathrm{id}_{\mathbf{1}} \\ &= (\lambda_g \circ \lambda_{g'}) \sqcup \mathrm{id}_{\mathbf{1}} \\ &= (\lambda_g \sqcup \mathrm{id}_{\mathbf{1}}) \circ (\lambda_{g'} \sqcup \mathrm{id}_{\mathbf{1}}) \\ &= \varphi(g) \circ \varphi(g'),\end{aligned}$$

so φ is a homomorphism. We further have

$$\psi(gg') = \rho \circ \varphi(gg') \circ \rho^{-1} = (\rho \circ \varphi(g) \circ \rho^{-1}) \circ (\rho \circ \varphi(g') \circ \rho^{-1}) = \psi(g) \circ \psi(g'),$$

and so ψ is also a homomorphism.

Next notice that if $g \in H$, then $g(eH) = eH$, so

$$\psi(g)(*) = (\rho \circ \varphi(g) \circ \rho^{-1})(*) = (\rho \circ \varphi(g))(eH) = \rho(eH) = * = \varphi(g)(*),$$

and we similarly find that $\varphi(g)(g'H) = \psi(g)(g'H)$ when $g' \in H$, since then $g'H = eH$. For $g' \in G \setminus H$ we have $gg' \notin H$, so

$$\psi(g)(g'H) = (\rho \circ \varphi(g) \circ \rho^{-1})(g'H) = (\rho \circ \varphi(g))(g'H) = \rho(gg'H) = gg'H = \varphi(g)(g'H).$$

Hence $\varphi(g) = \psi(g)$ when $g \in H$. Now assume that $g \notin H$. Then also $g^{-1} \notin H$, so

$$\psi(g)(g^{-1}H) = (\rho \circ \varphi(g) \circ \rho^{-1})(g^{-1}H) = (\rho \circ \varphi(g))(g^{-1}H) = \rho(eH) = *.$$

On the other hand, $\varphi(g)(g^{-1}H) = eH$, so $\varphi(g) \neq \psi(g)$ when $g \notin H$. In total, H is the equaliser subgroup of φ and ψ.

Notice that if G is finite then K is also finite, so this argument shows that in the category **FinGrp** of finite groups, every subgroup is also an equaliser.⌟

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 $i, j \in \mathbb{N}$.[3] 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.

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 $g \in G$. But then $\gamma_a = 1_G$, so $\mathrm{Inn}(G)$ is generated by 1_G and hence 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

[3] The natural numbers include zero.

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 $f\colon A\to G$ 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 $m=\operatorname{lcm}(q_1,\dots,q_n)$. 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 6.14

If m is a positive integer, denote by $\varphi(m)$ the number of positive integers $r<m$ that are relatively prime to m; this is called *Euler's φ- (or 'totient') function*. In other words, $\varphi(m)$ is the order of the group $(\mathbb{Z}/m\mathbb{Z})^*$; cf. Proposition 2.6. Put together the following observations:

(a) $\varphi(m)$ equals the number of generators of C_m,

(b) every element of C_n generates a subgroup of C_n,

(c) the discussion following Proposition 6.11 (in particular, every subgroup of C_n is isomorphic to C_m for some $m\mid n$),

to obtain a proof of the formula

$$\sum_{m>0,m|n} \varphi(m) = n.$$

SOLUTION. (a) This is just Corollary 2.5, which says that $[n]_m$ generates $\mathbb{Z}/m\mathbb{Z}$ iff $\gcd(m,n) = 1$.

(b) This is obvious.

(c) In additive notation, every subgroup H of $\mathbb{Z}/n\mathbb{Z}$ is cyclic, hence isomorphic to $\mathbb{Z}/m\mathbb{Z}$ for some m. Lagrange's theorem then implies that $m \mid n$.

Alternatively, Proposition 6.11 says that H is generated by $[d]_n$ for some $d \mid n$. But then

$$m := |[d]_n| = \frac{n}{\gcd(d,n)}$$

by Proposition 2.3, and m is also a divisor of n.

We now prove the formula. Denote by G_m the subset of C_n that generate a subgroup of order $m > 0$. Then $|G_m| = \varphi(m)$ by (a). Notice that every element in C_n lies in some G_m by (b), and that the G_m are disjoint so that they form a partition of C_n. Finally, $G_m = \emptyset$ unless $m \mid n$ by (c). In total we have

$$n = |C_n| = \sum_{m>0} |G_m| = \sum_{m>0,m|n} |G_m| = \sum_{m>0,m|n} \varphi(m),$$

as desired. □

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.9. 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 $\sim_f$ on X given by $x' \sim_f x$ if and only if $f(x) = f(x')$. As with e.g. group-theoretic kernels, f is injective if and only if $\ker f$ is trivial, i.e. equality. Furthermore, if $\sim$ is another equivalence relation on X, then f factors (uniquely) through $X/\!\sim$ if and only if $\sim \subseteq \ker f$. That is, f has to make the same identifications as $\sim$.

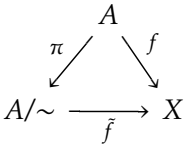
In **Set** we cannot say much more about this relation, but in **Grp** we recover the usual notion of kernel as follows: Recall that if H is a subgroup of a group G, then we define a left-invariant[4] equivalence relation $\sim_H$ on G by letting $a \sim_H b$ iff $a^{-1}b \in H$, for $a, b \in G$. If $\varphi\colon G \to G'$ is a group homomorphism, 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. In other words, $\sim_{\ker\varphi} = \sim_\varphi$.[5] Thus the equivalence relation generated by the subgroup $\ker\varphi$ is precisely the relation $\ker\varphi = \sim_\varphi$, and in particular the notation $G/\ker\varphi$ for the quotient group is unambiguous.

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

Remark II.10: Coslice categories and quotients.

Fix a set A, and let $\sim$ be an equivalence relation on A. Consider the category $\mathbf{Set}_\sim$, which is the subcategory of the coslice category $A/\mathbf{Set}$ whose objects are set functions $f\colon A \to X$ with the property that $a \sim a'$ implies $f(a) = f(a')$. We claim that the quotient map $\pi\colon A \to A/\!\sim$ is initial in $\mathbf{Set}_\sim$. That is, for any function f as above, there is a unique set function $\tilde f\colon A/\!\sim \to X$ making the diagram



commute. But this is just the function $\tilde f([a]) = f(a)$.

[4] We might as well have considered *right*-invariant relations.

[5] Already now we start to see that kernels are special kinds of subgroups. We defined $\sim_{\ker\varphi}$ as a *left*-invariant equivalence relation, but there is no reference to either left- or right-invariance in the definition of $\sim_\varphi$. Hence we might expect that $\sim_{\ker\varphi}$ is also *right*-invariant, which it indeed is since $\ker\varphi$ is normal.

Next fix a group G, and let $\sim$ be a both left- and right-invariant equivalence relation on G. Consider the category $\mathbf{Grp}_\sim$, which is the subcategory of $\mathbf{Set}_\sim$ whose objects and arrows are all group homomorphisms. Then the quotient map $\pi\colon G \to G/\!\sim$ is initial in $\mathbf{Set}_\sim$, and we claim that it is also initial in $\mathbf{Grp}_\sim$. This will follow if, in the diagram

$$\begin{array}{ccc} & G & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle\varphi} \\ G/\!\sim & \xrightarrow[\tilde\varphi]{} & H \end{array}$$

both π and $\tilde\varphi$ are group homomorphisms. But π is a homomorphism since $\sim$ is invariant, so π is indeed an object in $\mathbf{Grp}_\sim$. And $\tilde\varphi$ is easily seen to be a homomorphism, so it is indeed an arrow in $\mathbf{Grp}_\sim$.

Finally let G be an arbitrary group, and let $\mathbf{Ab}_G$ be the subcategory of $G/\mathbf{Grp}$ whose objects are group homomorphisms $\varphi\colon G \to H$ such that H is an *abelian* group. Notice that for such a φ, the commutator subgroup $[G,G]$ (which is normal by Exercise 7.11) is contained in $\ker\varphi$. Letting $\sim$ denote the equivalence relation on G generated by $[G,G]$, then φ respects $\sim$, and so $\mathbf{Ab}_G$ is a full subcategory of $\mathbf{Grp}_\sim$. But $G/\!\sim$ is the abelianisation $G_{ab} = G/[G,G]$ of G, in particular abelian by Exercise 7.11, so the quotient map $\pi\colon G \to G/\!\sim$ is initial in $\mathbf{Grp}_\sim$ and hence also in $\mathbf{Ab}_G$. This means that every homomorphism $\varphi\colon G \to H$ with H abelian factors uniquely through G_{ab}, i.e. there is a unique homomorphism $\tilde\varphi$ such that the diagram

$$\begin{array}{ccc} & G & \\ {\scriptstyle\pi}\swarrow & & \searrow{\scriptstyle\varphi} \\ G_{ab} & \xrightarrow[\tilde\varphi]{} & H \end{array}$$

commutes. ⌟

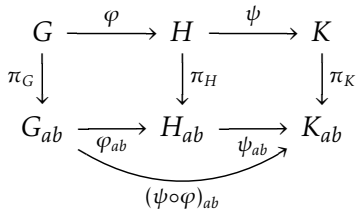
REMARK II.11: The abelianisation functor.

Let G and H be groups, and let $\pi_G\colon G \to G_{ab}$ and $\pi_H\colon H \to H_{ab}$ be the quotient maps onto their abelianisations. For any homomorphism $\varphi\colon G \to H$, the map $\pi_H \circ \varphi$ maps from a group to an abelian group, so there is a unique homomorphism $\varphi_{ab}\colon G_{ab} \to H_{ab}$ such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle\pi_G}\downarrow & & \downarrow{\scriptstyle\pi_H} \\ G_{ab} & \xrightarrow[\varphi_{ab}]{} & H_{ab} \end{array}$$

commutes. This gives rise to a map $(-)_{ab}\colon \mathbf{Grp} \to \mathbf{Ab}$ between categories. To see that this is a functor, let $\psi\colon H \to K$ be another group homomorphism, and

consider the diagram



By uniqueness we have $(\psi\circ\varphi)_{ab} = \psi_{ab}\circ\varphi_{ab}$, so $(-)_{ab}$ is indeed a functor. In fact, if $U\colon \mathbf{Ab} \to \mathbf{Grp}$ is the forgetful functor, we have an adjunction $(-)_{ab} \dashv U$. ⌟

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 $f\colon A \to G$ 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. □

EXERCISE 7.14

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

SOLUTION. Let $g \in G$ and $\varphi \in \mathrm{Aut}(G)$. For $h \in G$ we then have

$$(\varphi \circ \gamma_g \circ \varphi^{-1})(h) = \varphi\big(g\varphi^{-1}(h)g^{-1}\big) = \varphi(g)h\varphi(g)^{-1} = \gamma_{\varphi(g)}(h),$$

so $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)} \in \mathrm{Inn}(G)$ as desired. □

II.8. Canonical decomposition and Lagrange's theorem

REMARK II.12. 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:[6]

(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.

(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

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

[6] 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.

as desired. ⌟

REMARK II.13: Second isomorphism theorem.
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. The relevant sublattice of the lattice $\mathfrak{L}(G)$ of subgroups of G is seen in Figure 1.

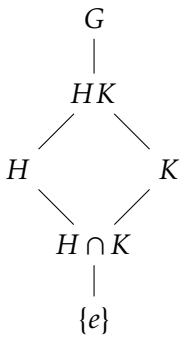


Figure 1: Sublattice of $\mathfrak{L}(G)$.

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

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

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. ⌟

REMARK II.14: Modular lattices.
Let $(\mathfrak{L}, \vee, \wedge)$ be a lattice. An element $x \in \mathfrak{L}$ is said to be *modular* if[7]

[7] There are a couple of different definitions of modularity of *elements*, but these are all equivalent for modularity of *lattices*. Some authors use only one of the following two properties in the definition.

(1) $a \vee (x \wedge c) = (a \vee x) \wedge c$ for all $a, c \in \mathfrak{L}$ with $a \leq c$, and

(2) $x \vee (b \wedge c) = (x \vee b) \wedge c$ for all $b, c \in \mathfrak{L}$ with $x \leq c$.

Furthermore, $\mathfrak{L}$ itself is said to be modular if every element of $\mathfrak{L}$ is modular. If G is a group, then a subgroup H of G is said to be modular if it is a modular element of the lattice $\mathfrak{L}(G)$ of subgroups of G.

