Errata for 'Algebra: Chapter 0', first (2009) printing

This is the errata for the **first** (2009) printing of Chapter 0. If you are looking for the errata for the second (2016) printing, click here.

Highlighted in red are the needed changes, embedded in text matching the published version and identified by page and position on the page (e.g., `p.10, top'). A **bold** reference indicates an error in the published version which may be more confusing, such as a missing hypothesis in an exercise. (My personal favorite is the missing abelian on p.49, Exercise 1.8.)

This list is bound to grow forever. (320 items, and counting.) The contribution of many readers is hereby gratefully acknowledged.

Last updated: 5/9/20.

-

preface

- p.xvii, end of first paragraph:

  case of Dirichlet's theorem on primes in arithmetic progressions, and that this will

---

-

Chapter I

- **p.8, Exercise 1.2:**

  1.2. ▷ Prove that if $\sim$ is an equivalence relation on a set S, then the corresponding family $\mathscr{P}_\sim$ defined in §1.5 is indeed a partition of S: that is, its elements are nonempty, disjoint, and their union is S. [§1.5]

- p.9, middle:

  The action of a function $f : A \to B$ on an element $a \in A$ is sometimes indicated by a 'decorated' arrow, as in

---

- p.9, bottom:

If S is a subset of A, we denote by $f(S)$ the subset of B defined by

$$f(S) := \{b \in B \mid (\exists a \in S)\, b = f(a)\}.$$

That is, $f(S)$ is the subset of B consisting of all elements that are images of elements

---

- p.10, top:

That is, $f|_S$ is the composition (in the sense explained in §2.3) $f \circ i$, where $i : S \to A$ is the inclusion. Note that $f(S) = \mathrm{im}(f|_S)$.

- p.11, middle:

  - A function $f : A \to B$ is *injective* (or *an injection* or *one-to-one*) if

$$(\forall a' \in A)\,(\forall a'' \in A) \quad a' \neq a'' \implies f(a') \neq f(a'') :$$

that is, if f sends different elements to different elements[9].

- p.13, middle:

This is not completely innocent: if f has both *a* left-inverse and *a* right-inverse, why should it have *one* inverse that works as both on the left and on the right? Try to prove this by yourself now. We will come back to this issue soon (in §4).

If a function is injective *but not surjective*, then it will not have a right-inverse, and if the source has at least two elements, it will necessarily have more than one left-inverse (this should be clear from the argument given in the proof of Proposition 2.1). Similarly, a surjective function will in general have many right-inverses; they are often called *sections*.

- p.16, bottom half:

Injective: If $\tilde{f}([a']_\sim) = \tilde{f}([a'']_\sim)$, then $f(a') = f(a'')$ by definition of $\tilde{f}$; hence $a' \sim a''$ by definition of $\sim$, and then $[a']_\sim = [a'']_\sim$. Therefore

$$\tilde{f}([a']_\sim) = \tilde{f}([a'']_\sim) \implies [a']_\sim = [a'']_\sim$$

proving injectivity.

- p.17, Exercise 2.2:

2.2. ▷ Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint nonempty subsets of a set, there is a way to choose one element in each member of the family[13]. [§2.5, V.3.3]

- p.21, middle:

tells us that $\mathrm{Hom}(a,b)$ is nonempty, and according to the definition of morphisms in this category that means that $a \sim b$, and f is in fact the element (a,b) of $S \times S$. Similarly, $g \in \mathrm{Hom}(b,c)$ tells us $b \sim c$ and $g = (b,c)$. Now

$$a \sim b \text{ and } b \sim c \implies a \sim c$$

since we are assuming that $\sim$ *is transitive.* This tells us that $\mathrm{Hom}(a,c)$ consists of the single element (a,c). Thus we again have no choice: we must let

$$gf := (a,c) \in \mathrm{Hom}(a,c).$$

- p.23, middle:

  That is, morphisms $f_1 \to f_2$ correspond precisely to those morphisms $\sigma : Z_1 \to Z_2$ in C *such that* $f_1 = f_2\sigma$.

- p.33, middle:

  the assertion that $\emptyset$ is initial in the category Set.

-

Chapter II

- p.44, top:

  Proof. This actually follows from Proposition I.4.2 (by viewing G as the set of isomorphisms of a groupoid with a single object). The reader should construct a stand-alone proof, using the same trick, but carefully hiding any reference to morphisms. □

- **p.49, Exercise 1.8:**

  1.8. ¬ Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$. [4.16]

- **p.52, second-to-last paragraph:**

The *dihedral* groups may be defined as these groups of symmetries for the *regular polygons*. Placing the polygon so that it is centered at the origin (thereby excluding translations as possible symmetries), we see that the dihedral group for a regular n-sided polygon consists of the n rotations by $2\pi/n$ radians about the origin and the n distinct reflections about lines through the origin and a vertex or a midpoint of a side. Thus, the dihedral group for a regular n-sided polygon consists of $2n$ elements; we will denote[11] this group by the symbol D_{2n}.

- p.54, middle:

$$[0]_n, \quad [1]_n, \quad \cdots, \quad [n-1]_n.$$

- p.55, Remark 2.4:

Remark 2.4. As a consequence, the order of every element of $\mathbb{Z}/n\mathbb{Z}$ divides $n = |\mathbb{Z}/n\mathbb{Z}|$, the order of the group. We will see later (Example 8.15) that this is a general feature of the order of elements in any finite group. ⌟

- **p.56, Exercise 2.1:**

2.1. ¬ One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$ by letting the entry at $(i, (i)\sigma)$ be 1 and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

would be

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

Prove that, with this notation,

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

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices. [IV.4.13]

- p.57, Exercise 2.6:

2.6. ▷ For every positive integer n construct a group containing elements g, h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$. (Hint: For $n > 1$, D_{2n} will do.) [§1.6]

- p.57, Exercise 2.10:

2.10. Prove that if $n > 0$, then $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

- p.57, Exercise 2.12:

2.12. Prove that there are no nonzero integers a, b, c such that $a^2+b^2 = 3c^2$. (Hint: By studying the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$, show that a, b, c would all have to be even. Letting $a = 2k$, $b = 2\ell$, $c = 2m$, you would have $k^2 + \ell^2 = 3m^2$. What's wrong with that?)

- p.57, Exercise 2.15, second point:

  - Prove that if $\gcd(r, 2n) = 1$, then $\gcd(\frac{r-n}{2}, n) = 1$. (Ditto.)

- p.58, Exercise 2.18:

2.18. For $d \leq n$, define an injective function $\mathbb{Z}/d\mathbb{Z} \to S_n$ preserving the operation, that is, such that the sum of equivalence classes in $\mathbb{Z}/d\mathbb{Z}$ corresponds to the product of the corresponding permutations.

- p.60, middle:

$$\iota_G : G \to G, \quad \iota_G(g) := g^{-1}.$$

- p.61, middle:

To see that trivial groups are initial, let $T = \{e\}$ be a trivial group; for any group G, define $\varphi : T \to G$ by $\varphi(e) = e_G$. This is clearly a group homomorphism,

---

- **p.63, Exercise 3.1:**

3.1. ▷ Let $\varphi : G \to H$ be a morphism in a category C with products. Explain why there is a unique morphism $(\varphi \times \varphi) : G \times G \to H \times H$ compatible in the evident way with the natural projections.

(This morphism is defined explicitly for $\mathsf{C} = \mathsf{Set}$ in §3.1.) [§3.1, 3.2]

- p.63, Exercise 3.9:

3.9. Show that *fiber* products and coproducts exist in Ab. (Cf. Exercise I.5.12. For coproducts, you may have to wait until you know about *quotients*.)

- p.65, bottom:

that a homomorphism must send the identity to the identity (Proposition 3.2), and that already rules out all but 343 functions (why?); still, it is unrealistic to write all of them out explicitly to see if any is a homomorphism.

- p.68, middle:

instance of this observation. As we have seen, $\mathrm{Hom}_{\mathsf{Grp}}(G, H)$ is a *pointed set* for any two groups G, H. In Ab, we can say much more: $\mathrm{Hom}_{\mathsf{Ab}}(G, H)$ *is a* group *(in fact, an abelian group) for any two abelian groups* G, H.

- p.69, top:

a commutative group, then $H^A = \mathrm{Hom}_{\mathsf{Set}}(A, H)$ is a commutative group for all sets A; we will come back to this group in §5.4.

- p.69, Exercise 4.2:

4.2. Show that the homomorphism $\pi_2^4 \times \pi_2^4 : C_4 \to C_2 \times C_2$ is *not* an isomorphism. In fact, is there *any* isomorphism $C_4 \to C_2 \times C_2$?

- p.70, Exercise 4.14:

4.14. ▷ Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r \leq n$ that are *relatively prime* to n. (This is called *Euler's ϕ-function;* cf. Exercise 6.14.) [§IV.1.4, IV.1.22, §IV.2.5]

- p.70, Exercise 4.16:

4.16. ¬ Prove *Wilson's theorem: an integer $p > 1$ is prime if and only if*

$$(p-1)! \equiv -1 \mod p.$$

- p.72, top:

one element $g = f(a) \in G$. Now *there is a unique* homomorphism $\varphi : \mathbb{Z} \to G$ making the diagram

---

- p.77, bottom:

$$\sum_{a \in A} m_a j_a, \quad m_a \neq 0 \text{ for only finitely many } a;$$

- p.79, bottom:

$a = h_1$, $b = h_2^{-1}$; the stated condition says that

$$h_1 h_2 = h_1((h_2)^{-1})^{-1} = ab^{-1} \in H,$$

proving that H is closed under the operation.

- p.80, Lemma 6.3:

$$H = \bigcap_{\alpha \in A} H_\alpha$$

- p.80, middle:

thus, $ab^{-1} \in \varphi^{-1}(H')$. This implies that $\varphi^{-1}(H')$ is a subgroup of G, by Proposition 6.2. □

- p.81, proof of Proposition 6.6:

Proof. If $\alpha : K \to G$ is such that $\varphi \circ \alpha$ is the trivial map, then $\forall k \in K$

$$\varphi \circ \alpha(k) = \varphi(\alpha(k)) = e_{G'},$$

that is, $\alpha(k) \in \ker \varphi$. We can (and must) then let $\overline{\alpha} : K \to \ker \varphi$ simply be α itself, with restricted target. □

- p.81, Remark 6.7:

such that the image of $\varphi \circ \alpha$ is the identity in G' must factor (as a set-function)

- p.81, bottom half:

6.3. Example: Subgroup generated by a subset. If $A \subseteq G$ is *any* subset, we have a unique group homomorphism

$$\varphi_A : F(A) \to G$$

extending this inclusion, by the universal property of free groups. The image of this homomorphism is a subgroup of G, the *subgroup generated by* A in G, often denoted[27] $\langle A \rangle$.

- p.82, top:

The reader who has not (yet) developed a taste for free groups may prefer the following alternative description: $\langle A \rangle$ is the intersection of all subgroups of G containing A,

---

- p.83, middle:

The inclusion $d\mathbb{Z} \subseteq G$ is clear. To verify the inclusion $G \subseteq d\mathbb{Z}$, let $m \in G$, and apply 'division with remainder' to write

$$m = dq + r,$$

with $0 \leq r < d$. Since $m \in G$ and $d\mathbb{Z} \subseteq G$ and since G is a subgroup, we see that

---

- p.85, Exercise 6.1:

  - $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) \,|\, \det(M) = 1\}$;
  - $\mathrm{U}(n) = \{M \in \mathrm{GL}_n(\mathbb{C}) \,|\, MM^\dagger = M^\dagger M = I_n\}$;
  - $\mathrm{SU}(n) = \{M \in \mathrm{U}(n) \,|\, \det(M) = 1\}$.

- p.86, Exercise 6.3:

6.3. ¬ Prove that every matrix in $\mathrm{SU}(2)$ may be written in the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2 + b^2 + c^2 + d^2 = 1$. (Thus, $\mathrm{SU}(2)$ may be realized as a three-dimensional spher e embedded in $\mathbb{R}^4$; in particular, it is *simply connected.*) [8.9, III.2.5]

- p.87, Exercise 6.11:

6.11. Since direct sums are coproducts in Ab, the classification theorem for abelian groups mentioned in the text says that every finitely generated *abelian group* is a coproduct of cyclic groups in Ab. The reader may be tempted to conjecture that every finitely generated *group* is a coproduct of cyclic groups *in* Grp. Show that this is not the case, by proving that S_3 is not a coproduct of cyclic groups.

- p.87, Exercise 6.14:

6.14. ▷ If m is a positive integer, denote by $\phi(m)$ the number of positive integers $r \leq m$ that are *relatively prime* to m (that is, for which the gcd of r and m is 1);

- p.88, Exercise 6.15:

6.15. ▷ Prove that if a group homomorphism $\varphi : G \to G'$ has a left-inverse, that is, a group homomorphism $\psi : G' \to G$ such that $\psi \circ \varphi = \mathrm{id}_G$, then φ is a monomorphism. [§6.5, 6.16]

- p.92, middle:

Further

$$(\forall a \in G): \quad a \in aH \cap Ha;$$

hence, if $aH = Hb$ for any b, then in fact necessarily $aH = Ha$. This is of course automatically true if G is commutative, but it is simply not the case in general.

- p.94, bottom half:

By Corollary 1.11,

$$\ker \epsilon_g = \{N \in \mathbb{Z} \mid N \text{ is a multiple of } |g|\} = n\mathbb{Z}.$$

Theorem 7.12 then implies right away that ϵ_g factors through the quotient:

- p.99, bottom half:

Thus, a presentation of a group G is usually encoded as a pair $(A|\mathscr{R})$, where A is a set and $\mathscr{R} \subseteq F(A)$ is a set of words, such that $G \cong F(A)/R$ with R as above.

A group is *finitely presented* if it admits a presentation $(A|\mathscr{R})$ in which both A and $\mathscr{R}$ are finite. Finitely presented groups are not (necessarily) 'small': for example, the free group on finitely many generators is (trivially) finitely presented.

- p.102, Footnote 37:

make better sense when we get to Example 9.4. In any case, there is a bijection between the set of left-cosets and the set of right-cosets: Exercise 9.10.

- p.104, bottom half:

which is initial with respect to all morphisms α such that $\alpha \circ \varphi = 0$. That is, every homomorphism $\alpha : G' \to L$ such that $\alpha \circ \varphi$ is the trivial map must factor (uniquely) through $\operatorname{coker} \varphi$:

- p.106, Exercise 8.9:

8.9. ¬ (Ditto.) Prove that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$, where I_2 is the identity matrix. (Hint: It so happens that every matrix in $\mathrm{SO}_3(\mathbb{R})$ can be written in the form

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2+b^2+c^2+d^2 = 1$. Proving this fact is not hard, but at this stage you will probably find it computationally demanding. Feel free to assume this, and use Exercise 6.3 to construct a surjective homomorphism $\mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$; compute the kernel of this homomorphism.)

- p.107, Exercise 8.13:

8.13. ¬ Let G be a finite group, and assume $|G|$ is odd. Prove that every element of G is a square. [8.14]

- p.107, Exercise 8.15:

8.15. Let a, n be positive integers, with $a > 1$. Prove that n divides $\phi(a^n - 1)$, where ϕ is Euler's ϕ-function; see Exercise 6.14. (Hint: Example 8.15.)

- p.107, Exercise 8.17:

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. (Hint: Let $g \neq e$ be an element of G, and consider the subgroup $\langle g \rangle$; use the fact that this subgroup is cyclic to show that there is an element $h \in \langle g \rangle$ in G of *prime* order q. If $q = p$, you are done; otherwise, use the quotient $G/\langle h \rangle$ and induction.) [§8.5, 8.18, 8.20, §IV.2.1]

- p.111, Proposition 9.9:

Proposition 9.9. *Every transitive left-action of G on a nonempty set A is isomorphic to the left-multiplication of G on G/H, for $H =$ the stabilizer of any $a \in A$.*

- p.113, Exercise 9.1:
  - Find an interesting action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$. (Hint: Exercise 8.9.)

- p.113, Exercise 9.2:

on the plane is respectively to flip the plane about the x-axis and to rotate it 90°

- p.113, Exercise 9.3:

  9.3. ▷ If $G = (G, \cdot)$ is a group, we can define an 'opposite' group $G^\circ = (G, \bullet)$

- **p.116, top:**

  in C such that the diagrams

$$\begin{array}{ccccc} (G \times G) \times G & \xrightarrow{m \times \mathrm{id}_G} & G \times G & \xrightarrow{m} & G \\ \downarrow \cong & & & & \| \\ G \times (G \times G) & \xrightarrow{\mathrm{id}_G \times m} & G \times G & \xrightarrow{m} & G \end{array}$$

-

Chapter III

- p.120, top:

  (which make $(R, \cdot)$ a *monoid*), and further interacting with $+$ via the following *distributive* properties:

  - $(\forall r, s, t \in R):\quad (r+s)\cdot t = r\cdot t + s\cdot t$ and $t\cdot(r+s) = t\cdot r + t\cdot s$. ⌟

- p.123, Proposition 1.12:

  - *u is a left- (resp., right-) unit if and only if left- (resp., right-) multiplication by u is a* surjective *function* $R \to R$;

- p.125, bottom:

$$\deg(([1] + [2]x) \cdot ([1] + [3]x)) = \deg([1] + [5]x) = 1 \neq 1 + 1.$$

  Polynomials of degree 0 (together with 0) are called *constants*; they form a 'copy' of R in $R[x]$, since the operations $+, \cdot$ on constant polynomials are nothing but the original operations in R, up to this identification. It is sometimes convenient to assign to the polynomial 0 the degree $-\infty$.

- p.126, bottom:

  where the 'coefficients' a_m are elements of R and $a_m \neq 0$ for at most finitely many

---

- p.127, Exercise 1.3:

  R^S is just a copy of R if S is a singleton. [2.3]

- p.127, Exercise 1.4:

  - $\mathfrak{su}(n) = \{M \in \mathfrak{s}\, l_n(\mathbb{C}) \mid M + M^\dagger = 0\}$.

- p.129, bottom:

$$(\forall n \in \mathbb{Z}): \quad \varphi(n) = n1_R,$$

- p.130, footnote:

  [5]For the reader interested in generalizations: only the requirement that $j(a_1), \ldots, j(a_n)$ commute with one another is needed here.