We first prove the *modular property of groups*: If H, K, L are subgroups of G with $H \leq L$, then $HK \cap L = H(K \cap L)$. The inclusion '$\supseteq$' is clear since

$$H(K \cap L) \subseteq HK \cap HL = HK \cap L.$$

For the other inclusion, let $h \in H$ and $k \in K$ be such that $hk \in L$. Then since also $h \in L$ we have

$$k = h^{-1}hk \in L,$$

so $k \in K \cap L$. In total, $hk \in H(K \cap L)$.

A subgroup H of G is said to be *permutable* (or *quasinormal*) in G if it commutes with every subgroup K of G, i.e. $HK = KH$. Every normal subgroup of G is thus permutable in G. We claim that H is permutable in G only if H is modular. First notice that $HK = H \vee K$ since H and K commute. Since also $H \cap K = H \wedge K$, the modularity property immediately implies the second of the two criteria. To prove the first criterion, it suffices to show that H and $K \cap L$ also commute if H and K do. If $h \in H$ and $k \in K \cap L$, then since H and K commute there exist $h' \in H$ and $k' \in K$ such that $hk = k'h'$. But then notice that

$$k' = (hk)(h')^{-1},$$

which lies in L. Hence $H(K \cap L) \subseteq (K \cap L)H$, and the opposite inclusion follows similarly.

Next we claim that the set $\mathfrak{N}(G)$ of normal subgroups of G forms a modular sublattice of $\mathfrak{L}(G)$. If M and N are normal subgroups of G, then MN is also normal, since for $g \in G$ we have

$$g(MN) = (gM)N = (Mg)N = M(gN) = M(Ng) = (MN)g.$$

Furthermore, the subgroup $M \cap N$ is also normal, since

$$g(M \cap N) = gM \cap gN = Mg \cap Ng = (M \cap N)g.$$

Hence $\mathfrak{N}(G)$ is indeed a sublattice. We showed above that every permutable (hence every normal) subgroup is modular, so $\mathfrak{N}(G)$ is modular.

Finally we provide some intuition for the definition of modularity in lattices. If $\mathfrak{L}$ is a lattice and $a, x, b \in \mathfrak{L}$ with $a \leq b$, we can 'project' x onto the up set $\uparrow a = \{y \in \mathfrak{L} \mid a \leq y\}$ by joining it with a, i.e. $a \vee x$. Afterwards we may

further project it onto the down set $\downarrow b = \{y \in \mathfrak{L} \mid y \leq b\}$ by meeting it with b, i.e. $(a \vee x) \wedge b$. Notice that since $a \leq b$, we still have $a \leq (a \vee x) \wedge b$. Hence we obtain a projection of x onto the interval

$$[a, b] = (\uparrow a) \cap (\downarrow b) = \{y \in \mathfrak{L} \mid a \leq y \leq b\}.$$

Dually we might have instead used the projection $a \vee (x \wedge b)$, i.e. reversing the order of the two projections. A lattice is modular just when these two projections always give the same result, so in some sense projection onto an interval only really makes sense in a modular lattice. ⌟

REMARK II.15: A 'rank-nullity theorem' for finite groups.
Let $\varphi\colon G \to H$ be a group homomorphism, where G is a finite group. This induces an isomorphism $\tilde{\varphi}\colon G/\ker\varphi \to \varphi(G)$. Hence

$$|G| = |\ker\varphi|\,[G : \ker\varphi] = |\ker\varphi|\,|\varphi(G)|.$$

In particular we see that the order of the image of φ, which is a subgroup of the *codomain*, divides the order of the *domain*. Compare the rank-nullity theorem from linear algebra:

$$\dim V = \dim\ker T + \dim T(V),$$

where $T\colon V \to W$ is a linear map. ⌟

REMARK II.16: Epimorphism ⇒ surjective.
Clearly, surjective homomorphisms are epimorphisms, but the converse is also true.

In Remark II.8 we showed that every subgroup of a group is an equaliser subgroup, and the above is an easy corollary: Let $\varphi\colon G \to H$ be an epimorphism in **Grp** (or in **FinGrp**, the argument is the same). Since $\varphi(G)$ is a subgroup of H, there are group homomorphisms $\psi_1, \psi_2\colon H \to K$ (where K is finite if we are working in **FinGrp**) such that $\varphi(G)$ is the equaliser subgroup of ψ_1 and ψ_2. But then $\psi_1 \circ \varphi = \psi_2 \circ \varphi$, and since φ is epic we have $\psi_1 = \psi_2$, so the two homomorphisms in fact agree on H. Hence $\varphi(G) = H$ and φ is surjective. ⌟

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 $1 \leq i, j \leq n$ 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 8.16

Generalize Fermat's little theorem to congruences modulo arbitrary (that is, possibly nonprime) integers.

SOLUTION. We prove *Euler's theorem*:

If n and a are coprime positive integers, then

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

The class $[a]_n$ lies in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ which has order $\varphi(n)$, so Lagrange's theorem implies that

$$[a]_n^{\varphi(n)} = [1]_n$$

as claimed.

We also have the following corollary:[8]

If n is a product of distinct primes and $a, v \in \mathbb{Z}$, then

$$a^{1+\varphi(n)v} \equiv a \pmod{n}. \tag{II.1}$$

If $n = p$ is a prime and $p \mid a$, then both sides are zero mod p. If instead a and p are coprime, then the claim follows from Euler's theorem (or Fermat's little theorem).

[8] This result allows us to solve congruences like $x^k \equiv b \bmod n$ if we know $\varphi(n)$, and k and $\varphi(n)$ are coprime. Bezout's identity (Exercise 2.13) furnishes $u, v \in \mathbb{Z}$ such that $ku + \varphi(n)v = 1$, which implies that

$$b^u \equiv x^{ku} = x^{1-\varphi(n)v} \equiv x \pmod{n}.$$

Notice that u is in fact a multiplicative inverse of k mod $\varphi(n)$; of course any such inverse will do.

Note also that the corollary does not hold (in general) without the assumption on n. For a prime p we have $\varphi(p^2) = p(p-1)$ which is even, say $\varphi(p^2) = 2k$. Thus

$$p^{1+\varphi(p^2)v} = p(p^2)^{kv} \equiv 0 \pmod{p^2}.$$

Next, if m and n are coprime and (II.1) holds as stated, as well as with n replaced by m, then by Exercise V.6.8 we have

$$a^{1+\varphi(mn)v} = a^{1+\varphi(m)\varphi(n)v} \equiv a \pmod{m},$$

and similarly mod n. Since m and n are coprime this also holds mod mn. The claim now follows by induction. □

Exercise 8.17

Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p.

Solution. We argue by induction in $|G|$. If $|G| = 1$ then $|G|$ has no prime divisors, hence the claim is trivial. Assume then that $|G| > 1$, and let $g \neq e$ be an element of G. We claim that the cyclic group $\langle g \rangle$ contains an element of prime order. Let q be a prime divisor of $|g|$ and write $|g| = qd$. The element g^d then has order

$$|g^d| = \frac{\operatorname{lcm}(|g|, d)}{d} = \frac{|g|}{d} = q$$

by Proposition 1.13 as claimed. If $q = p$ then we are done. If $q \neq p$ then let $H = \langle g^d \rangle$ and consider the quotient[9] G/H. This has order $|G|/q < |G|$, and since p divides $|G|/q$ it contains an element aH of order p by induction. By Proposition 4.1, $p = |aH|$ divides $|a|$, so write $|a| = pk$. Then a^k has order p as desired. □

Exercise 8.19

Let G be a finite group, and let d be a proper divisor of $|G|$. Is it necessarily true that there exists an element of G of order d? Give a proof or a counterexample.

Solution. The (abelian!) group $C_2 \times C_2 \times C_2$ is of order 8, but all its nontrivial elements are of order 2. □

Exercise 8.20

Assume G is a finite abelian group, and let d be a divisor of $|G|$. Prove that there exists a subgroup $H \subseteq G$ of order d.

Solution. We argue by induction in $|G|$. If $|G| = 1$ then this is obvious, so assume that $|G| > 1$ and let d be a divisor of $|G|$. If d is prime, then the claim follows directly from Exercise 8.17, so assume that d is composite and let $d = kp$ with p prime. Then there is an element $h \in G$ of order p by Exercise 8.17,

[9] Here we use that G is abelian, since then $\langle g^d \rangle$ is a normal subgroup.

and the quotient $G/\langle h\rangle$ has order $k < |G|$. Induction yields a subgroup of $G/\langle h\rangle$ of order k, and by Proposition 8.9 this subgroup is on the form $H/\langle h\rangle$ for some subgroup H of G. Finally notice that

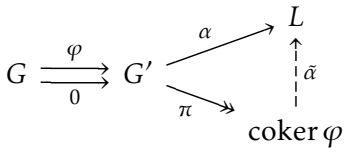
$$|H| = [H : \langle h\rangle]\,|h| = kp = d$$

as desired. □

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.17: *G*-sets in universal algebra.
Let $\sigma\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A)$ and $\tau\colon G \to \mathrm{Aut}_{\mathbf{Set}}(B)$ be group actions. The G-set structure on e.g. A may be captured by the algebra

$$\mathfrak{A} = \left\langle A, \langle \sigma_g \mid g \in G \rangle \right\rangle,$$

where $\sigma_g = \sigma(g)$. A homomorphism (i.e. a G-equivariant map) is then a map $\varphi\colon A \to B$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \sigma_g}\downarrow & & \downarrow{\scriptstyle \tau_g} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

commutes for all $g \in G$. This is of course equivalent to the diagram

$$\begin{array}{ccc} G \times A & \xrightarrow{\mathrm{id}_G \times \varphi} & G \times B \\ \downarrow & & \downarrow \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

where the vertical maps are the maps from Definition 9.2. ⌟

REMARK II.18. 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 $g_1^{-1} g_2 \in \mathrm{Stab}_G(a)$. Since $e_G \in \mathrm{Stab}_G(a)$ we see that $\sim$ agrees with the equivalence relation induced by $\mathrm{Stab}_G(a)$ 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

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

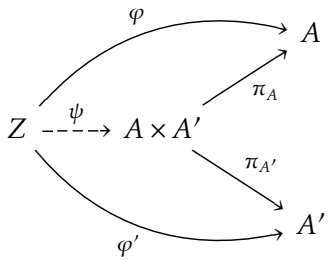
This is clearly also an automorphism. Thus $\langle\sigma,\sigma'\rangle$ is an action of G on $A\times A'$. For $g\in G$ we thus have $\langle\sigma,\sigma'\rangle(g) = \sigma(g)\times\sigma'(g)$, so $a\in A$ and $a'\in A'$ this is given explicitly by

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

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

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

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

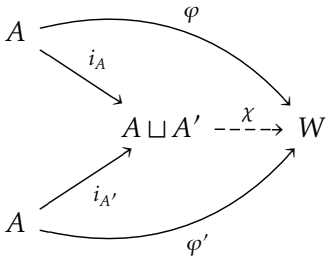
$$\begin{aligned}(\sigma \oplus \sigma')(gh)(a) &= \Big(\sigma(gh) \oplus \sigma'(gh)\Big)(a) = \sigma(gh)(a) = \sigma(g) \circ \sigma(h)(a) \\ &= \Big(\sigma(g) \oplus \sigma'(g)\Big) \circ \Big(\sigma(h) \oplus \sigma'(h)\Big)(a) \\ &= (\sigma \oplus \sigma')(g) \circ (\sigma \oplus \sigma')(h)(a),\end{aligned}$$

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 $A \sqcup A'$.

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 $\chi \colon A \sqcup A' \to W$ 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

REMARK III.1. Let $(R,+,\cdot)$ be a ring. The definition includes the hypothesis that $(R,+)$ be an *abelian* group, but if R has a multiplicative identity this is actually superfluous. The distributive laws imply that

$$(1+1)(r+s) = 1(r+s)+1(r+s) = r+s+r+s,$$

and that

$$(1+1)(r+s) = (1+1)r+(1+1)s = r+r+s+s,$$

and then cancellation implies that $r+s = s+r$. ⌟

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 $N - i \geq n$ (i.e., each term in the sum contains either a large power of a or of b), 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 $a + b$ is invertible and hence not nilpotent: indeed, $(a+b)^2$ is the identity matrix. □

EXERCISE 1.17

Explain in what sense $R[x]$ agrees with the monoid ring $R[\mathbb{N}]$.