- p.131, middle:

$$\begin{aligned}\varphi(\sum m_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n}) &= \sum \varphi(m_{i_1\cdots i_n})\varphi(x_1)^{i_1}\cdots\varphi(x_n)^{i_n} \\ &= \sum \iota(m_{i_1\cdots i_n}) j(a_1)^{i_1}\cdots j(a_n)^{i_n},\end{aligned}$$

- p.132, middle:

  we obtain unique ring homomorphisms $\mathrm{ev}_r : \mathbb{Z}[x] \to R$ such that $\mathrm{ev}_r(x) = r$ and

---

- p.133, middle:

  2.4. Products. *Products* exist in Ring: if R_1, R_2 are rings, then $R_1 \times R_2$ may be defined by endowing the direct product of *groups* $R_1 \times R_2$ (cf. §II.3.4) with componentwise multiplication. Thus, both operations on $R_1 \times R_2$ are defined componentwise: $\forall (a_1, a_2), (b_1, b_2) \in R_1 \times R_2$,

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2), \\ (a_1, a_2) \cdot (b_1, b_2) &:= (a_1 \cdot b_1, a_2 \cdot b_2).\end{aligned}$$

- p.136, bottom:

  this homomorphism is isomorphic to SU(2) (cf. Exercise II.6.3). [4.10, IV.5.17,

---

- p.137, Exercise 2.11:

- If R is not commutative, then its center C (Exercise 2.9) is a proper subring of R. Prove that C would then consist of p elements.

- **p.138, Exercise 2.17:**

2.17. ¬ Let R be a ring, and let $E = \mathrm{End}_{\mathsf{Ab}}(R)$ be the ring of endomorphisms of the underlying abelian group $(R, +)$. Prove that the center of E is isomorphic to a subring of the center of R. (Prove that if $\alpha \in E$ commutes with all right-multiplications by elements of R, then α is left-multiplication by an element of R; then use Proposition 2.7.)

- p.139, middle:

Indeed, we know already that $\ker \varphi$ is a subgroup; we have to verify the absorption properties. These are an immediate consequence of Lemma 1.2: for all $r \in R$, all $a \in \ker \varphi$, we have

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0,$$

$$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0.$$

- p.144, Exercise 3.9:

3.9. ¬ Counterpoint to Exercise 3.8: It is *not* true that a 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, and division rings are simple.

Prove that $\mathcal{M}_n(\mathbb{R})$ is simple. (Use Exercise 3.6.) [4.20]

- p.144, Exercise 3.15:

3.15. ¬ A ring R is[14] *Boolean* if $a^2 = a$ for all $a \in R$. Prove that $\mathscr{P}(S)$ is Boolean, for every set S (cf. Exercise 1.2). Prove that every nonzero Boolean ring is commutative and has characteristic 2. Prove that if an integral domain R is Boolean, then $R \cong \mathbb{Z}/2\mathbb{Z}$. [4.23, V.6.3]

- p.149, Example 4.8:

Example 4.8. It is fun to analyze higher-degree examples. For every monic $f(x) \in R[x]$ of degree d, Proposition 4.6 gives a potentially *different* ring (that is, $R[x]/(f(x))$) isomorphic to $R^{\oplus d}$ as a group; one can then use this isomorphism to define a new ring structure onto the group $R^{\oplus d}$.

- p.152, middle:

This picture is particularly appealing for fields such as $k = \mathbb{C}$, which are *algebraically closed,* that is, in which for every nonconstant $f(x) \in k[x]$ there exists $r \in k$ such that $f(r) = 0$. It would take us too far afield to discuss this notion at any length now; but the reader should be aware that $\mathbb{C}$ is algebraically closed. We will come back to this[20]. Assuming this fact, it is easy to verify (Exercise 4.21) that the maximal ideals in $\mathbb{C}[x]$ are all and only the ideals

---

- p.153, top:

In general, the *(Krull) dimension* of a commutative ring R is the length of the longest chain of prime ideals in R. Thus, Proposition 4.13 tells us that PIDs other than fields, such as $\mathbb{Z}$, have 'dimension 1'. In the lingo of algebraic geometry, they all correspond to curves. ⌟

- p.154, top:

4.5. ▷ Let I, J be ideals in a commutative ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$. [§4.1]

4.6. Let I, J be ideals in a commutative ring R. Assume that $R/(IJ)$ is reduced (that is, it has no nonzero nilpotent elements; cf. Exercise 3.13). Prove that $IJ = I \cap J$.

- **p.154, Exercise 4.9:**

4.9. Generalize the result of Exercise 4.8, as follows. Let R be a commutative ring, and let $f(x)$ be a zero-divisor in $R[x]$. Prove that $\exists b \in R$, $b \neq 0$, such that $f(x)b = 0$. (Hint: Let $f(x) = a_d x^d + \cdots + a_0$, and let $g(x) = b_e x^e + \cdots + b_0$ be a nonzero polynomial of minimal degree e such that $f(x)g(x) = 0$. Deduce that $a_d g(x) = 0$, and then prove $a_{d-i} g(x) = 0$ for all i. by induction. What does this say about b_e?)

- p.154, Exercise 4.10:

  - 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 $z \in \mathbb{Q}(\sqrt{d})$, $z \neq 0$.

- **p.155, Exercise 4.17:**

4.17. ¬ (If you know a little topology...) 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 $f_1, \ldots, f_r \in R$ have no common zeros, then $(f_1, \ldots, f_r) = (1)$. (Hint: Consider $f_1^2 + \cdots + f_r^2$.)

(iii) Prove that every maximal ideal M in R is of the form M_p for some $p \in K$. (Hint: You will use the compactness of K and (ii).)

If further K is Hausdorff (and, as Bourbaki would have it, compact spaces are Hausdorff), then Urysohn's lemma shows that for any two points $p \neq q$ in K there exists a function $f \in R$ such that $f(p) = 0$ and $f(q) = 1$. If this is the case, conclude that $p \mapsto M_p$ defines a bijection from K to the set of maximal ideals of R. (The set of maximal ideals of a commutative ring R is called the *maximal spectrum* of R; it is contained in the (prime) spectrum $\operatorname{Spec} R$ defined in §4.3. Relating commutative rings and 'geometric' entities such as topological spaces is the business of *algebraic geometry*.)

The compactness hypothesis is necessary: cf. Exercise V.3.10. [V.3.10]

- **p.160, bottom:**

Example 5.10. If r is in the center of R and M is an R-module, then $rM = \{rm \mid m \in M\}$ is a submodule of M. If I is any (left-)ideal of R, then $IM = \{\sum_i r_i m_i \mid r_i \in I, m_i \in M\}$ is a submodule of M.

- p.162, Proposition 5.17:

Proposition 5.17. *Let N be a submodule of an R-module M, and let P be a submodule of M containing N. Then P/N is a submodule of M/N, and*

$$\frac{M/N}{P/N} \cong \frac{M}{P}.$$

- p.163, Exercise 5.5:

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

- p.163, Exercise 5.6:

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. (Hint: First prove that every nonidentity element of G has necessarily infinite order. Alternative hint: The unique ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism.)

- p.163, Exercise 5.11:

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 on M (extending the given R-module structure) and $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. [§VI.7.1]

- p.164, Exercise 5.17:

5.17. ▷ Let R be a commutative ring, and let I be an ideal of R. Noting that $I^j \cdot I^k \subseteq I^{j+k}$, define a ring structure on the direct sum

---

- p.167, bottom half:

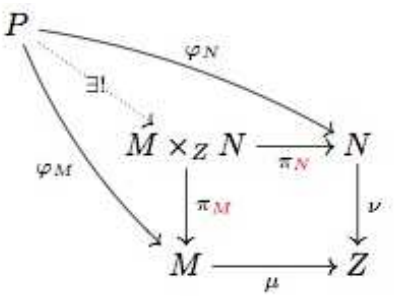
By the way, whatever happened to the conditions characterizing monomorphisms and epimorphisms in Set (Proposition I.2.1)? In Set, a function with nonempty source is a monomorphism if and only if it has a left-inverse, and it is an epimorphism if and only if it has a right-inverse. We have learned not to expect any

---

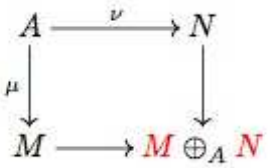
- p.173, top:

such that $\alpha = \varphi \circ \beta$. (Free modules are *projective*, as we will see in Chapter VIII.) [7.8, VI.5.5]

- p.173, Exercise 6.10:



- p.173, Exercise 6.11:



- p.174, Exercise 6.17:
  - Prove that $\mathrm{Hom}_{R\text{-Mod}}(M,N) \cong \{n \in N \mid (\forall a \in I), an = 0\}$.
  - For $a, b \in \mathbb{Z}$, prove that $\mathrm{Hom}_{\mathsf{Ab}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}$.

- p.179, bottom:

where $L_\bullet$ is the complex $0 \longrightarrow L_1 \xrightarrow{\lambda} L_0 \longrightarrow 0$, etc. The snake lemma

---

- p.181, middle:
  - Finally, let $f \in \operatorname{coker} \lambda$ be the image of e.

- p.184, Exercise 7.11:

7.11. ▷ Let

$$(*) \qquad 0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

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 $N \to M_1 \oplus M_2$ making

---

- **p.184, Exercise 7.12:**

7.12. ¬ Practice your diagram chasing skills by proving the 'four-lemma': if

$$\begin{array}{ccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} \\ A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, α is an epimorphism, and β, δ are monomorphisms, then γ is a monomorphism. [7.13, IX.2.3]

- **p.185, Exercise 7.13:**

7.13. Prove another[37] version of the 'four-lemma' of Exercise 7.12: if

$$\begin{array}{ccccccc} B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\epsilon} \\ B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 & \longrightarrow & E_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, β and δ are epimorphisms, and ϵ is a monomorphism, then γ is an epimorphism.

-

Chapter IV

- p.195, bottom half:

Proof of Theorem 2.1. Consider the set S of ordered p-tuples of elements of G:

$$(a_1, \ldots, a_p)$$

such that $a_1 \cdots a_p = e$. We claim that $|S| = |G|^{p-1}$: indeed, once $a_1, \ldots, a_{p-1}$ are chosen (arbitrarily), then a_p is determined as it is the inverse of $a_1 \cdots a_{p-1}$.

Therefore, p divides the order of S as it divides the order of G.

Also note that if $a_1 \cdots a_p = e$, then

$$a_2 \cdots a_p a_1 = e$$

(even if G is not commutative): because if a_1 is a left-inverse to $a_2 \cdots a_p$, then it is also a right-inverse to it.

Therefore, we may act with the group $\mathbb{Z}/p\mathbb{Z}$ on S: given $[m]$ in $\mathbb{Z}/p\mathbb{Z}$, with $0 \leq m < p$, act by $[m]$ on

$$(a_1, \ldots, a_p)$$

by sending it to

$$(a_{m+1}, \ldots, a_p, a_1, \ldots, a_m) :$$

as we just observed, this is still an element of S.

Now Corollary 1.3 implies

$$|Z| \equiv |S| \equiv 0 \mod p,$$

where Z is the set of fixed points of this action. Fixed points are p-tuples of the form

$$(*) \qquad (a, \ldots, a);$$

and note that $Z \neq \emptyset$, since $\{e, \ldots, e\} \in Z$. Since $p \geq 2$ and p divides $|Z|$, we conclude that $|Z| > 1$; therefore there exists some element in Z of the form (*), with $a \neq e$.

- p.196, Definition 2.3:

Definition 2.3. A group G is *simple* if it is nontrivial and its only normal subgroups are $\{e\}$ and G itself. ⌟

- p.196, first paragraph of 2.2:

2.2. Sylow I. Let p be a prime integer. A *p-Sylow subgroup* of a finite group G is a subgroup of order p^r, where $|G| = p^r m$ and $\gcd(p, m) = 1$. That is, $P \subseteq G$ is a p-Sylow subgroup if it is a p-group and p does not divide $[G : P]$.

- p.196, second paragraph of 2.2:

If p does *not* divide the order of G, then G contains a p-Sylow subgroup: namely,

---

- p.197, second to last paragraph:

One can be more precise: the second Sylow theorem tells us that *every* maximal p-group in G is in fact a p-Sylow subgroup. It is as large as is allowed by Lagrange's theorem.

- p.199, Theorem 2.11:

Theorem 2.11 (Third Sylow theorem)**.** *Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p does not divide m. Then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p.*

- p.201, middle:

Since H is normal, conjugation gives an action of G on H, hence (by Exercise 1.21) a homomorphism $\gamma : G \to \mathrm{Aut}(H)$. Now H is cyclic of order p, so $|\mathrm{Aut}(H)| = p - 1$ (Exercise II.4.14); the order of $\gamma(G)$ must divide both pq and $p - 1$, and it follows that γ is the trivial map.

- p.201, bottom half:

The condition $q \not\equiv 1 \bmod p$ in Claim 2.16 is clearly necessary: indeed, $|S_3| = 2 \cdot 3$ is the product of two distinct primes, and yet S_3 is *not* cyclic. The argument given in the proof shows that if $|G| = pq$, with $p < q$ prime, and G has a normal subgroup

---

- **p.203, Exercise 2.4:**

2.4. ▷ Prove that a nontrivial finite 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). (Note: One implication is true for arbitrary groups, while $\mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$ is a non-simple group which is isomorphic to its nontrivial homomorphic images, as the reader may enjoy verifying.) [§3.2]

- p.203, Exercise 2.13:

2.13. ¬ Let P be a p-Sylow subgroup of a finite group G.

- Prove that if P is normal in G, then it is in fact characteristic in G (cf. Exercise 2.2).
- Let $H \subseteq G$ be a subgroup containing the Sylow subgroup P. Assume P is normal in H and H is normal in G. Prove that P is normal in G.
- Prove that $N_G(N_G(P)) = N_G(P)$.

- **p.205, Exercise 2.22:**

2.22. Let G be a finite noncommutative group, $n = |G|$, and p be a prime divisor of n. Assume that the only divisor of n that is congruent to 1 modulo p is 1. Prove that G is not simple.

- p.205, Exercise 2.23:

2.23. ¬ Let N_p denote the number of p-Sylow subgroups of a group G. Prove that if G is simple, then $|G|$ divides $N_p!$ for all primes p in the factorization of $|G|$. More generally, prove that if G is simple and H is a subgroup of G of index $N > 1$, then $|G|$ divides $N!$. (Hint: Exercise II.9.12.) This problem capitalizes on the idea behind Example 2.15. [2.25]

- p.205, Exercise 2.25:

2.25. ¬ Assume that G is a *simple* group of order 60.

- Use Sylow's theorems and simple numerology to prove that G has either five or fifteen 2-Sylow subgroups, accounting for fifteen elements of order 2 or 4. (Exercise 2.23 will likely be helpful.)
- Show that in fact G has *exactly five* 2-Sylow subgroups.

Conclude that every simple group[10] of order 60 contains a subgroup of index 5. [4.22]

- p.205, bottom:

$\ell(G) = 0$ if and only if G is trivial, and $\ell(G) = 1$ if and only if G is *simple:* for a simple group, the only maximal normal series is

$$G \supsetneq \{e\}.$$

- p.206, top:

if a normal series has maximal length $\ell(G)$, then it is a composition series. What is *not* clear is that the converse holds: conceivably, there could exist composition series of different lengths (the longest ones having length $\ell(G)$). For example, why

---

- p.207, top:

be a composition series for K. (We will see in Proposition 3.4 that K does have a composition series.) By Proposition II.8.11 (the "second isomorphism theorem"),

---

- p.209, top:

the kernel is clearly $G_{i+1} \cap N$; therefore (by the first isomorphism theorem) we have an injective homomorphism

---

- p.209, middle:

this is *surjective* (check!), and the subgroup G_{i+1} of the source is sent to the identity element in the target; hence (by Theorem II.7.12) there is an onto homomorphism

$$\frac{G_i}{G_{i+1}} \twoheadrightarrow \frac{G_i N}{G_{i+1} N}.$$

Since G_i/G_{i+1} is simple, it follows that $(G_i N)/(G_{i+1} N)$ is either trivial or isomorphic to it (Exercise 2.4), as needed.

- p.209, before Proposition 3.5:

One nice consequence of the Jordan-Hölder theorem is the following observation. A series is a *refinement* of another series if all terms of the second appear in the first.

- p.212, Corollary 3.13:

Corollary 3.13. *Let N be a normal subgroup of a finite group G. Then G is solvable if and only if both N and G/N are solvable.*

- p.212, bottom:

It is worth mentioning that *every* subgroup H of a solvable group is solvable: indeed, the commutator H' of H is a subgroup of the commutator G' of G, hence $H'' \subseteq G''$, $H''' \subseteq G'''$, and so on.

The *Feit-Thompson* theorem asserts that every finite group of *odd* order is solvable. This result is many orders of magnitude beyond the scope of this book: the original 1963 proof runs about 250 pages.

- p.220, Lemma 4.12:

Proof. This follows immediately from the facts that ϵ is a homomorphism and the sign of a transposition is -1: indeed, (ij) acts on Δ_n by permuting its factors and changing the sign of an odd number of factors (for $i < j$, the factor $(x_i - x_j)$ and the pairs of factors $(x_i - x_k)$, $(x_k - x_j)$ for all $i < k < j$). □

- p.221, top half:

If $Z_{S_n}(\sigma) \not\subseteq A_n$, then note that $A_n Z_{S_n}(\sigma) = S_n$: indeed, $A_n Z_{S_n}(\sigma)$ is a subgroup of S_n (because A_n is normal; cf. Proposition II.8.11), and it properly contains A_n, so it must equal S_n as A_n has index 2 in S_n. By index considerations (cf. Exercise II.8.21)

$$[A_n : Z_{A_n}(\sigma)] = [A_n : A_n \cap Z_{S_n}(\sigma)] = [A_n Z_{S_n}(\sigma) : Z_{S_n}(\sigma)] = [S_n : Z_{S_n}(\sigma)],$$

- p.224, middle:

In particular, S_5 is a nonsolvable group of order 120. This is in fact the smallest order of a nonsimple, nonsolvable group; cf. Exercise 3.16.

- p.226, Exercise 4.19:

4.19. Prove that for $n \geq 5$ there are no nontrivial actions of A_n on any set S with $|S| < n$. Construct[21] a nontrivial action of A_4 on a set S, $|S| = 3$. Is there a nontrivial action of A_4 on a set S with $|S| = 2$?

- p.226, Exercise 4.22:

4.22. ¬ Verify that A_5 is the *only* simple group of order 60, up to isomorphism. (Hint: By Exercise 2.25, a simple group G of order 60 contains a subgroup of index 5. Use this fact to construct a homomorphism $G \to S_5$, and prove that the image of this homomorphism must be A_5.) [2.25]

- p.227, top:

$[n, h] \in N$; the second expression and the normality of H show that $[n, h] \in H$. $\square$

- **p.229, Definition 5.6:**

Definition 5.6. An exact sequence of groups

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

(or the corresponding extension) is said to *split* if ψ has a right inverse. ⌟

In this case H may be identified with a subgroup of G so that $N \cap H = \{e\}$.