SOLUTION. As a group, $R[\mathbb{N}]$ is just the direct sum $R^{\oplus\mathbb{N}}$ of the abelian groups $(R,+)$, which agrees with the definition of $R[x]$ as a group. As for the multiplication in $R[\mathbb{N}]$, this is given by

$$\left(\sum_{n\in\mathbb{N}} a_n \cdot n\right) \cdot \left(\sum_{n\in\mathbb{N}} b_n \cdot n\right) = \sum_{n\in\mathbb{N}} \sum_{n=n_1+n_2} (a_{n_1} b_{n_2}) \cdot n.$$

The multiplication in $R[x]$ is given by

$$\left(\sum_{n\in\mathbb{N}} a_n x^n\right) \cdot \left(\sum_{n\in\mathbb{N}} b_n x^n\right) = \sum_{n\in\mathbb{N}} \sum_{n=n_1+n_2} (a_{n_1} b_{n_2}) x^n,$$

which agrees with the multiplication on $R[\mathbb{N}]$ after substituting $n \to x^n$. □

III.2. The category **Ring**

REMARK III.2. Let S be a ring and $s \in S$. According to Example 2.2 there exists a unique ring homomorphism $\varphi\colon \mathbb{Z}[x] \to S$ that sends x to s. This is guaranteed by the proof of Proposition 2.1 as long as s commutes with every element in $\iota(\mathbb{Z})$, where $\iota\colon \mathbb{Z} \to S$ is the unique ring homomorphism. We claim that this is in fact the case:

The *set function* φ always exists. In order for it to be a ring homomorphism, notice that s indeed needs only commute with $\iota(\mathbb{Z})$, since the elements in $\varphi(\mathbb{Z}[x])$ are on the form

$$\varphi\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \sum_{n\in\mathbb{N}} \varphi(a_n)\varphi(x)^n = \sum_{n\in\mathbb{N}} \iota(a_n) s^n$$

for $a_n \in \mathbb{Z}$. 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

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

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

We can also give a more structural argument for this final claim based on Remark II.4: 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. ⌟

REMARK III.3: Naturality of $\mathbb{Z}$.

The *group* $\mathbb{Z}$ is first constructured as the free group on one generator. It turns out that this is abelian, so we may consider the set $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$. If $\varphi, \psi \colon \mathbb{Z} \to \mathbb{Z}$ are group homomorphisms, we may define $\varphi + \psi$ pointwise by

$$(\varphi + \psi)(n) = \varphi(n) + \psi(n),$$

which makes $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ itself into an abelian group. Composition of elements in $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ makes it into a monoid. To show that it is a ring, we check the distributive laws: First of all,

$$(\varphi + \psi) \circ \chi(n) = (\varphi + \psi)(\chi(n)) = \varphi(\chi(n)) + \psi(\chi(n)) = \varphi \circ \chi(n) + \psi \circ \chi(n).$$

Notice that we haven't used that the maps are group homomorphisms. Furthermore,

$$\chi \circ (\varphi + \psi)(n) = \chi(\varphi(n) + \psi(n)) = \chi(\varphi(n)) + \chi(\psi(n)) = \chi \circ \varphi(n) + \chi \circ \psi(n),$$

where the second equality uses that χ is a homomorphism. Hence $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ is a ring. Finally, Proposition 2.6 shows that $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$ equipped with the usual ring structure, showing that $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ is a commutative ring. But notice that we only use this isomorphism to show that $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ is commutative; its definition is entirely 'natural' and does not depend on the integers as such.

We may prove that $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$ as follows: For $a \in \mathbb{Z}$ define $\alpha_a \colon \mathbb{Z} \to \mathbb{Z}$ by $\alpha_a(n) = an$. This is clearly a group homomorhism. Then define $\psi \colon \mathbb{Z} \to \mathrm{End}_{\mathbf{Ab}}(\mathbb{Z})$ by $\psi(a) = \alpha_a$. Notice that

$$(\alpha_a + \alpha_b)(n) = \alpha_a(n) + \alpha_b(n) = an + bn = (a + b)n = \alpha_{a+b}(n)$$

and

$$(\alpha_a \circ \alpha_b)(n) = \alpha_a(\alpha_b(n)) = a(bn) = (ab)n = \alpha_{ab}(n),$$

showing that ψ is a ring homomorphism. Then define a map $\varphi \colon \mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Z}) \to \mathbb{Z}$ by $\varphi(\alpha) = \alpha(1)$. Notice that

$$(\varphi \circ \psi)(a) = \varphi(\alpha_a) = \alpha_a(1) = a,$$

and that

$$(\psi \circ \varphi)(\alpha) = \psi(\alpha(1)) = \alpha_{\alpha(1)},$$

and furthermore that $\alpha_{\alpha(1)}(n) = \alpha(1)n = \alpha(n)$ since α is a group homomorphism. Thus φ and ψ are inverses.

Aluffi instead proves that φ is a ring homomorphism, but it seems more natural to prove that ψ is instead. However, Proposition 2.7 is a generalisation of the above whose proof is identical. ⌟

REMARK III.4. We elaborate on the claim that Proposition 2.7 is a 'ring analogue' of Cauchy's theorem. The latter says that any group G acts faithfully on some set, namely itself by left multiplication. In other words, there is an injective group homomorphism

$$\sigma\colon G \to \mathrm{Aut}_{\mathbf{Set}}(G).$$

Notice that the automorphisms are on the *set* G. Since σ is injective we may identify G with a subgroup of $\mathrm{Aut}_{\mathbf{Set}}(G)$.

Similarly, we recall that if G is an abelian group, then $\mathrm{End}_{\mathbf{Ab}}(G)$ is a ring where the multiplication is given by function composition. The statement of Proposition 2.7 is that there is an injective ring homomorphism

$$\lambda\colon R \to \mathrm{End}_{\mathbf{Ab}}(R).$$

And just as $\sigma(g)$ is left-multiplication by $g \in G$ in the *group* G considered as a *set*, $\lambda(r) = \lambda_r$ is left-multiplication by $r \in R$ in the *ring* R considered as an *abelian group*. The fact that multiplication does not make R into a group is captured by the fact that λ maps R into the set of all endomorphisms of R, and not just the automorphisms.

We might view σ as providing a sort of 'prototype' for group actions: To obtain more general actions we consider group homomorphisms $\sigma\colon G \to \mathrm{Aut}_{\mathbf{Set}}(A)$, where A is *any* set. If we consider such a map σ as belonging to the set A, then we arrive at concept of *G-sets*. Transferring this interpretation to rings, we might contemplate actions $\lambda\colon R \to \mathrm{End}_{\mathbf{Ab}}(M)$ for any abelian group M. Similarly thinking of λ as belonging to the group M, this is precisely what defines an R-module structure on M (indeed, in analogy with G-**Set** we could have denoted the category of R-modules by R-**Ab** instead of R-**Mod**). ⌟

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:

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

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

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

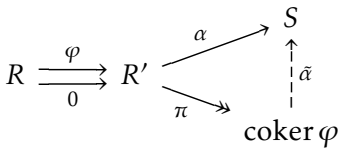
which proves the claim. □

EXERCISE 2.12

Consider the inclusion map $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. Describe the cokernel of ι in **Ab** and its cokernel in **Ring** (as defined by the appropriate universal property in the style of the one given in §II.8.6).

SOLUTION. In **Ab**, the cokernel of ι is the quotient $\mathbb{Q}/\mathbb{Z}$. This is (isomorphic to) the subgroup of the circle S^1 containing the results of rotations by $2\pi r$ radians for rational r. This is nontrivial, so ι is not an epimorphism (indeed it is clearly not surjective).

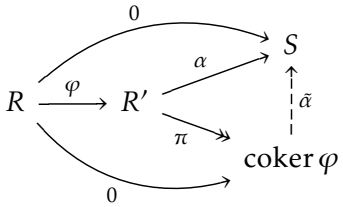
If $\varphi\colon R \to R'$ is a ring homomorphism, then a cokernel of φ would seem to be a ring $\operatorname{coker}\varphi$ along with a homomorphism $\pi\colon R' \to \operatorname{coker}\varphi$ such that, for any ring homomorphism $\alpha\colon R' \to S$ with $\alpha \circ \varphi = \alpha \circ 0$, there is a unique homomorphism $\tilde{\alpha}\colon \operatorname{coker}\varphi \to S$ such that the diagram



commutes, where 0 is a suitable (fixed) map, playing the role of the zero group homomorphism. In **Ring** it is not so clear what this map should be, since we cannot simply send everything to zero when R' is nontrivial. In other words, since there is no null object in **Ring**, there is no canonical way to get it to work using the language of (co)equalisers.

Using Aluffi's slightly different (but in **Grp** and **Ab** equivalent) definition of cokernels, we would instead require that π be initial with respect to homomorphisms $\alpha\colon R' \to S$ with $\alpha \circ \varphi = 0$. Then α should factor uniquely through

$\operatorname{coker}\varphi$:



Hence we must in particular have $\pi \circ \varphi = 0$, but the zero map is only a ring homomorphism if its codomain is zero, so $\operatorname{coker}\varphi = 0$. We see that the cokernel of *any* ring homomorphism is the zero ring, so there is no useful concept of cokernel in **Ring**. □

EXERCISE 2.15

For $m > 1$, the abelian groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ are manifestly isomorphic: the function $\varphi\colon \mathbb{Z} \to m\mathbb{Z}$, $n \mapsto mn$ is a group isomorphism. Use this isomorphism to transfer the structure of 'ring without identity' $(m\mathbb{Z}, +, \cdot)$ back onto $\mathbb{Z}$: give an explicit formula for the 'multiplication' $*$ this defines on $\mathbb{Z}$ (that is, such that $\varphi(a*b) = \varphi(a)\cdot\varphi(b)$). Explain why structures induced by different positive integers m are nonisomorphic as 'rings without 1'.

SOLUTION. We have

$$a * b = \varphi^{-1}\Big(\varphi(a)\cdot\varphi(b)\Big) = \varphi^{-1}(ma\cdot mb) = \varphi^{-1}\Big(\varphi(mab)\Big) = mab.$$

Let $m, n > 1$ and denote the multiplications by $*_m$ and $*_n$. If $\psi\colon (\mathbb{Z}, +, *_m) \to (\mathbb{Z}, +, *_n)$ is a homomorphism, then

$$m\cdot\psi(1) = \psi(1+\cdots+1) = \psi(m\cdot 1) = \psi(1 *_m 1) = \psi(1) *_n \psi(1) = n\cdot\psi(1)^2,$$

which is only possible if either $\psi \equiv 0$ or if $m = n\cdot\psi(1)$. In the latter case we have $n \mid m$, and ψ is multiplication by d, where $m = nd$. And

$$\psi(a *_m b) = d(a *_m b) = dmab = d^2nab = n\cdot\psi(a)\cdot\psi(b) = \psi(a) *_n \psi(b),$$

so ψ indeed preserves multiplication. Hence there is a nonzero homomorphism $(\mathbb{Z}, +, *_m) \to (\mathbb{Z}, +, *_n)$ if and only if $n \mid m$, in which case this is unique and is given by multiplication by $\frac{m}{n}$. In particular, this is an isomorphism if and only if $m = n$. □

EXERCISE 2.16

Prove that there is (up to isomorphism) only one structure of ring with identity on the abelian group $(\mathbb{Z}, +)$.

SOLUTION. Let R be a ring whose underlying abelian group is $\mathbb{Z}$. Consider the ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathbf{Ab}}(R)$ given by $\lambda(r) = \lambda_r$, which has the left-inverse $\varphi\colon \mathrm{End}_{\mathbf{Ab}}(R) \to R$ given by $\varphi(\alpha) = \alpha(1)$. Then φ is always a group homomorphism that preserves the identity. But in this case it is a true inverse of λ, since $(\lambda \circ \varphi)(\alpha) = \lambda_{\alpha(1)}$, and

$$\lambda_{\alpha(1)}(1) = \alpha(1) \cdot 1 = \alpha(1)$$

so since R's undelying abelian group is generated by 1 (and both $\lambda_{\alpha(1)}$ and α are group homomorphisms), we have $\lambda_{\alpha(1)} = \alpha$. □

EXERCISE 2.17

Let R be a ring. Prove that the center of $\mathrm{End}_{\mathbf{Ab}}(R)$ is isomorphic to a subring of the center of R.

SOLUTION. This is obvious since R is isomorphic to a subring of $\mathrm{End}_{\mathbf{Ab}}(R)$, and everything that commutes with all elements of a ring certainly commutes with all elements of a subring. □

EXERCISE 2.19

Prove that for $n \in \mathbb{Z}$ a positive integer, $\mathrm{End}_{\mathbf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as a ring.

SOLUTION. Since $\mathbb{Z}/n\mathbb{Z}$ is also cyclic, the argument in the case of $\mathbb{Z}$ carries over verbatim. □

III.3. Ideals and quotient rings

REMARK III.5: Ideals and homomorphisms.

The image or preimage of a *subring* under a ring homomorphism is a subring, but there is no reason (in universal algebra) to expect e.g. that the kernel of a homomorphism have any sort of special structure: Since a ring has two constants (i.e. nullary operations, namely 0 and 1), the subset $\{0\}$ is not generally a subring.