- p.232, proof of Proposition 5.11:

by $\varphi(n, h) = nh$; this is clearly a bijection. We need to verify that φ is a homomorphism, and indeed $(\forall n_1, n_2 \in N)$, $(\forall h_1, h_2 \in H)$:

- **p.233, Exercise 5.3**:

5.3. Let

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = \{e\}$$

be a normal series. Show how to 'connect' $\{e\}$ to G by means of r exact sequences of groups using the groups G_i and the quotients $H_i = G_i/G_{i+1}$.

- **p.234, bottom half:**

5.15. ▷ Let G be a group of order 28.

- Prove that G contains a normal subgroup N of order 7.
- Recall (or prove again) that, up to isomorphism, the only groups of order 4 are C_4 and $C_2 \times C_2$. Prove that there are two homomorphisms $C_4 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ and two homomorphisms $C_2 \times C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ up to the choice of generators for the sources.
- Conclude that there are four groups of order 28 up to isomorphism: the two direct products $C_4 \times C_7$, $C_2 \times C_2 \times C_7$, and two noncommutative groups.
- Prove that $D_{28} \cong C_2 \times D_{14}$. The other noncommutative group of order 28 is a *generalized quaternionic group*.

- p.234, Exercise 5.17:

5.17. Prove that the multiplicative group $\mathbb{H}^*$ of nonzero quaternions (cf. Exercise III.1.12) is isomorphic to a semidirect product $\mathrm{SU}(2) \rtimes \mathbb{R}^+$. (Hint: Exercise III.2.5.) Is this semidirect product in fact direct?

- p.237, Theorem 6.6:

$$G \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{ij}}\mathbb{Z}};$$

- p.239, Lemma 6.9:

Lemma 6.9. *Let G be a finite abelian group, and assume that for every integer $n > 0$ the number of elements $g \in G$ such that $ng = 0$ is at most n. Then G is cyclic.*

- p.239, middle:

$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$

- p.239, Theorem 6.10:

Theorem 6.10. *Let F be a field, and let G be a finite subgroup of the multiplicative group $(F^*, \cdot)$. Then G is cyclic.*

- p.241, Exercise 6.8:

6.8. ¬ Let G be a finite abelian p-group, with elementary divisors $p^{n_1}, \ldots, p^{n_r}$ ($n_1 \geq n_2 \geq \cdots$). Prove that G has a subgroup H with elementary divisors $p^{m_1}, \ldots, p^{m_s}$

- p.241, Exercise 6.10:

In §VIII.6.5 we will encounter another notion of 'dual' of a group.

-

Chapter V

- p.244, first paragraph of 1.1:

is an exact sequence of R-modules, then M is Noetherian if and only if both N and P are Noetherian (Proposition III.6.7, restated here using the language introduced in §III.7.1). An easy and useful consequence of this fact is that every finitely generated module over a Noetherian ring is Noetherian (Corollary III.6.8).

- p.245, top half:

chain as follows: let N_1 be any element of $\mathscr{F}$; since N_1 is not maximal in $\mathscr{F}$, there exists an element N_2 of $\mathscr{F}$ such that $N_1 \subsetneq N_2$; since N_2 is not maximal in $\mathscr{F}$, there exists an element N_3 of $\mathscr{F}$ such that $N_2 \subsetneq N_3$; etc. The chain

$$N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$$

does not stabilize, showing that (2) does not hold.

(3) $\Longrightarrow$ (1): Assume (3) holds, and let N be a submodule of M. Then the family $\mathscr{F}$ of *finitely generated* submodules of N is nonempty (as $(0) \in \mathscr{F}$); hence it has a maximal element N'. Say that $N' = \langle n_1, \ldots, n_r \rangle$. Now we claim that $N' = N$: indeed, let $n \in N$; the submodule $\langle n_1, \ldots, n_r, n \rangle$ is finitely generated, and therefore it is in $\mathscr{F}$; as it contains N' and N' is maximal, necessarily $\langle n_1, \ldots, n_r, n \rangle = N'$; in particular $n \in N'$, as needed.

This shows that $N = N'$ is finitely generated, and since $N \subseteq M$ was arbitrary, this implies that M is Noetherian. □

- p.246, middle:

has degree $< d$. (If $\deg \alpha(x) < d$ to begin with, we may choose $\beta_1(x) = \cdots = \beta_r(x) = 0$ with the same result.) But this places this element in $M \cap I$; therefore $\exists c_1, \ldots, c_s \in R$ such that

---

- **p.247, top half**:

Incidentally, here the reader sees why it is convenient to restrict our attention to integral domains. This argument really shows that if $(a) = (b) \neq (0)$ in an integral domain, and $b = ca$, then c is necessarily a unit. Away from the comfortable environment of integral domains, even such harmless-looking statements may fail: in $\mathbb{Z}/6\mathbb{Z}$ the classes $[2]_6$, $[4]_6$ of 2 and 4 are associates according to our definition, and $[4]_6 = [2]_6 \cdot [2]_6$, yet $[2]_6$ is not a unit. However, $[4]_6 = [5]_6 \cdot [2]_6$ and $[5]_6$ *is* a unit, so this is not a counterexample to Lemma 1.5. In fact, Lemma 1.5 may fail over rings with 'non-harmless' zero-divisors (yes, there is such a notion).

The notions reviewed above generalize directly the corresponding notions in $\mathbb{Z}$. We are going to explore analogs of other common notions in $\mathbb{Z}$, such as 'primality' and 'irreducibility', in more general integral domains.

- p.247, bottom half:

Note that 0 is always reducible (integral domains are nonzero rings!). For nonzero elements, there are useful alternative ways to think about the notion of 'irreducible': a nonunit $a \neq 0$ is irreducible if and only if

---

- p.247, bottom half:

It is important to realize that primality and irreducibility are *not equivalent,* even for nonzero elements; this is somewhat counterintuitive since they *are* equivalent in $\mathbb{Z}$, as the reader should verify[2] (Exercise 1.13). What *is* true in general is that *prime* is stronger than *irreducible:*

- **p.250, Exercise 1.12**:

1.12. ▷ Let R be an integral domain. Prove that a nonzero $a \in R$ is irreducible if and only if (a) is maximal among proper principal ideals of R. [§1.2, §2.3]

- **p.250, Exercise 1.13**:

1.13. ▷ Prove that, for nonzero elements, prime $\iff$ irreducible in $\mathbb{Z}$. [§1.2, §2.3]

- p.251, Exercise 1.17:

1.17. ▷ Consider the subring of $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

- Prove that this ring is isomorphic to $\mathbb{Z}[t]/(t^2 + 5)$.

- p.255, middle:

Proposition 2.6 justifies another feature of the picture given at the beginning of this chapter: the class of PIDs is contained in the class of UFDs. We will soon see that the inclusion is proper, that is, that there are UFDs which are not PIDs;

- p.257, bottom:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\dots \end{aligned}$$

- p.258, top half:

Thus the table of divisions with remainders must be as follows: letting $r_0 = b$,

$$\begin{aligned} a &= r_0 q_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\dots \\ r_{N-3} &= r_{N-2} q_{N-1} + r_{N-1}, \\ r_{N-2} &= r_{N-1} q_N \end{aligned}$$

with $r_{N-1} \neq 0$.

- p.259, Exercise 2.10:

2.10. ¬ It is a consequence of a theorem known as *Krull's Hauptidealsatz* that every nonzero, nonunit element in a Noetherian domain is contained in a prime ideal of height 1. Assuming this, prove a converse to Exercise 2.9, and conclude that a Noetherian domain R is a UFD if and only if every prime ideal of height 1 in R is principal. [4.16]

- p.260, Exercise 2.19:

2.19. ¬ A *discrete valuation* on a field k is a surjective homomorphism of abelian groups $v : (k^*, \cdot) \to (\mathbb{Z}, +)$ such that $v(a+b) \geq \min(v(a), v(b))$ for all $a, b \in k^*$ such that $a + b \in k^*$.

- p.260, Exercise 2.20:

2.20. ¬ As seen in Exercise 2.19, DVRs are Euclidean domains. In particular, they must be PIDs. Check this directly, as follows. Let R be a DVR, and let $t \in R$ be an element such that $v(t) = 1$. Prove that if $I \subseteq R$ is any nonzero ideal, then $I = (t^k)$ for some $k \geq 0$. (The element t is called a 'local parameter' of R.) [4.13, VII.2.18]

- p.261, first paragraph of 3.1:

of objects. However, we will occasionally need to refer to a less 'intuitively obvious' set-theoretic statement: for example, this statement is needed in order to show that every proper ideal in a ring is contained in a maximal ideal (Proposition 3.5).

- p.264, bottom:

3.2. Application: Existence of maximal ideals. Recall (§III.4.3) that an ideal $\mathfrak{m}$ of a ring R is *maximal* if and only if $R/\mathfrak{m}$ is a field, if and only if no other ideal stands between $\mathfrak{m}$ and $R = (1)$, that is, if and only if $\mathfrak{m}$ is maximal with respect to inclusion, in the family of proper ideals of R. It is not obvious from this definition that maximal ideals *exist,* but they do:

- p.265, Proof of Proposition 3.5:

To verify our claim, it is clear that U contains I and that it is an ideal (for example, if $a, b \in U$, then $\exists J \in \mathscr{C}$ such that $a, b \in J$; hence $a \pm b \in J$, and therefore

---

- **p.267, Exercise 3.13:**

3.13. ¬ Let R be a commutative ring, and let N be its nilradical (Exercise III.3.12). Let $r \notin N$.

- Consider the family $\mathscr{F}$ of ideals of R that do not contain any power r^k of r for $k > 0$. Prove that $\mathscr{F}$ has maximal elements.
- Let I be a maximal element of $\mathscr{F}$. Prove that I is prime.
- Conclude $r \notin N \implies r$ is not in the intersection of all prime ideals of R.

Together with Exercise III.4.18, this shows that the nilradical of a commutative ring R equals the intersection of all prime ideals of R. [III.4.18, VII.2.8]

- p.267, Exercise 3.15:

- If $\mathscr{F} \neq \emptyset$, prove that it has a maximal element I.
- Prove that R/I is Noetherian.
- Prove that there are ideals J_1, J_2 properly containing I, such that $J_1 J_2 \subseteq I$.
- Give a structure of R/I module to I/J_1J_2 and J_1/J_1J_2.
- Prove that I/J_1J_2 is a finitely generated R/I-module.
- Prove that I is finitely generated, thereby reaching a contradiction.

- p.269, bottom:

approach and deal with principal ideals throughout, rather than with individual (but only defined up to unit) elements. The reader should keep in mind that ideals may be multiplied (cf. §III.4.1), and if (a), (b) are principal ideals, then their product $(a)(b)$ is the principal ideal (ab).

- p.272, middle:

for all $\frac{r}{s} \neq \frac{0}{1}$ (that is, for all $r \neq 0$), every nonzero element in $K(R)$ has an inverse,

---

- p.274, proof of Lemma 4.15:

in $R[x]$. By Gauss's lemma and since $\underline{h}$ is primitive,

$$(a \operatorname{cont}_f) = (b \operatorname{cont}_g);$$

- p.277, bottom:

  - If $\ell : R \to S^{-1}R$ is the natural homomorphism, prove that if J is a proper ideal of $S^{-1}R$, then $J^c := \ell^{-1}(J)$ is an ideal of R such that $J^c \cap S = \emptyset$.

- **p.278, Exercise 4.10:**

4.10. ¬ With notation as in Exercise 4.9, prove that the assignment $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives an inclusion-preserving bijection between the set of *prime* ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$. (Prove that $(\mathfrak{p}^e)^c = \mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal disjoint from S.) [4.16]

- p.278, Exercise 4.12:

(Hint: For the interesting implication, suppose that $m \neq 0$ in M; then the ideal $\{r \in R \,|\, rm = 0\}$ is proper. By Proposition 3.5, it is contained in a maximal ideal $\mathfrak{m}$. What can you say about $M_{\mathfrak{m}}$?) [VIII.1.26, VIII.2.21]

- p.280, Exercise 4.25:

The same pattern of proof would work in any environment where unique factorization is available; if adjoining to $\mathbb{Z}$ a primitive n-th root of 1 and roots of other elements as needed in this argument led to a unique factorization domain, the full-fledged Fermat's last theorem would be as easy to prove as indicated in this exercise. This is not the case, a fact famously missed by G. Lamé as he announced a 'proof' of Fermat's last theorem to the Paris Academy on March 1, 1847.

- p.281, top:

5.1. Roots and reducibility. Let R be a ring and $f \in R[x]$. An element $a \in R$ is a *root of f* if $f(a) = 0$. Recall (Example III.4.7) that a polynomial $f(x) \in R[x]$ is divisible by $(x - a)$ if and only if a is a root of f. More generally, we say that a is a root of f with *multiplicity* r if $(x - a)^r$ divides f and $(x - a)^{r+1}$ does *not* divide f.

- p.282, top:

The innocent Lemma 5.1 has important applications: for example, we used it (without much fanfare) in the proof of Theorem IV.6.10. Also, recall that a polynomial $f \in R[x]$ determines an 'evaluation function' (cf. Example III.2.3) $R \to R$, namely $r \mapsto f(r)$. The reader checked in Exercise III.2.7 that in general the

---

- p.285, Lemma 5.10:

Lemma 5.10. *A field k is algebraically closed if and only if every nonconstant polynomial $f \in k[x]$ factors completely as a product of linear factors, if and only if every nonconstant polynomial $f \in k[x]$ has a root in k.*

- p.286, top:

'Algebraic' proofs of the fundamental theorem of algebra require more than we know at this point (we will encounter one in §VII.7, after we have seen a little Galois theory); curiously, a little *complex analysis* makes the statement nearly trivial. Here

---

- **p.288, Proof of Proposition 5.17:**

Proof. Argue by contradiction. Assume $f = gh$ in $R[x]$, with both $d = \deg g$ and $e = \deg h$ less than $n = \deg f$; write

$$g = b_0 + b_1 x + \cdots + b_d x^d, \quad h = c_0 + c_1 x + \cdots + c_e x^e.$$

Consider f modulo $\mathfrak{p}$: thus

$$\underline{f} = \underline{g}\,\underline{h} \quad \text{in } (R/\mathfrak{p})[x],$$

where $\underline{f}$ denotes f modulo $\mathfrak{p}$, etc.

By hypothesis, $\underline{f} = \underline{a}_n x^n$ modulo $\mathfrak{p}$, where $\underline{a}_n \neq 0$ in $R/\mathfrak{p}$. Since $R/\mathfrak{p}$ is an integral domain, factors of $\underline{f}$ must also be monomials: that is, necessarily

$$\underline{g} = \underline{b}_{d'} x^{d'}, \quad \underline{h} = \underline{c}_{e'} x^{e'}$$

with $d' \leq d < n$, $e' \leq e < n$. Since $d' + e' = n$, we have $d' > 0$, $e' > 0$, and this implies $b_0 \in \mathfrak{p}$, $c_0 \in \mathfrak{p}$.

But then $a_0 = b_0 c_0 \in \mathfrak{p}^2$, contradicting the hypothesis. □

- **p.289, Exercise 5.1:**

5.1. ¬ Let $f(x) \in \mathbb{C}[x]$. Prove that $a \in \mathbb{C}$ is a root of f with multiplicity r if and only if $f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0$ and $f^{(r)}(a) \neq 0$, where $f^{(k)}(a)$ denotes the value of the k-th derivative of f at a. Deduce that $f(x) \in \mathbb{C}[x]$ has multiple roots if and only if $\gcd(f(x), f'(x)) \neq 1$. [5.2]

- p.289, Exercise 5.3:

5.3. Let R be a ring, and let $f(x) = a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \cdots + a_2x^2 + a_0 \in R[x]$ be a polynomial only involving *even* powers of x. Prove that if $g(x)$ is a factor of $f(x)$, so is $g(-x)$.

- p.290, Exercise 5.8:

5.8. ¬ Let K be a field, and let $a_0, \ldots, a_d$ be distinct elements of K. Given any elements $b_0, \ldots, b_d$ in K, construct explicitly a polynomial $f(x) \in K[x]$ of degree at most d such that $f(a_0) = b_0, \ldots, f(a_d) = b_d$, and show that this polynomial is unique. (Hint: First solve the problem assuming that only one b_i is not equal to zero.) This process is called *Lagrange interpolation*. [5.9]

- p.290, Exercise 5.11:

5.11. ▷ Let F be a finite field. Prove that there are irreducible polynomials in $F[x]$ of arbitrarily high degree. (Hint: Exercise 2.24.) [§5.3]

- p.292, proof of Lemma 6.2:

Proof. A simple induction (based on the case $k = 3$ of Lemma 6.3 below) reduces the general statement to the case $k = 2$. Therefore, assume I and J are ideals of R, such that $I + J = (1)$. The inclusion $IJ \subseteq I \cap J$ holds for all ideals I, J, so the task amounts to proving $I \cap J \subseteq IJ$ when $I + J = (1)$.

- p.292, proof of Lemma 6.3:

Proof. By hypothesis, for $i = 1, \ldots, k-1$ there exists $a_i \in I_k$ such that $1 - a_i \in I_i$.

- p.295, bottom:

Let $z, w \in \mathbb{Z}[i]$, and assume $w \neq 0$. The ideal (w) is a lattice superimposed on $\mathbb{Z}[i]$. The given z is either one of the vertices of this lattice (in which case z is a multiple of w, so that the division z/w can be performed in $\mathbb{Z}[i]$, with remainder 0) or it sits inside one of the 'boxes' of the lattice. In the latter case, pick any vertex of the box on the side closest to z; this is a multiple qw of w, and let $r = z - qw$. The situation may look as follows:

- p.299, middle:

is an even number, say 2ℓ: thus g has order $|G| = 2\ell$. Also, denote the class of an integer n mod (p) by $\underline{n}$. Since g is a generator of G, for every integer $n \notin (p)$ there is an integer m such that $\underline{n} = g^m$.