In the interpretation of an ideal I in a ring R as a subset capable of being 'set equal to zero', then there seems to be no reason to expect the image of an ideal to also be an ideal. For instance, $2\mathbb{Z}$ is an ideal in $\mathbb{Z}$, but the image $2\mathbb{Z}$ of the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is not an ideal in $\mathbb{Q}$, since forcing all even numbers to be zero in $\mathbb{Q}$ would also force many other numbers to be zero (indeed all numbers since $\mathbb{Q}$ is a field).

On the other hand, it seems more natural for kernels to be ideals. If a homomorphism φ annihilates elements a and b, then it should also annihilate all elements on the form $a+b$ or ra. If we extend the meaning of 'annihilate' to also allow φ to map elements into some ideal of its codomain, then it also seems natural enough for the preimage of any ideal to be an ideal. ⌟

REMARK III.6: Ideals in universal algebra.

One might wonder whether there is an algebraic theory of (say, left) ideals. If I is an ideal in a ring R, then I is in particular an abelian group $\langle I, +, -, 0\rangle$ under addition. Furthermore, for $a \in I$ and $r \in R$ we must have $ra \in I$, so each element r in R determines a unitary operation λ_r given by $\lambda_r(a) = ra$. Hence an ideal is an algebra

$$\mathfrak{I} = \left\langle I, +, -, 0, \langle \lambda_r \mid r \in R\rangle \right\rangle$$

satisfying the obvious identities, and further satisfying that $I \subseteq R$. We immediately notice that we are only able to construct an algebraic theory of ideals of a *fixed* ring. But this already defeats the purpose since we want a theory of *ideals* and not a theory of *ideals in R*.

However, if we allow I to be any set and not just a subset of R, then we arrive precisely at the theory of (left) R-modules. ⌟

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

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

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) Let $\iota\colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Then $\iota(n\mathbb{Z}) = n\mathbb{Z}$, but this is clearly not an ideal in $\mathbb{Q}$.

(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 3.5

Let J be a *two-sided* ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R. Prove that a matrix $A \in \mathcal{M}_n(R)$ belongs to J if and only if the matrices obtained by placing any entry of A in any position, and 0 elsewhere, belong to J.

SOLUTION. Let $E_{ij} \in \mathcal{M}_n(R)$ denote the matrix with $(E_{ij})_{kl} = \delta_{ik}\delta_{jl}$, i.e. the matrix with a 1 in the (i,j)-th entry and 0 elsewhere. For $A = (a_{ij}) \in \mathcal{M}_n(R)$ we then have

$$E_{ij}AE_{kl} = a_{jk}E_{il}.$$

The matrix on the right-hand side is precisely of the type described, and every matrix such described can we written on this form. If $A \in J$, then since J is a two-sided ideal, all matrices on the form $a_{jk}E_{il}$ also lie in J. Since A is a sum of matrices on this form, the converse also holds. This proves the claim. □

EXERCISE 3.6

Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R, and let $I \subseteq R$ be the set of $(1,1)$ entries of matrices in J. Prove that I is a two-sided ideal of R and J consists precisely of those matrices whose entries all belong to I.

SOLUTION. Let $a \in I$ and $r \in R$. Then a is the $(1,1)$-th entry of some matrix in J. By Exercise 3.5 the matrix aE_{11} also belongs to J, and hence so does the product $(aE_{11})(rE_{11}) = arE_{11}$ since J is an ideal. Thus $ar \in I$, and we similarly find that $ra \in I$, so I is a two-sided ideal.

If $A = (a_{ij}) \in \mathcal{M}_n(R)$ is a matrix whose entries all belong to I, then the matrices $a_{ij}E_{11}$ all lie in J. By Exercise 3.5 so do the matrices $a_{ij}E_{ij}$, and since A is a sum of these matrices we also have $A \in J$. Conversely, if $A = (a_{ij}) \in J$, then also $a_{ij}E_{11} \in J$ by Exercise 3.5. But then $a_{ij} \in I$. □

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 R are its only (left- or right-) 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 of course $r_1 = r_2$). □

Exercise 3.9

Counterpoint to Exercise 3.8: It is *not* true that a (nonzero) ring R is a division ring if and only if its only two-sided ideals are $\{0\}$ and R. A nonzero ring with this property is said to be *simple*; by Exercise 3.8, fields are the only simple *commutative* rings.

Prove that $\mathcal{M}_n(\mathbb{R})$ is simple.

Solution. Let $J \neq (0)$ be a two-sided ideal of $\mathcal{M}_n(\mathbb{R})$, and let I be the set of $(1,1)$-th entries of matrices in J. Since $J \neq (0)$ there is a matrix in J with a nonzero entry. By Exercise 3.5 there is then matrix in J with a nonzero $(1,1)$-th entry, so I contains this element, and $I \neq (0)$.

By Exercise 3.6, I is an ideal in $\mathbb{R}$, and since $\mathbb{R}$ is a field we must have $I = (1)$. Again by Exercise 3.6, J must contain all matrices in $\mathcal{M}_n(\mathbb{R})$, so $J = (1)$. Thus $\mathcal{M}_n(\mathbb{R})$ is simple.

Notice that we only use the fact that $\mathbb{R}$ is a field, so the same argument shows that $\mathcal{M}_n(k)$ is simple for any field k. □

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.

Alternatively, since R is nonzero φ is nontrivial, $\ker \varphi \neq R$. And $\ker \varphi$ is an ideal in k, so $\ker \varphi = \{0\}$ by Exercise 3.8. □

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

REMARK III.7: Polynomial division.

Let R be a nonzero ring. We prove the following result:

Let $f(x), g(x) \in R[x]$ with $f(x)$ monic. There exist polynomials $q(x), r(x) \in R[x]$ with $\deg r(x) < \deg f(x)$ such that

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

Furthermore, Lemma 4.5 shows that $q(x)$ and $r(x)$ are uniquely determined.

Let $d = \deg f(x)$ and assume that $g(x) = ax^n$ with $a \neq 0$. If $n < d$ then $q(x) = 0$ and $r(x) = g(x)$ work. If instead $n \geq d$, then we have

$$ax^n = ax^{n-d} f(x) + \left(ax^n - ax^{n-d} f(x)\right),$$

and the latter polynomial has degree strictly less than d. By induction we may thus perform division when $g(x)$ is a monomial. The claim for general $g(x)$ follows by linearity. ⌟

REMARK III.8: Fields and maximal ideals.

If R is a commutative ring and $I \subseteq R$ is any subset, we know that it makes sense to consider the quotient ring R/I only when I is an ideal. By taking the quotient with I we are effectively forcing every element of I to be zero, and only these elements to be zero. First of all we must then have $0 \in I$, and I must also be closed under addition since $0 + 0 = 0$. Clearly $-0 = 0$, so each element in I must also have an additive inverse. Thus I is a group.

Furthermore, multiplication of any element in R by zero must again yield zero, so I must be closed under multiplication with any element in R. This is precisely the definition of an ideal.

When is it possible to force an element to be zero? If we force a unit u to be zero, then we would intuitively have $1 = uu^{-1} = 0u^{-1} = 0$. If we don't want to end up with the zero ring, then we cannot force units to be zero. In a field every non-zero element is a unit, so fields cannot have any non-trivial ideals.

Put another way: We *can* force non-units to be zero. By doing this we first of all eliminate some of the non-units entirely, and some of the non-units may become units. For instance, in $\mathbb{Z}$ the number 2 is not a unit, but in $\mathbb{Z}/3\mathbb{Z}$ the corresponding class $[2]_3$ *is* a unit since $[2]_3[2]_3 = [4]_3 = [1]_3$. The idea is that by collapsing the ideal I to zero, we are forced to identify a bunch of other elements if their difference lies in I. Hence many elements in the original ring R may correspond to the identity 1 after collapsing I to zero, and so it is easier for a product to equal 1.

Let I be a maximal ideal. Then we are not able to force any more elements to be zero without reducing R to the zero ring. Hence R/I in some sense contains the minimal number of non-units. Indeed, if R/I contained *any* non-units whatsoever, say the element r, then taking the quotient by (r) removes even more non-units. But we had already removed the maximal amount of non-units, so this is impossible. Hence R/I cannot contain any non-units and is thus a field. ⌟

REMARK III.9: Lattice of ideals.

Let R be a ring. Since $(R,+)$ is a (commutative) group we may consider its lattice $\mathfrak{L}(R)$ of subgroups. If H and K are subgroups of $(R,+)$, then their join and meet in $\mathfrak{L}(R)$ are $H+K$ (in additive notation) and $H\cap K$ respectively. If I and J are ideals in R, then they are in particular subgroups, and it is easy to check that $I+J$ and $I\cap J$ are also ideals. Hence the subset $\mathfrak{I}(R)\subseteq\mathfrak{L}(R)$ of ideals is in fact a sublattice.

In groups we only have one operation with which to combine subgroups. In a ring we have an addition, used above to define $I+J$, but we also have a multiplication: We define the product of the ideals I and J in R by

$$IJ = (I\cdot J) = (ij \mid i\in I, j\in J),$$

i.e., IJ is the ideal generated by products ij for $i\in I$ and $j\in J$. Notice that $IJ\subseteq I\cap J$, but that I and J do not generally lie in IJ. We give a series of properties of the product of ideals:

(a) If R is commutative and $a,b\in R$, then $(a)(b)=(ab)$. Clearly $ab\in(a)(b)$ so $(ab)\subseteq(a)(b)$, and for the opposite inclusion notice that

$$\sum_{i=1}^{n}(r_i a)(s_i b) = ab\sum_{i=1}^{n} r_i s_i \in (ab),$$

so $(a)(b)\subseteq(ab)$.

In $\mathbb{Z}$ we have $(a)\cap(b)=(\operatorname{lcm}(a,b))$, so here $(a)(b)=(a)\cap(b)$ just when a and b are relatively prime.

(b) If R is a PID, then of course $(a)(b)=(c)$ for some c, but as far as I know there is no general relation between a,b,c. ⌟

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 subgroups or -rings.[10]

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

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

[10] Note that while for subalgebras this can be proven generally in universal algebra, we need a separate proof for ideals.

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 $IJ = I \cap J$.

Ideals I and J in a (not necessarily commutative) ring R are said to be *comaximal* if $I + J = R$. A set $\mathcal{I}$ of ideals in R is called *(pairwise) comaximal* if I and J are comaximal for all distinct $I, J \in \mathcal{I}$.

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

$$f_i(x) = (x - a)q_i(x) + r_i$$

for some $q_i(x) \in R[x]$ and $r_i \in R$. Evaluating in $x = a$ we find that $r_i = f_i(a)$, 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 the identity on the 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. (Strictly speaking the ideal in the denominator of the middle quotient is the one generated by equivalence classes $f_i(a) + (x-a)$. The isomorphism $R[x]/(x-a) \to R$ is evaluation at $x = a$, so this sends $f_i(a) + (x-a)$ to $f_i(a)$, so the second isomorphism holds.) □

Exercise 4.12

Let R be a commutative ring and $a_1,\dots,a_n$ elements of R. Prove that

$$\frac{R[x_1,\dots,x_n]}{(x_1-a_1,\dots,x_n-a_n)} \cong R.$$

Solution. By Exercise 4.11 we have

$$\frac{R[x_1,\dots,x_n]}{(x_1-a_1,\dots,x_n-a_n)} \cong \frac{R[x_1,\dots,x_{n-1}][x_n]}{(x_1-a_1,\dots,x_n-a_n)} \cong \frac{R[x_1,\dots,x_{n-1}]}{(x_1-a_1,\dots,x_{n-1}-a_{n-1})},$$

and repeating this $n-1$ times yields the claim. □

Exercise 4.13

Let R be an integral domain. For all $k = 1,\dots,n$ prove that $(x_1,\dots,x_k)$ is prime in $R[x_1,\dots,x_n]$.

Solution. By Exercise 4.12 we have

$$\frac{R[x_1,\dots,x_n]}{(x_1,\dots,x_k)} \cong \frac{R[x_{k+1},\dots,x_n][x_1,\dots,x_k]}{(x_1,\dots,x_k)} \cong R[x_{k+1},\dots,x_n],$$

which is an integral domain. Hence $(x_1,\dots,x_k)$ is by definition prime. □

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 $P \supseteq \bigcap_{j=1}^{\infty} I_j$, then P contains one of the ideals I_j.

SOLUTION. (i) If at least one of the ideals $I_2, \ldots, I_r$ are contained in P, then we are done, so assume that neither of them are. Thus there exist $i_2 \in I_2, \ldots, i_r \in I_r$, 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 $i_1, \ldots, i_r$ lie in P. But none of the elements $i_2, \ldots, i_r$ do, so we must have $i_1 \in P$. Hence $I_1 \subseteq P$.

(ii) We give a counterexample. Notice that

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

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

EXERCISE 4.20

Let M be a two-sided ideal in a (not necessarily commutative) ring R. Prove that M is maximal if and only if R/M is a simple ring (cf. Exercise 3.9).

SOLUTION. Aluffi does not provide a definition of maximal ideals in noncommutative rings, so we give one: We say that a two-sided ideal $I \neq (1)$ of a ring R is *maximal* if, for every two-sided ideal $J \subseteq R$, $I \subseteq J$ implies that either $I = J$ or $J = R$. In other words, I is maximal with respect to set inclusion among all proper two-sided ideals of R.

With this definition, the claim follows as in the proof of Proposition 4.11 from the one-to-one correspondence, preserving inclusion, between ideals of R/M and ideals of R containing M. □

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 $f(x) \in J \setminus I$. 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 $J = k[x]$.

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 $f(r) = 0$, and so $x - r$ divides $f(x)$. 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 $I = \mathbb{R}[x]$.

Alternatively, Example 4.8 shows that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ which is a field, in particular a simple ring. But then either Proposition 4.11 or Exercise 4.20 implies that (x^2+1) is maximal. □

III.5. Modules over a ring

REMARK III.10: Modules in universal algebra.
Let R be a fixed ring. A (left) R-module is an algebra

$$\mathfrak{M} = \left\langle M, +, -, 0, \langle \lambda_r \mid r \in R \rangle \right\rangle$$

such that $\langle M, +, -, 0 \rangle$ is an abelian group, each λ_r is a unitary operation, and which satisfies the usual identities. Hence, an R-module homomorphism $\varphi\colon \mathfrak{M} \to \mathfrak{N}$ (where $\mathfrak{N}$ has underlying set N) is a homomorphism of the underlying abelian groups, for which the diagrams

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle \lambda_r^{\mathfrak{M}}}\downarrow & & \downarrow{\scriptstyle \lambda_r^{\mathfrak{N}}} \\ M & \xrightarrow[\varphi]{} & N \end{array}$$

commute for all $r \in R$. ⌟

REMARK III.11: *R*-algebras.

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. ⌟

REMARK III.12: The category of R-algebras.

Above we saw two ways of thinking of algebras over a commutative ring R. In fact we have at least four ways of thinking about R-algebras:

(a) An R-algebra is a ring homomorphism $\alpha\colon R \to S$ whose image $\alpha(R)$ lies in the centre of S. This (even without this latter assumption) induces a module structure on S given by $\lambda \circ \alpha$, where λ is left-multiplication in S. Hence an R-algebra is a ring equipped with an R-action.

(b) An R-algebra is simultaneously an R-module and a ring, and the two structures are compatible: The ring addition and the module addition coincide, and the R-action commutes with the ring multiplication. The latter precisely corresponds to the above requirement that $\alpha(R)$ lie in the centre of S.

(c) We may also consider R-algebras as algebraic structures in the sense of universal algebra. Thus an R-algebra is a structure

$$\mathfrak{S} = \Big\langle S, +, \cdot, -, 0, \langle \lambda_r \mid r \in R\rangle \Big\rangle,$$

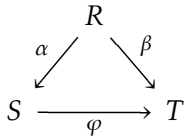
such that $\langle S, +, \cdot, -, 0\rangle$ is a ring, $\langle S, +, -, 0, \langle \lambda_r \mid r \in R\rangle\rangle$ is an R-module, and which satisfies the laws

$$\lambda_r(s) \cdot s' = \lambda_r(s \cdot s') = s \cdot \lambda_r(s')$$

for all $r \in R$. This is essentially the same as the above.

(d) Finally we may construct the category R-**Alg** of R-algebras more categorically and see that we recover the above definition. Indeed we may define this category as the subcategory of the coslice category R/**Ring** whose objects (which are homomorphisms in **Ring**) have the property that their image lies in the centre of their codomain.

More explicitly, an object in R-**Alg** is a ring homomorphism $\alpha\colon R \to S$ such that $\alpha(R)$ lies in the centre of S, and an arrow from α to $\beta\colon R \to T$ in R-**Alg** is a commutative diagram



in **Ring**. Since φ is a ring homomorphism, this means that

$$\varphi(rs) = \varphi(\alpha(r)s) = \varphi(\alpha(r))\varphi(s) = \beta(r)\varphi(s) = r\varphi(s).$$

Hence φ respects the module structures on S and T. Conversely, if $\varphi\colon S \to T$ respects both the ring and module structures on S and T, then

$$\varphi(\alpha(r))\varphi(s) = \varphi(\alpha(r)s) = \varphi(rs) = r\varphi(s) = \beta(r)\varphi(s),$$

and letting $s = 1_S$ yields $\varphi \circ \alpha = \beta$. Hence this definition of R-**Alg** is equivalent to the ones above.

Furthermore, since R is already assumed commutative, the category of *commutative* R-algebras may simply be defined as the coslice category $R/\mathbf{CRing}$. ⌟

REMARK III.13: Every ring is a $\mathbb{Z}$-algebra.
Just as every abelian group is a $\mathbb{Z}$-module, every ring R is a $\mathbb{Z}$-algebra in a unique way: First of all, there is a unique ring homomorphism $\iota\colon \mathbb{Z} \to R$. Thus we only need to verify that $\iota(\mathbb{Z})$ lies in the centre of R. But this is clear since the centre $Z(R)$ of R is a subring (of course containing 1_R), so

$$\iota(\mathbb{Z}) = \iota(\langle 1\rangle) = \langle \iota(1)\rangle = \langle 1_R\rangle \subseteq Z(R).$$

Hence the categories **Ring** and $\mathbb{Z}$-**Alg** are the same. ⌟

REMARK III.14. In §5.2 we see that $\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(M,N)$ is itself an R-module if R is commutative. In fact, for any ring R and any set A the set of functions N^A is a module with operations defined pointwise (recall from §II.4.4 that H^A is a group if H is a *commutative* group, which is also the case here). Of course we may then restrict to module homomorphisms $M \to N$, but it is only when R is commutative that this class is closed under scalar multiplication. ⌟

EXERCISE 5.4

Let R be a ring. A nonzero R-module M is *simple* (or *irreducible*) if its only submodules are $\{0\}$ and M. Let M,N be simple modules, and let $\varphi\colon M \to N$ be a homomorphism of R-modules. Prove that either $\varphi = 0$ or φ is an isomorphism.

SOLUTION. Assume that $\varphi \neq 0$. The image of φ is a submodule of N, but since $\varphi \neq 0$ it cannot be $\{0\}$. Hence it must be N, so φ is surjective. Similarly, the kernel of φ is a submodule of N, but since $\varphi \neq 0$ it cannot be M. Thus it must be $\{0\}$, so φ is injective. In total, φ is bijective hence an isomorphism. □

EXERCISE 5.5

Let R be a commutative 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.

Recall (cf. §5.3) that if M and N are modules over a (not necessarily commutative) ring R, then $\mathrm{Hom}_{R\text{-}\mathbf{Mod}}(M,N)$ is an abelian group, but that we need R to be commutative for this to also be a module in general.

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 $\beta(m) = \beta_m$. This is also a module homomorphism: For $m, m' \in M$ and $r, s \in R$ we have

$$\beta(rm+m')(s) = \beta_{rm+m'}(s) = s(rm+m') = r(sm) + sm' = (r\beta(m) + \beta(m'))(s),$$

so $\beta(rm+m') = r\beta(m) + \beta(m')$.

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

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

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**.

More simply put, each homomorphism $R \to M$ is multiplication by m for some $m \in M$. □

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 $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$. □

EXERCISE 5.11

Let R be a commutative ring, and let M be an R-module. Prove that there is a bijection between the set of $R[x]$-module structures (extending the given R-module structure) on M and $\mathrm{End}_{R\text{-}\mathbf{Mod}}(M)$.

This result says that, given an R-module structure on M, the only thing needed to extend this to an $R[x]$-module structure is to fix what the action of x is. If we think of $R[x]$ the ring generated by R along with an element x, it makes sense that the $R[x]$-module structure should be 'generated' by R and some endomorphism of M (respecting the R-module structure, it turns out).

SOLUTION. The R-module structure on M is a ring homomorphism

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

Given an R-module homomorphism $\varphi\colon M \to M$, it is easy to see that $\varphi \circ \sigma(r) = \sigma(r) \circ \varphi$ for all $r \in R$. Example 2.3 then yields a unique ring homomorphism

$$\overline{\sigma}\colon R[x] \to \mathrm{End}_{\mathbf{Ab}}(M)$$

extending σ and sending x to φ, i.e. an $R[x]$-module structure on M extending the given R-module structure σ. This defines a map

$$\Phi\colon \mathrm{End}_{R\text{-}\mathbf{Mod}}(M) \to \mathrm{Hom}_{\mathbf{Ring}}(R[x], \mathrm{End}_{\mathbf{Ab}}(M))$$

sending σ to $\overline{\sigma}$, and by the uniqueness above Φ is injective.

Conversely, let $\tau\colon R[x] \to \mathrm{End}_{\mathbf{Ab}}(M)$ be an $R[x]$-module structure on M extending σ. Then $\varphi = \tau(x)\colon M \to M$ is a ring homomorphism, and we claim that it is in fact an R-module homomorphism. For[11] $rx = xr$ in $R[x]$ for all $r \in R$, so since τ is a ring homomorphism we have

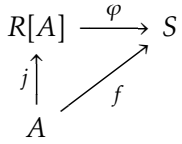
$$\tau(r) \circ \varphi = \tau(rx) = \tau(xr) = \varphi \circ \tau(r).$$

But then $\tau = \Phi(\varphi)$ by the uniqueness of $\overline{\sigma}$ above, so Φ is also surjective, hence a bijection as claimed. □

*III.6. Products, coproducts, etc., in R-***Mod**

REMARK III.15: Free commutative R-algebras.

In the proof of Proposition 6.4, Aluffi proves that, given a commutative R-algebra S and a set function $f\colon A \to S$ from a finite set $A = \{1, \dots, n\}$, there exists a unique *ring homomorphism* $\varphi\colon R[A] \to S$ such that the diagram



commutes. He then claims that φ is automatically an R-module homomorphism. Indeed, Aluffi constructs φ by extending the structure $\alpha\colon R \to S$ making S an R-algebra, and thus it is in fact an R-module homomorphism: Denoting the R-algebra structure on $R[A]$ by $\iota\colon R \to R[A]$ we find that

$$\varphi(rm) = \varphi(\iota(r)m) = \varphi(\iota(r))\varphi(m) = \alpha(r)\varphi(m) = r\varphi(m)$$

for $r \in R$ and $m \in R[A]$. Here we use that φ is a ring homomorphism, and that $\varphi \circ \iota = \alpha$ since φ extends α.

[11] The expression rx denotes the product in $R[x]$ of the polynomials r and x, and similarly for xr.

However, this only shows that φ is unique among R-algebra homomorphisms that extend α. If $\psi\colon R[A] \to S$ is any R-algebra homomorphism we have

$$\psi(r) = \psi(\iota(r)1_{R[A]}) = \psi(\iota(r))\psi(1_{R[A]}) = \alpha(r),$$

now using that $\psi \circ \iota = \alpha$ since ψ is an R-algebra homomorphism. But then we see that ψ must extend α, and so φ above is indeed unique. ⌟

EXERCISE 6.3

Let R be a ring, M an R-module, and $p\colon M \to M$ an R-module homomorphism such that $p^2 = p$. (Such a map is called a *projection*.) Prove that $M = \ker p \oplus \operatorname{im} p$.

SOLUTION. Consider the map

$$[i_{\ker p}, i_{\operatorname{im} p}]\colon \ker p \oplus \operatorname{im} p \to M,$$
$$(n, m) \mapsto n + m,$$

i.e. the coproduct map of the inclusions $i_{\ker p}$ and $i_{\operatorname{im} p}$ into M. This has the inverse $m \mapsto (m - p(m), p(m))$, hence is an isomorphism. □

EXERCISE 6.4

Let R be a ring, and let $n > 1$. View $R^{\oplus(n-1)}$ as a submodule of $R^{\oplus n}$, via the injective homomorphism $R^{\oplus(n-1)} \hookrightarrow R^{\oplus n}$ defined by

$$(r_1, \ldots, r_{n-1}) \mapsto (r_1, \ldots, r_{n-1}, 0)$$

Give a one-line proof that

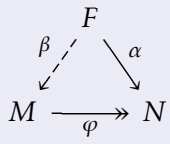
$$\frac{R^{\oplus n}}{R^{\oplus(n-1)}} \cong R.$$

SOLUTION. This follows from the first isomorphism theorem since the projection $\pi_n\colon R^{\oplus n} \to R$ given by $\pi_n(r_1, \ldots, r_n) = r_n$ is surjective and has kernel $R^{\oplus(n-1)}$. □

EXERCISE 6.9

Let R be a ring, F a nonzero free R-module, and let $\varphi\colon M \to N$ be a homomorphism of R-modules. Prove that φ is onto if and only if for all R-module homomorphisms $\alpha\colon F \to N$ there exists an R-module homomorphism

$\beta\colon F \to M$ such that $\alpha = \varphi \circ \beta$:



(Free modules are *projective*, as we will see in Chapter VIII. See also Remark III.17.)