- p.300, Exercise 6.3:

6.3. Recall (Exercise III.3.15) that a ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Let R be a finite Boolean ring; prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

- p.301, third bullet of Exercise 6.8:

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

---

- p.301, Exercise 6.9:

6.9. Let I be a nonzero ideal of $\mathbb{Z}[i]$. Prove that $\mathbb{Z}[i]/I$ is finite.

- p.301, Exercise 6.12:

6.12. ¬ Prove Lemma 6.5 without any 'visual' aid. (Hint: Let $z = a+bi$, $w = c+di$ be Gaussian integers, with $w \neq 0$. Then $z/w = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$. Find integers e, f such that $|e - \frac{ac+bd}{c^2+d^2}| \leq \frac{1}{2}$ and $|f - \frac{bc-ad}{c^2+d^2}| \leq \frac{1}{2}$, and set $q = e + if$. Prove that $|\frac{z}{w} - q| < 1$. Why does this do the job?) [6.13]

- p.303, Exercise 6.21:

  - Let $z \in \mathbb{I}$ and $n \in \mathbb{Z}$. Prove that the greatest common right-divisor of z and n in $\mathbb{I}$ is 1 if and only if $(N(z), n) = 1$ in $\mathbb{Z}$. (If $\alpha z + \beta n = 1$, then $N(\alpha)N(z) = N(1-\beta n) = (1-\beta n)(1-\overline{\beta} n)$, where $\overline{\beta}$ is obtained by changing the signs of the coefficients of i, j, k. Expand, and deduce that $(N(z), n) \mid 1$.)

-

Chapter VI

- p.308, top:

Bases are necessarily maximal linearly independent subsets and minimal generating subsets; this holds over every ring. What will make modules over a *field*,

---

- p.311, middle:

Proposition 1.9 tells us that every linearly independent subset S of a free R-module M must have cardinality lower than or equal to $\mathrm{rk}_R M$. Similarly, every *generating set* must have cardinality *higher* than or equal to the rank. Indeed,

---

- p.312, Exercise 1.3:

1.3. Prove that $\mathfrak{su}(2) \cong \mathfrak{so}_3(\mathbb{R})$ as $\mathbb{R}$-vector spaces. (This is immediate, and not particularly interesting, from the dimension computation of Exercise 1.2. However, these two spaces may be viewed as the tangent spaces to $\mathrm{SU}(2)$, resp., $\mathrm{SO}_3(\mathbb{R})$, at I ; the surjective homomorphism $\mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$ you constructed in Exercise II.8.9 induces a more 'meaningful' isomorphism $\mathfrak{su}(2) \to \mathfrak{so}_3(\mathbb{R})$. Can you find this isomorphism?)

- p.312, Exercise 1.4:

  - $\mathfrak{su}(2)$ and $\mathfrak{so}_3(\mathbb{R})$ are isomorphic as Lie algebras over $\mathbb{R}$.

- p.313, Exercise 1.15:

Show that there is an R-module homomorphism $\varphi : F \to F$ such that $\operatorname{im} \varphi^{n+1} \subsetneq \operatorname{im} \varphi^n$ for all $n \geq 0$.

- p.316, top:

In particular, we have a binary operation on the abelian group $\mathcal{M}_n(R)$ of *square* $n \times n$-matrices, and this operation is associative, distributive w.r.t. $+$, and admits the identity element

---

- p.317, footnote:

[9]Here we are reversing the order of the Hom sets on the left w.r.t. the convention used in Definition I.3.1.

- p.319, bottom:

For example, let's work out the action of a change of basis on the matrix representation of a homomorphism $\alpha : F \to G$ of two free modules. The diagram taking care of the needed manipulations is

---

- p.334, proof of Claim 3.10:

Proof. Let $n = \dim V$ and $m = \dim W$. By Proposition 2.10 we can represent α by an $m \times n$ matrix of the form

---

- p.349, Exercises 4.15-4.16:

4.15. ▷ View $\mathbb{Z}$ as a module over the ring $R = \mathbb{Z}[x, y]$, where x and y act by 0. Find a free resolution of $\mathbb{Z}$ over R. [VIII.4.21]

4.16. ▷ Let $\varphi : R^n \to R^m$ and $\psi : R^p \to R^q$ be two R-module homomorphisms, and let

$$\varphi \oplus \psi : R^n \oplus R^p \to R^m \oplus R^q$$

be the morphism induced on direct sums. Prove that

$$\operatorname{coker}(\varphi \oplus \psi) = \operatorname{coker} \varphi \oplus \operatorname{coker} \psi.$$

- p.350, Lemma 5.2:

Lemma 5.2. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a nonzero submodule. Then there exist $a \in R$, $x \in F$, $y \in M$, and submodules $F' \subseteq F$ and $M' \subseteq M$, such that $y = ax \neq 0$, $M' = F' \cap M$, and*

$$F = \langle x \rangle \oplus F', \quad M = \langle y \rangle \oplus M'.$$

- p.351, middle:

Since R is a PID, $\alpha(M)$ is principal: $\alpha(M) = (a)$ for some $a \in R, a \neq 0$. Since $a \in \alpha(M)$, there exists an element $y \in M$, $y \neq 0$, such that $\alpha(y) = a$. These are the elements a, y mentioned in the statement.

- p.354, Theorem 5.6:
  - *There exist distinct prime ideals $(q_1), \ldots, (q_n) \subsetneq R$, positive integers r_{ij}, and an isomorphism*

- p.356, middle:

$$\frac{R}{(q^{r_1})} \oplus \cdots \oplus \frac{R}{(q^{r_m})} \cong \frac{R}{(q^{s_1})} \oplus \cdots \oplus \frac{R}{(q^{s_n})},$$

- p.358, Exercise 5.8:

If R is a PID, then N may be chosen so that $0 \to N \to M \to M/N \to 0$ splits.

- p.364, bottom:

$$(A - I)^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

- p.367, bottom:

Contemplating this example will convince the reader that the geometric multiplicity of an eigenvalue is always *less than or equal to* its algebraic multiplicity. In the neatest possible situation, and working over a field for simplicity, an operator α on a vector space V of dimension n may have all its n eigenvalues in the base field, and each algebraic multiplicity may agree with the corresponding geometric multiplicity. If this is the case, V may then be expressed as a direct sum of the eigenspaces, producing the so-called *spectral decomposition* of V determined by α (cf. Exercise 6.15 for a concrete instance of this situation). The action of α on V is then completely transparent, as it amounts to simply applying a different scaling factor on each piece of the spectral decomposition.

- p.368, Exercise 6.4:

6.4. ▷ Let F be a finitely generated free R-module, and let α be a linear transformation of F. Give an example of an injective α which is not surjective; in fact, prove that α is not surjective precisely when $\det \alpha$ is not a unit. [§6.2]

- p.370, top:

combination $r_1\mathbf{v}_{i_1} + \cdots + r_m\mathbf{v}_{i_m} = 0$ with all $r_j \in R$, $r_j \neq 0$. Compare the action of α on this linear combination with the product by λ_{i_1}.)

It follows that if a vector space V has dimension n and $\alpha : V \to V$ has n distinct eigenvalues, then α induces a spectral decomposition of V. [§6.3, VII.6.14]

- p.370, Exercise 6.16:

Likewise, prove that a matrix $M \in \mathcal{M}_n(\mathbb{C})$ belongs to $\mathrm{U}(n)$ if and only if it preserves the standard hermitian product on $\mathbb{C}^n$. [6.18]

- p.370, Exercise 6.18:

Formulate and prove an analogous statement for $\mathrm{U}(n)$. (The group $\mathrm{U}(n)$ is

---

- p.370, footnote:

[32]See Exercise II.6.1 for the definitions of $O_n(\mathbb{R})$ and $U(n)$. We trust that basic facts on inner products are not new to the reader. Among these, recall that for $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, $(\mathbf{v}, \mathbf{v})$ equals the

---

- p.371, Exercise 6.21:

6.21. ¬ A matrix $M \in \mathcal{M}_n(\mathbb{R})$ is *symmetric* if $M^t = M$. Prove that M is symmetric if and only if $(\forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^n)$, $(M\mathbf{v}, \mathbf{w}) = (\mathbf{v}, M\mathbf{w})$.

A matrix $M \in \mathcal{M}_n(\mathbb{C})$ is *hermitian* if $M^\dagger = M$. Prove that M is hermitian if and only if $(\forall \mathbf{v}, \mathbf{w} \in \mathbb{C}^n)$, $(M\mathbf{v}, \mathbf{w}) = (\mathbf{v}, M\mathbf{w})$.

In both cases, one may say that M is *self-adjoint;* this means that shuttling it from one side of the product to the other does not change the result of the operation.

A hermitian matrix with real entries is symmetric. It is in fact useful to think of real symmetric matrices as particular cases of hermitian matrices. [6.22]

- p.371, Exercise 6.22:

6.22. ¬ Prove that the eigenvalues of a hermitian matrix (Exercise 6.21) are real. Also, prove that if $\mathbf{v}$, $\mathbf{w}$ are eigenvectors of a hermitian matrix, corresponding to different eigenvalues, then $(\mathbf{v}, \mathbf{w}) = 0$. (Thus, eigenvectors with distinct eigenvalues for a real symmetric matrix are orthogonal.) [7.20]

- p.378, following the proof:

The elementary divisor decomposition splits V into a different collection of cyclic modules than the decomposition in invariant factors: the basic cyclic bricks are now of the form $k[t]/(p(t)^r)$ for a monic prime $p(t)$; by Lemma 7.12, assuming that the characteristic polynomial factors completely over k, they are in fact of the form

$$\frac{k[t]}{((t-\lambda)^r)}$$

- p.383, Exercise 7.16:

7.16. *(Schur form)* Let $A \in \mathcal{M}_n(\mathbb{C})$. Prove that there exists a *unitary* matrix $P \in U(n)$ such that

---

- p.383, Exercise 7.16:

the matrix A can in fact be chosen to be in $U(n)$. (Argue inductively on n. Since

---

-

Chapter VII

- p.387, bottom:

We have always found the notation $k(\alpha)$ somewhat unfortunate, since it suggests that all such extensions are in some way isomorphic and possibly all isomorphic to the field $k(t)$ of rational functions in one indeterminate t (cf. Definition V.4.13). This is not true, although it is clear that every element of $k(\alpha)$ may be written as a rational function in α with coefficients in k (Exercise 1.3). In any case, it is easy to classify simple extensions: they are either isomorphic to $k(t)$ or they are of the prototypical kind recalled above. Here is the precise statement.