SOLUTION. Say that $F = F^R(A)$ for a nonempty set A. Assume first that φ is surjective, and let $\alpha\colon F \to N$ be a homomorphism. For each $n \in \operatorname{im}\alpha$, choose some $m_n \in \varphi^{-1}(\{n\})$, and let $A_n = \alpha^{-1}(\{n\})$. Notice that the sets A_n constitute a partition of A. Then define a set function $f\colon A \to M$ by $f(a) = m_n$ for $a \in A_n$. This extends to a homomorphism $\beta\colon F \to M$. Then notice that, for $a \in A_n$,

$$\varphi(\beta(a)) = \varphi(f(a)) = \varphi(m_n) = n = \alpha(a),$$

so $\varphi \circ \beta$ and α agree on A, hence on F by the uniqueness part of the universal property of F.

Conversely, let $n \in N$ and define a set function $g\colon A \to N$ by $g(a) = n$ for all $a \in A$. By the universal property of F there exists an R-module homomorphism $\alpha\colon F \to N$ extending g. Then there further exists a homomorphism $\beta\colon F \to M$ such that $\alpha = \varphi \circ \beta$, so n lies in the image of φ. Since n was arbitrary, this shows that φ is surjective. □

EXERCISE 6.13

Prove that every homomorphic image of a finitely generated module is finitely generated.

SOLUTION. Let M be a finitely generated R-module, and let $\varphi\colon M \to N$ be a homomorphism. We may assume that φ is surjective. Since M is finitely generated, there is an $n \in \mathbb{N}$ and a surjective homomorphism $R^{\oplus n} \twoheadrightarrow M$. Composing this with φ yields a surjective homomorphism $R^{\oplus n} \twoheadrightarrow N$, so N is also finitely generated. □

EXERCISE 6.14

Prove that the ideal $(x_1, x_2, \ldots)$ of the ring $R = \mathbb{Z}[x_1, x_2, \ldots]$ is not finitely generated (as an ideal, i.e., as an R-module).

SOLUTION. Let A be a finite subset of R that generates a module contained in $(x_1, x_2, \ldots)$. In particular, A cannot contain 1. Furthermore, since A is finite

and each element of A is a polynomial, there is a largest $n \in \mathbb{N}$ such that x_n appears in a polynomial in A. Then it is clear that $x_{n+1} \notin (x_1, x_2, \ldots)$ since $1 \notin A$. □

EXERCISE 6.18

Let M be an R-module, and let N be a submodule of M. Prove that if N and M/N are both finitely generated, then M is finitely generated.

SOLUTION. Choose $a_1, \ldots, a_m, b_1, \ldots, a_n \in M$ such that

$$\frac{M}{N} = \langle a_1 + N, \ldots, a_m + N \rangle \quad \text{and} \quad N = \langle b_1, \ldots, b_n \rangle.$$

For $m \in M$ we thus have

$$m + N = \sum_{i=1}^{m} r_i(a_i + N) = \sum_{i=1}^{m} r_i a_i + N,$$

so $m - \sum_{i=1}^{m} r_i a_i \in N$. Hence

$$m = \sum_{i=1}^{m} r_i a_i + \sum_{j=1}^{n} s_i b_i,$$

so $M = \langle a_1, \ldots, a_m, b_1, \ldots, a_n \rangle$. □

III.7. Complexes and homology

REMARK III.16: Split exact sequences.
If

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0 \tag{III.2}$$

is exact, then $L \cong \ker \beta$ and $N \cong \operatorname{coker} \alpha$. On the other hand we may immediately extend the exact sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M,$$

which precisely says that α is injective, to the exact sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M \longrightarrow \operatorname{coker} \alpha \longrightarrow 0.$$

These then carry exactly the same information, assuming that α is injective. But this extended sequence also allows us to talk about splitting, so we have ways of characterising both monomorphisms and split monomorphisms using short exact sequences. Of course we may do similarly with epimorphisms.

Since any sequence on the form (III.2) is isomorphic to one on the form

$$0 \longrightarrow \ker\beta \xrightarrow{\alpha} M \xrightarrow{\beta} \operatorname{coker}\alpha \longrightarrow 0,$$

the content of Proposition 7.5 is in fact that this splits iff α has a left-inverse iff β has a right-inverse. ⌟

REMARK III.17: Projective modules.
In any category $\mathcal{C}$, an object P is said to be *projective* if, given an epimorphism $e\colon A \twoheadrightarrow B$, for any arrow $f\colon P \to B$ there is an arrow $\overline{f}\colon P \to A$ such that $f = e \circ \overline{f}$, i.e. such that the diagram

$$\begin{array}{ccc} & & P \\ & \overset{\overline{f}}{\swarrow} & \downarrow{\scriptstyle f} \\ A & \xrightarrow[e]{} & B \end{array}$$

commutes. Note that $\overline{f}$ is not required to be unique; this is not a universal property of P. In particular, if $B = P$ then e has a right-inverse, namely $\overline{1}_A$.

In R-**Mod**, the following are equivalent for an R-module P:

(a) P is projective in R-**Mod**.

(b) Every short exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

splits.

(c) P is a direct summand of a free module, i.e. there exist R-modules F and Q, with F free, such that $F \cong P \oplus Q$.

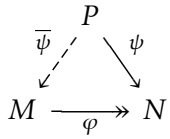
(a) ⇒ (b): By Proposition 7.5, the sequence above splits happens exactly when the homomorphism $\beta\colon N \to P$ has a right-inverse. But since β is an epimorphism, we noted above that it has a right-inverse when P is projective.

(b) ⇒ (c): Next assume that any such sequence splits. Consider the free module $R^{\oplus P}$ and the surjection $\varphi\colon R^{\oplus P} \to P$ induced by the set function id_P. As in Remark III.16 this gives rise to the short exact sequence

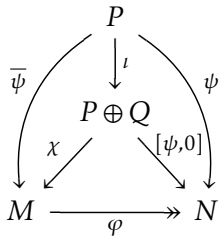
$$0 \longrightarrow \ker\varphi \longrightarrow R^{\oplus P} \xrightarrow{\varphi} P \longrightarrow 0,$$

and this splits by assumption, so $R^{\oplus P} \cong P \oplus \ker\varphi$.

(c) ⇒ (a): Finally assume that $F \cong P \oplus Q$, let $\varphi\colon M \to N$ be an epimorphism, and let $\psi\colon P \to N$ be any homomorphism. We must then find a $\overline{\psi}\colon P \to M$ so that the diagram



commutes. Since F is free it is projective by Exercise 6.9, so there is a homomorphism $\chi\colon P \oplus Q \to M$ such that $\varphi \circ \chi$ equals the coproduct map $[\psi, 0]$, where $0\colon Q \to N$ is the zero homomorphism (though any homomorphism will do). Letting $\iota\colon P \to P \oplus Q$ be the canonical injection and putting $\overline{\psi} = \chi \circ \iota$, notice that the diagram



commutes, so $\varphi \circ \overline{\psi} = \psi$ as desired. ⌟

EXERCISE 7.1

Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong 0$.

SOLUTION. The kernel of the map $M \to 0$ is M itself, and this equals the image of the map $0 \to M$. Hence M must be zero. □

EXERCISE 7.2

Assume that the complex

$$\cdots \longrightarrow 0 \xrightarrow{\alpha} M \xrightarrow{\varphi} M' \xrightarrow{\beta} 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong M'$

SOLUTION. We have $\ker\varphi = \operatorname{im}\alpha = 0$, so φ is injective. We further have $\operatorname{im}\varphi = \ker\beta = M'$ since β is trivial, so φ is surjective.

Alternatively we may simply apply Examples 7.1 and 7.2. □

EXERCISE 7.3

Assume that the complex

$$\cdots \longrightarrow 0 \xrightarrow{\alpha} L \xrightarrow{\beta} M \xrightarrow{\varphi} M' \xrightarrow{\gamma} N \xrightarrow{\delta} 0 \longrightarrow \cdots$$

is exact. Show that, up to natural identifications, $L = \ker\varphi$ and $N = \operatorname{coker}\varphi$.

SOLUTION. Notice that $\ker\beta = \operatorname{im}\alpha = 0$, so $L \cong \operatorname{im}\beta = \ker\varphi$. Furthermore, $\operatorname{im}\gamma = \ker\delta = N$, and

$$N = \operatorname{im}\gamma \cong \frac{M'}{\ker\gamma} = \frac{M'}{\operatorname{im}\varphi} = \operatorname{coker}\varphi. \qquad \square$$

EXERCISE 7.5

Assume that the complex

$$\cdots \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow \cdots$$

is exact and that L and N are Noetherian. Prove that M is Noetherian.

SOLUTION. The discussion in §7.1 shows that $N \cong M/L$, so this follows directly from Proposition 6.7. $\square$

EXERCISE 7.7

Let

$$0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$$

be a short exact sequence of R-modules, and let L be an R-module.

(a) Prove that there is an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(P,L) \longrightarrow \operatorname{Hom}_R(N,L) \longrightarrow \operatorname{Hom}_R(M,L)$$

of R-modules if R is commutative, and of abelian groups otherwise.

(b) TODO

(c) TODO

(d) Show that if the original sequence splits, then the rightmost homomorphism in (i) is onto.

SOLUTION. (a) We claim that the sequence

$$0 \longrightarrow \operatorname{Hom}_R(P,L) \xrightarrow{\beta^*} \operatorname{Hom}_R(N,L) \xrightarrow{\alpha^*} \operatorname{Hom}_R(M,L)$$

is exact, where β^* and α^* are the pullbacks of β and α respectively. We first show that β^* is a homomorphism of abelian groups. For $\varphi, \psi \in \mathrm{Hom}_R(P, L)$ and $n \in N$ we have

$$\beta^*(\varphi + \psi) = (\varphi + \psi) \circ \beta(n) = \varphi(\beta(n)) + \psi(\beta(n)) = (\beta^*\varphi + \beta^*\psi)(n)$$

as claimed. Assuming that R is commutative and $r \in R$, the map $r\varphi$ is also an R-module homomorphism. In this case we have

$$\beta^*(r\varphi)(n) = (r\varphi) \circ \beta(n) = r\varphi(\beta(n)) = r(\beta^*\varphi)(n)$$

as desired. Similarly for α^*.

Next note that β^* is injective, proving exactness at $\mathrm{Hom}_R(P, L)$:

$$\varphi \circ \beta = \beta^*\varphi = \beta^*\psi = \psi \circ \beta,$$

which implies that $\varphi = \psi$ since β is surjective.

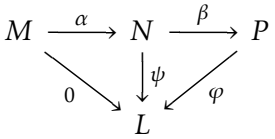
Finally we show exactness at $\mathrm{Hom}_R(N, L)$. First notice that

$$(\alpha^* \circ \beta^*)(\psi) = \psi \circ \beta \circ \alpha = \psi \circ 0,$$

showing that $\operatorname{im}\beta^* \subseteq \ker\alpha^*$. For the opposite inclusion, let $\psi \in \ker\alpha^*$. Then $\operatorname{im}\alpha \subseteq \ker\psi$, so since

$$P \cong \frac{N}{\ker\beta} = \frac{N}{\operatorname{im}\alpha},$$

by the universal property of quotients ψ factors (uniquely) through β, so $\psi = \varphi \circ \beta$ for some $\varphi\colon P \to L$. That is, the diagram



commutes. Thus $\psi = \beta^*\varphi$, so $\psi \in \operatorname{im}\beta^*$, showing exactness.

(b)

(c)

(d) If the original sequence splits, then α has a left-inverse γ by Proposition 7.5. For $\chi \in \mathrm{Hom}_R(M, L)$ we have

$$\alpha^*(\chi \circ \gamma) = (\chi \circ \gamma) \circ \alpha = \chi \circ (\gamma \circ \alpha) = \chi,$$

so α^* is surjective. □

EXERCISE 7.8

Prove that every exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow 0$$

of R-modules, with F *free*, splits.

SOLUTION. Since the map $\varphi\colon N \to F$ above is surjective, Exercise 6.9 (with $\alpha = \mathrm{id}_F$) yields an R-module homomorphism $\beta\colon F \to N$ such that $\mathrm{id}_F = \varphi \circ \beta$. That is, φ has a right-inverse, so Proposition 7.5 implies that the sequence splits. □

EXERCISE 7.9

Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow 0$$

be a short exact sequence of R-modules, with F free, and let L be an R-module. Prove that there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(F,L) \longrightarrow \mathrm{Hom}_R(N,L) \longrightarrow \mathrm{Hom}_R(M,L) \longrightarrow 0.$$

SOLUTION. Exercise 7.7 already yields an exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(F,L) \longrightarrow \mathrm{Hom}_R(N,L) \longrightarrow \mathrm{Hom}_R(M,L).$$

By Exercise 7.8 the first sequence above splits, so Exercise 7.7 again implies that the homomorphism $\mathrm{Hom}_R(N,L) \to \mathrm{Hom}_R(M,L)$ is surjective, yielding the rest of the sequence. □

EXERCISE 7.11

Let

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0 \tag{III.3}$$

be an exact sequence of R-modules. (This may be called an 'extension' of M_2 by M_1.) Suppose there is *any* R-module homomorphism $\varphi\colon N \to M_1 \oplus M_2$ making the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_1 & \xrightarrow{\alpha} & N & \xrightarrow{\beta} & M_2 & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\
0 & \longrightarrow & M_1 & \xrightarrow[\iota]{} & M_1 \oplus M_2 & \xrightarrow[\pi_2]{} & M_2 & \longrightarrow & 0
\end{array}$$

commute, where the bottom sequence is the standard sequence of a direct sum. Prove that (III.3) splits.

SOLUTION. It suffices to show that φ is bijective. To prove injectivity, let $n \in \ker\varphi$. Then $\varphi(n) = 0 = \iota(0)$, so n lies in the image of α. Pick $m \in M_1$ such that $\alpha(m) = n$, and notice that

$$\iota(m) = \varphi(\alpha(m)) = \varphi(n) = \iota(0),$$

and since ι is injective, we have $m = 0$.

To prove surjectivity, let $m_1 \in M_1$ and $m_2 \in M_2$. Since β is surjective there exists an $n' \in N$ such that $\beta(n') = m_2$. Now let $n = \alpha(m_1 - \pi_1(\varphi(n'))) + n'$ and notice that

$$\begin{aligned}
\varphi(n) &= \iota\Big(m_1 - \pi_1(\varphi(n'))\Big) + \varphi(n') \\
&= \Big(m_1 - \pi_1(\varphi(n')), 0\Big) + \Big(\pi_1(\varphi(n')), \pi_2(\varphi(n'))\Big) \\
&= \Big(m_1, \pi_2(\varphi(n'))\Big) \\
&= (m_1, \beta(n')) \\
&= (m_1, m_2).
\end{aligned}$$

Hence φ is also surjective and thus an isomorphism. □

IV • Groups, second encounter

IV.1. The conjugation action

REMARK IV.1: Normalisers and centralisers.
Let G be a group. For $g \in G$ we recall the inner automorphism $\gamma_g \colon G \to G$ given by $\gamma_g(a) = gag^{-1}$. This induces a map $\Gamma_g \colon 2^G \to 2^G$ given by $\Gamma_g(A) = \gamma_g(A) = gAg^{-1}$, and the map $g \mapsto \Gamma_g$ is then an action on 2^G. The stabiliser subgroup of a set $A \subseteq G$ with respect to this action is called the *normaliser* of A, denoted $N_G(A)$. More explicitly we have

$$\begin{aligned}
N_G(A) &= \{g \in G \mid \Gamma_g(A) = A\} \\
&= \{g \in G \mid gAg^{-1} = A\}.
\end{aligned}$$

If A is a singleton $\{a\}$, then we simply write $N_G(a)$ for its normaliser. If $g \in N_G(A)$ then $gAg^{-1} \subseteq A$. In other words, the set A is invariant under γ_g. Since γ_g is injective, if A is finite then the above inclusion is also sufficient for g to lie in $N_G(A)$, but this is not the case in general.

A subgroup H of G is a normal subgroup of the normaliser $N_G(H)$. In fact, $N_G(H)$ is the largest subgroup of G in which H is normal. It follows that H is normal in G if and only if $N_G(H) = G$. The orbit of H under the action on 2^G is the set $[H]$ of subgroups of H conjugate to H, i.e. its conjugacy class. The orbit-stabiliser theorem thus yields a bijection $G/N_G(H) \cong_{\mathbf{Set}} [H]$. If finite, the number of subgroups conjugate to H is thus the index $[G : N_G(H)]$ (this is Lemma 1.13).

If $g \in N_G(A)$ then A is invariant under γ_g, so γ_g restricts to a well-defined map $\gamma_g|_A \colon A \to A$. The *centraliser* of A is the subset of $N_G(A)$ of elements g such that $\gamma_g|_A$ is the identity on A, i.e.

$$\begin{aligned} Z_G(A) &= \{g \in N_G(A) \mid \gamma_g|_A = 1_A\} \\ &= \{g \in G \mid \forall a \in A \colon gag^{-1} = a\}. \end{aligned}$$

For a singleton $\{a\}$ we write $Z_G(a)$ for its centraliser. Notice that $Z_G(a) = N_G(a)$, and that this is the stabiliser of a under the conjugation action on G. If $\{A_i\}_{i\in I}$ is a family of subsets of G, then we clearly have

$$Z_G\Big(\bigcup_{i\in I} A_i\Big) = \bigcap_{i\in I} Z_G(A_i).$$

In particular we have

$$Z_G(A) = \bigcap_{a\in A} Z_G(a),$$

and so $Z_G(A)$ is a subgroup of G. Also notice that if $A \subseteq B \subseteq G$, then $Z_G(B) \subseteq Z_G(A)$. In particular,

$$\bigcup_{i\in I} Z_G(A_i) \subseteq Z_G\Big(\bigcap_{i\in I} A_i\Big).$$

The opposite inclusion probably (clearly?) doesn't hold in general, since the union of subgroups isn't necessarily a subgroup. Perhaps there is a closer relationship between the two sides of the inclusion, I don't know.

The *centre* of G is the centraliser $Z_G(G)$, denoted $Z(G)$. Equivalently, this is the kernel of the action $G \to \mathrm{Aut}_{\mathbf{Grp}}(G)$. Notice that this is the set of fixed points of the conjugation action on G, and contains the elements that commute with *all* elements in G. ⌟

EXERCISE 1.1

Let p be a prime integer, let G be a p-group, and let S be a finite set such that $|S| \not\equiv 0 \pmod{p}$. If G acts on S, prove that the action must have fixed points.

SOLUTION. If Z denotes the set of fixed points of the action, then Corollary 1.3 implies that

$$|Z| \equiv |S| \not\equiv 0 \mod p.$$

In particular, $|Z| \neq 0$, so the action has fixed points.

(Remark: Notice that we cannot use this type of argument to conclude from $|S| \equiv 0 \pmod{p}$ that the action has *no* fixed points: The number of fixed points just has to be a multiple of p.) □

Exercise 1.4

Let G be a group, and let N be a subgroup of $Z(G)$. Prove that N is normal in G.

Solution. For $g \in G$ and $n \in N$ we have $gn = ng$. But then $gN = Ng$, so N is normal in G. □

Exercise 1.5

Let G be a group. Prove that $G/Z(G)$ is isomorphic to the group $\mathrm{Inn}(G)$ of inner automorphisms of G. (Cf. Exercise II.4.8.) Then prove Lemma 1.5 again by using the result of Exercise II.6.7.

Solution. For $g \in G$ let $\gamma_g \colon G \to G$ be the corresponding inner automorphism given by $\gamma_g(a) = gag^{-1}$. Define a map $\gamma \colon G \to \mathrm{Inn}(G)$ by $\gamma(g) = \gamma_g$. Notice that γ_g is the identity on G exactly when g commutes with every element of G, i.e. when $g \in Z(G)$. Hence $\ker \gamma = Z(G)$, and since γ is surjective the first isomorphism theorem implies that $G/Z(G) \cong \mathrm{Inn}(G)$ as claimed.

By Exercise II.6.7 we know that $\mathrm{Inn}(G)$ is trivial if it is cyclic. If $G/Z(G)$ is cyclic the above thus implies that it is in fact trivial, and hence that $G = Z(G)$, i.e. that G is commutative. □

Exercise 1.6

Let p, q be prime integers, and let G be a group of order pq. Prove that either G is commutative or the center of G is trivial. Conclude (using Corollary 1.9) that every group of order p^2, for a prime p, is commutative.

Solution. Assume that the centre $Z(G)$ is nontrivial. Since it is a subgroup of G, Lagrange's theorem implies that $|Z(G)|$ divides $|G| = pq$, so assume that $|Z(G)| = p$. Hence $[G : Z(G)] = q$, but then Example II.8.16 implies that $G/Z(G)$ is cyclic. It follows from Lemma 1.5 that G is commutative.

In the case $p = q$, G is a p-group so Corollary 1.9 implies that its centre is nontrivial. The above then shows that in fact $Z(G) = G$. □

Exercise 1.8

Let p be a prime number, and let G be a p-group: $|G| = p^r$. Prove that G contains a normal subgroup of order p^k for every nonnegative $k \leq r$.

SOLUTION. We argue by induction on r. If $r = 0$ then this is obvious, so assume that $r > 0$. The centre of G is nontrivial by Corollary 1.9 and a p-group, and since $Z(G)$ is commutative it contains an element h of order p by Exercise II.8.17. Then $\langle h \rangle$ is a subgroup of $Z(G)$ of order p, hence is normal in G by Exercise 1.4. The quotient group $G/\langle h \rangle$ is of order p^{r-1}, so by induction it has a normal subgroup $\tilde{H}_k$ of order p^k for $k = 0, \dots, r-1$. By Proposition 8.9 each $\tilde{H}_k$ is on the form $H_k/\langle h \rangle$ for some subgroup H_k of G, and the third isomorphism theorem implies that H_k is normal in G. Also notice that

$$|H_k| = [H_k : \langle g \rangle]|g| = |\tilde{H}_k||g| = p^k p = p^{k+1}.$$

Hence G has normal subgroups of order p^k for $k = 1, \dots, r$ as desired. □

EXERCISE 1.9

Let p be a prime number, G a p-group, and H a nontrivial normal subgroup of G. Prove that $H \cap Z(G) \neq \{e\}$.

SOLUTION. Notice that H must also be a p-group. Also notice that H is a union of conjugacy classes since it is normal, and the order of each nontrivial conjugacy class divides the order of G, so they are divisible by p. It follows that the number of fixed points in H is also divisible by p, which proves the claim. □

EXERCISE 1.14

Let G be a group, and assume $[G : Z(G)] = n$ is finite. Let $A \subseteq G$ be any subset. Prove that the number of conjugates of A is at most n.

SOLUTION. Notice that the conjugates of A are precisely the images $\gamma_g(A) = gAg^{-1}$ of A under inner automorphisms for all $g \in G$. The number of conjugates of A are thus at most the number of inner automorphisms, and since $G/Z(G) \cong \mathrm{Inn}(G)$ by Exercise 1.5, this number is n. □

EXERCISE 1.17

Let H be a proper subgroup of a finite group G. Prove that G is not the union of the conjugates of H.

SOLUTION. By Lemma 1.13, the number of conjugates of H is $[G : N_G(H)]$. Since each of these conjugates overlap (at least in the identity), the number of elements in the union of the conjugates of H is *strictly* less than

$$[G : N_G(H)]|H| \leq [G : H]|H| = |G|.$$

The union of the conjugates of H is thus properly contained in G. □

EXERCISE 1.18

Let S be a set endowed with a transitive action of a finite group G, and assume $|S| \geq 2$. Prove that there exists a $g \in G$ without fixed points in S, that is, such that $gs \neq s$ for all $s \in S$.

SOLUTION. By the orbit-stabiliser theorem we may assume that $S = G/H$ with H a proper subgroup of G (since $|S| \geq 2$), and that the action on G/H is left-multiplication. By Exercise 1.17 there is a $g \in G$ that lies outside any conjugate of H, so that $g \notin aHa^{-1}$ for all $a \in G$. Hence $ga \notin aH$, so $gaH \neq aH$. □

EXERCISE 1.20

Let $G = \mathrm{GL}_2(\mathbb{C})$, and let H be the subgroup consisting of upper triangular matrices (Exercise II.6.2). Prove that G is the union of the conjugates of H. Thus, the finiteness hypothesis in Exercise 1.17 is necessary.

SOLUTION. This in fact holds for $\mathrm{GL}_n(\mathbb{C})$ for $n > 0$: If $A \in \mathrm{GL}_n(\mathbb{C})$, then Schur's theorem yields a unitary matrix Q and an upper triangular matrix U such that $A = QUQ^{-1}$. □

IV.2. The Sylow theorems

REMARK IV.2: Proof of Claim 2.2.

Note that the fixed points of the action are $(e,\dots,e)$ along with $(a,\dots,a)$ with $a \in G$ if and only if $\langle a \rangle$ is of order p. But the elements $a, a^2, \dots, a^{p-1}$ generate the same subgroup, so $|Z| = 1 + N(p-1)$, where N is the number of (cyclic) subgroups of order p. ⌟

EXERCISE 2.1

Prove Claim 2.2: Let G be a finite group, let p be a prime divisor of $|G|$, and let N be the number of cyclic subgroups of G of order p. Then $N \equiv 1 \pmod{p}$.

SOLUTION. Notice that an element of G lies in a (cyclic) subgroup of order p if and only if it is either the identity or of order p (by Lagrange's theorem). Thus any non-identity element of such a subgroup is a generator. Notice also that two distict such subgroups only intersect at the identity. It follows that, in the notation of the proof of Theorem 2.1, $|Z| = Np - N + 1$. Hence $N(p-1)+1 \equiv 0 \pmod{p}$, which implies that

$$N \equiv -N(p-1) \equiv 1 \mod p$$

as desired. □

EXERCISE 2.2

Let G be a group. A subgroup H of G is *characteristic* if $\varphi(H) \subseteq H$ for every automorphism φ of G.

(a) Prove that characteristic subgroups are normal.

(b) Let $H \subseteq K \subseteq G$, with H characteristic in K and K normal in G. Prove that H is normal in G.

(c) Let G, K be groups, and assume that G contains a single subgroup H isomorphic to K. Prove that H is normal in G.

(d) Let K be a normal subgroup of a finite group G, and assume that $|K|$ and $|G/K|$ are relatively prime. Prove that K is characteristic in G.

SOLUTION. (a) This is obvious, since then $gHg^{-1} \subseteq H$ for all $g \in G$.

(b) Let $g \in G$ and consider the inner automorphism $\gamma_g \in \mathrm{Inn}(G)$. Since K is normal in G, this restricts to an automorphism $\gamma_g|_K \colon K \to K$. And since H is characteristic in K, this implies that

$$gHg^{-1} = \gamma_g|_K(H) \subseteq H$$

so H is normal in G.

(c) For each $g \in G$, the subgroup gHg^{-1} is isomorphic to H, hence to K. But then we must have $gHg^{-1} = H$, so H is normal.

(d) We prove the following lemma:

> *Let G be a group, H a finite subgroup, and N a normal subgroup such that $[G : N]$ is finite. If $|H|$ and $[G : N]$ are relatively prime, then $H \subseteq N$.*

By the third isomorphism theorem we have

$$\frac{HN}{N} \cong \frac{H}{H \cap N},$$

and these groups are finite since H is. Notice that $[H : H \cap N]$ is then a divisor of $|H|$, and also a divisor of $[G : N]$ since $[HN : N]$ is. But then $[H : H \cap N] = 1$ by relative primality, showing that $H \cap N = H$.

We now prove the original claim. If φ is an automorphism of G, then $\varphi(K)$ is a subgroup of G with $|\varphi(K)| = |K|$. Hence $|\varphi(K)|$ and $[G : K]$ are relatively prime, so the lemma implies that $\varphi(K) \subseteq K$. Since the two subgroups are finite with the same cardinality, this inclusion is in fact an equality. □

EXERCISE 2.3

Prove that a nonzero abelian group G is simple if and only if $G \cong \mathbb{Z}/p\mathbb{Z}$ for some positive prime integer p.

SOLUTION. First notice that G must be cyclic: If $g \neq e$, then $\langle g \rangle$ is a nontrivial normal subgroup of G, hence must equal G. Hence it suffices to find the simple cyclic groups. But these are precisely the groups $\mathbb{Z}/p\mathbb{Z}$ for primes p. □

EXERCISE 2.4

Prove that a group G is simple if and only if its only homomorphic images (i.e., groups G' such that there is an onto homomorphism $G \to G'$) are the trivial group and G itself (up to isomorphism).

SOLUTION. First assume that G is simple, and let $\varphi\colon G \to G'$ be a homomorphism. This is either trivial or injective, and in the latter case $G \cong \varphi(G)$.

Conversely, assume that G is *not* simple, and let H be a nontrivial proper normal subgroup of G. Then G/H is the image of the quotient map $G \to G/H$, and this is neither trivial nor isomorphic to G. □

EXERCISE 2.5

Let G be a simple group, and assume $\varphi\colon G \to G'$ is a nontrivial group homomorphism. Prove that φ is injective.

SOLUTION. The kernel of φ is a normal subgroup of G, so this is either $\{e\}$ or G. The latter is impossible since φ is nontrivial, so $\ker \varphi = \{e\}$. Hence φ is injective. □

V • Irreducibility and factorization in integral domains

V.1. Chain conditions and existence of factorizations

Exercise 1.13

Prove that prime $\Leftrightarrow$ irreducible in $\mathbb{Z}$.

Solution. Since $\mathbb{Z}$ is an integral domain, it suffices by Lemma 1.7 to show that every irreducible element is prime, so let p be irreducible and assume that $p \mid ab$. If $p \mid a$ then we are done, so assume that $p \nmid a$. Then p and a are coprime, so there exist $c, d \in \mathbb{Z}$ such that $pc + ad = 1$. This implies that $pbc + abd = b$, and p divides the left-hand side so it divides b. □

V.2. UFDs, PIDs, Euclidean domains

V.3. Intermezzo: Zorn's lemma

V.4. Unique factorization in polynomial rings

Exercise 4.17

Let F be a field, and recall the notion of characteristic of a ring (Definition III.3.7); the characteristic of a field is either 0 or a prime integer (Exercise III.3.14).

(a) Show that F has characteristic 0 if and only if it contains a copy of $\mathbb{Q}$ and that F has characteristic p if and only if it contains a copy of the field $\mathbb{Z}/p\mathbb{Z}$.

(b) Show that (in both cases) this determines the smallest subfield of F; it is called the *prime subfield* of F.

Solution. First assume that F has characteristic 0. Then the unique ring homomorphism $\iota\colon \mathbb{Z} \to F$ is injective, so $\iota(n)$ is a unit for $n \neq 0$. Define the map $\varphi\colon \mathbb{Q} \to F$ by

$$\varphi\left(\frac{m}{n}\right) = \iota(m)\iota(n)^{-1}.$$

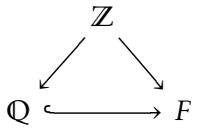
This is clearly well-defined. Notice that

$$\varphi\left(\frac{m}{n}\frac{p}{q}\right) = \varphi\left(\frac{mp}{nq}\right) = \iota(mp)\iota(nq)^{-1} = \iota(m)\iota(n)^{-1}\iota(p)\iota(q)^{-1} = \varphi\left(\frac{m}{n}\right)\varphi\left(\frac{p}{q}\right),$$

and that

$$\begin{aligned}\varphi\left(\frac{m}{n}+\frac{p}{q}\right)=\varphi\left(\frac{mq+pn}{nq}\right)&=\iota(mq+pn)\iota(nq)^{-1}\\&=\iota(mq)\iota(nq)^{-1}+\iota(pn)\iota(nq)^{-1}\\&=\iota(m)\iota(n)^{-1}+\iota(p)\iota(q)^{-1}\\&=\varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{p}{q}\right).\end{aligned}$$

Thus φ is a ring homomorphism, and since $\mathbb{Q}$ is a field it is also injective. Hence F contains a copy of $\mathbb{Q}$. Conversely, if there is an injective map $\mathbb{Q}\to F$ then the diagram



commutes by uniqueness. Hence $\mathbb{Z}\to\mathbb{Q}$ and $\mathbb{Z}\to F$ have the same kernel, implying that $\operatorname{char} F=\operatorname{char}\mathbb{Q}=0$.

Next assume that F has characteristic p. The unique ring homomorphism $\iota\colon\mathbb{Z}\to F$ then has kernel $p\mathbb{Z}$ so it induces an injection $\tilde{\iota}\colon\mathbb{Z}/p\mathbb{Z}\to F$ by the canonical decomposition. The converse follows as before.

TODO (b)? □

V.5. Irreducibility of polynomials

V.6. Further remarks and examples

EXERCISE 6.8

Let $n\in\mathbb{Z}$ be a positive integer and $n=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ its prime factorisation. By the classification theorem for finite abelian groups (or, in fact, simpler considerations; cf. Exercise II.4.9)

$$\frac{\mathbb{Z}}{(n)}\cong\frac{\mathbb{Z}}{(p_1^{\alpha_1})}\times\cdots\times\frac{\mathbb{Z}}{(p_r^{\alpha_r})}$$

as abelian groups.

(a) Use the CRT to prove that this is in fact a *ring* isomorphism.

(b) Prove that

$$\left(\frac{\mathbb{Z}}{(n)}\right)^*\cong\left(\frac{\mathbb{Z}}{(p_1^{\alpha_1})}\right)^*\times\cdots\times\left(\frac{\mathbb{Z}}{(p_r^{\alpha_r})}\right)^*$$

(recall that $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the group of units of $\mathbb{Z}/n\mathbb{Z}$).

(c) Recall (Exercise II.6.14) that *Euler's φ-function* $\varphi(n)$ denotes the number of positive integers $< n$ that are relatively prime to n. Prove that

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)\cdots p_r^{\alpha_r - 1}(p_r - 1).$$

SOLUTION. (a) We prove this without appealing to the CRT. Simply notice that the maps π_m^{mn} and π_n^{mn} are ring isomorphisms for coprime m and n. The claim then follows by induction.

(b) We prove that $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ for coprime m and n, where the (multiplicative) group isomorphism is just the restriction of the ring isomorphism above; the claim will then follow by induction. If $[a]_{mn} \in (\mathbb{Z}/mn\mathbb{Z})^*$, then a is also relatively prime to both m and n, so $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$ and similarly for n.

Conversely, if $[b]_m \in (\mathbb{Z}/m\mathbb{Z})^*$ and $[c]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, then there exists an $a \in \mathbb{Z}$ such that $\pi_m^{mn}([a]_{mn}) = [b]_m$ and $\pi_n^{mn}([a]_{mn}) = [c]_n$. But then $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, so a is relatively prime to both m and n, hence to mn as desired.

(c) We first notice that, by (b), $\varphi(mn) = \varphi(m)\varphi(n)$ for coprime m and n. Next notice that $\varphi(p^k) = p^k - p^{k-1}$ for a prime p. The claim follows. □

VI • Linear algebra

VII • Fields

VII.1. Field extensions, I

REMARK VII.1: Initial objects in $\mathbf{Fld}_0$ and $\mathbf{Fld}_p$.
We first show that $\mathbb{Q}$ is initial in $\mathbf{Fld}_0$. Let k be a field of characteristic 0. Then Exercise V.4.17 implies the existence of a ring homomorphism $\varphi\colon \mathbb{Q} \to k$. Let $\psi\colon \mathbb{Q} \to k$ be another homomorphism, and let $\iota\colon \mathbb{Z} \to \mathbb{Q}$ be the unique ring homomorphism. Then $\varphi \circ \iota = \psi \circ \iota$ by uniqueness, and since ι is an epimorphism by §III.2.3 it follows that $\varphi = \psi$.

The same argument works in $\mathbf{Fld}_p$ with the quotient map π_p playing the role of ι, so $\mathbb{F}_p$ is initial in $\mathbf{Fld}_p$. ⌟

EXERCISE 1.1

Prove that if $k \subseteq K$ is a field extension, then $\operatorname{char} k = \operatorname{char} K$. Prove that the category **Fld** has no initial object.

SOLUTION. Let $\varphi\colon k \to K$ be a field extension, and let $\iota_k\colon \mathbb{Z} \to k$ and $\iota_K\colon \mathbb{Z} \to K$ be the unique ring homomorphisms. Notice that φ is injective by [ref], so since $\iota_K = \varphi \circ \iota_k$ by uniqueness, we have $\ker \iota_k = \ker \iota_K$ and hence $\operatorname{char} k = \operatorname{char} K$.

If k is any field and $\operatorname{char} k = p$, then there is no homomorphism $k \to \mathbb{F}_q$ for $q \neq p$. Hence k is not initial in **Fld**. □