- p.388, top half:

The polynomial $p(t)$ appearing in this statement is called the *minimal polynomial* of α over k.

- p.389, Proposition 1.5:

Proposition 1.5. *Let $k_1 \subseteq F_1 = k_1(\alpha_1)$, $k_2 \subseteq F_2 = k_2(\alpha_2)$ be two finite simple extensions. Let $p_1(t) \in k_1[t]$, resp., $p_2(t) \in k_2[t]$, be the minimal polynomials of α_1, resp., α_2. Let $i : k_1 \to k_2$ be an isomorphism, such that*[4]

$$i(p_1(t)) = p_2(t).$$

Then there exists a unique isomorphism $j : F_1 \to F_2$ agreeing with i on k_1 and such that $j(\alpha_1) = \alpha_2$.

- p.391, Definition 1.8:

Definition 1.8. Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. Then α is *algebraic over k, of degree n* if $n = [k(\alpha) : k]$ is finite; α is *transcendental over k* otherwise.

The extension $k \subseteq F$ is *algebraic* if every $\alpha \in F$ is algebraic over k. ⌟

- p.393, Example 1.12:

Example 1.12. Let $k \subseteq F$ be a field extension, and let $\alpha \in F$ be an algebraic element over k, of *odd* degree. Then we claim that α may be written as a polynomial in α^2, with coefficients in k.

- p.397, Exercise 1.6:

1.6. ▷ Let $k \subseteq F$ be a field extension, and let $f(x) \in k[x]$ be a polynomial. Prove that $\mathrm{Aut}_k(F)$ acts on the set of roots of $f(x)$ contained in F. Provide examples showing that this action need not be transitive or faithful. [§1.2, §1.3]

- **p.397, Exercise 1.8:**

1.8. ¬ Let $f(x) \in k[x]$ be a polynomial over a field k of degree d, and let $\alpha_1, \dots, \alpha_d$ be the roots of $f(x)$ in an extension of k where the polynomial factors completely. For a subset $I \subseteq \{1, \dots, d\}$, denote by α_I the sum $\sum_{i \in I} \alpha_i$. Assume that $\alpha_I \in k$ only for $I = \emptyset$ and $I = \{1, \dots, d\}$. Prove that $f(x)$ is irreducible over k. [7.14]

- p.400, Exercise 1.29:

Prove that any field extension $k \subseteq F$ may be decomposed as a purely transcendental extension followed by an algebraic extension. (Not all field extensions

---

- p.402, proof of Claim 2.5:

Proof. If $f(x) \in L[x]$ is a nonconstant polynomial, then $f(x) \in K_i[x]$ for some i; hence $f(x)$ has a root in $K_{i+1} \subseteq L$. That is, every nonconstant polynomial in $L[x]$ has a root in L, as needed. □

- **p.403, top:**

By Corollary 1.16, $\overline{k}$ is a field, and the extension $k \subseteq \overline{k}$ is tautologically algebraic. To verify that $\overline{k}$ is algebraically closed, let $\overline{k} \subseteq \overline{k}(\alpha)$ be a simple algebraic extension. The minimal polynomial of α has a root in L since L is algebraically closed, so by versality (Proposition V.5.7) there exists an embedding $\overline{k}(\alpha) \subseteq L$. We can then view α as an element of L; $k \subseteq \overline{k} \subseteq \overline{k}(\alpha)$ is a composition of algebraic extensions, so $k \subseteq \overline{k}(\alpha)$ is algebraic (Corollary 1.18), and in particular α is algebraic over k. But then $\alpha \in \overline{k}$, by definition of the latter. It follows that $\overline{k}$ is algebraically closed, by Lemma 2.1. □

- p.403, bottom:

By Zorn's lemma, Z admits a maximal element i_G, corresponding to an intermediate field $k \subseteq G \subseteq F$. Let $H = i_G(G)$ be the image of G in L.

- p.404, top:

thus, it is a root of an irreducible polynomial $g(x) \in G[x]$. Consider the induced homomorphism

- p.410, top:

$$f(x_1,\dots,x_n)=\sum_{i=1}^{n} g_i(x_1,\dots,x_n)(x_i-c_i).$$

In particular,

$$f(c_1,\dots,c_n)=\sum_{i=1}^{n} g_i(c_1,\dots,c_n)(c_i-c_i)=0:$$

- p.411, top:

Indeed, assume on the contrary that $\mathscr{V}(J)\neq\emptyset$, and let $p=(a_1,\dots,a_n,b)$ in $\mathbb{A}_K^{n+1}$ be a point of $\mathscr{V}(J)$. Then for $i=1,\dots,r$

$$G_i(a_1,\dots,a_n,b)=0;$$

- p.421, proof of Lemma 3.3:

Proof. The set $\mathscr{C}_{\mathbb{R}}\subseteq\mathbb{R}$ is nonempty, so in order to show it is a field, we only need to show that it is closed with respect to subtraction and division by a nonzero constructible number (cf. Proposition II.6.2).

- p.423, bottom:

$$\begin{cases} x^2+y^2+a_1x+b_1y+c_1=0,\\ (a_1-a_2)x+(b_1-b_2)y+(c_1-c_2)=0, \end{cases}$$

- p.426, middle:

Squaring circles requires constructing $\sqrt{\pi}$. But if $\sqrt{\pi}$ were algebraic, then π would be algebraic, and it is not (although, as we have mentioned, the proof of this fact is not elementary), so this is also not possible.

- p.436, beginning of 4.3:

4.3. Separable extensions and embeddings in algebraic closures. The terminology examined in the previous section extends to the language of field extensions. If $k\subseteq F$ is an extension and $\alpha\in F$ is algebraic over k, we say that α is *separable* over k if the minimal polynomial of α over k is separable; α is *inseparable* otherwise.

- p.439, bottom:

Deduce that the set of elements of F which are separable over k form an intermediate field F_{sep}, such that every element $\alpha \in F$, $\alpha \notin F_{\text{sep}}$ is *inseparable* over F_{sep}.

- p.446, near the top:

$$\Phi_n(x) := \prod_{\zeta \text{ primitive } n\text{-th root of } 1} (x - \zeta) = \prod_{1 \le m \le n, (m,n)=1} (x - \zeta_n^m)$$

- p.447, end of proof of Corollary 5.12:

in $\mathbb{C}[x]$. Therefore

$$f(x)(\Phi_n(x) - q(x)) = r(x)$$

in $\mathbb{C}[x]$. But this forces $r(x) = 0$ (otherwise we would have $\deg r(x) \geq \deg f(x)$). Therefore $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$. □

- p.448, proof of Proposition 5.16:

Proof. We know that $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ has cardinality $\phi(n)$ (Corollary 1.7; the roots are distinct since $\Phi_n(x)$ is separable), so all we need to do is exhibit an injective homomorphism

---

- p.449, Example 5.17:

Example 5.17. The reader should consider Example 4.4 again: by what we have

---

- p.450, top:

For every $c \in k$, we have the intermediate field

$$k \subseteq k(c\alpha + \beta) \subseteq k(\alpha, \beta).$$

- p.450, bottom:

(each ι extends id_k, so $\iota(c) = c$). Since the cardinality of I is $[F : k]_s$ (Definition 4.21) and each $\iota(\gamma)$ is a root of the minimal polynomial of γ over k, we have

$$[F : k]_s \leq [k(\gamma) : k] \leq [F : k].$$

- p.452, second line of Exercise 5.7:

a linear transformation of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^d}$. Find the rational canonical form

---

- p.452, first line of Exercise 5.11:

5.11. Prove that if $n > 1$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$. (Hint: Draw the primitive

---

- p.453, top:

- For every $r \in R$, prove that the centralizer of r in the multiplicative group $(R^*, \cdot)$ has order $q^d - 1$ for some $d \leq n$.

- p.457, Proof of Theorem 6.9:

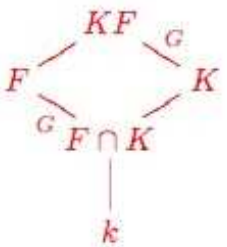
(1) $\iff$ (2) by Theorem 4.8; (2) $\implies$ (3) by Corollary 5.20. (3) $\iff$ (4) follows from Proposition 6.5, applied to the extension $F^{\mathrm{Aut}_k(F)} \subseteq F$: by Proposition 6.5, we have

$$[F : F^{\mathrm{Aut}_k(F)}] = |\mathrm{Aut}_k(F)|;$$

since $k \subseteq F^{\mathrm{Aut}_k(F)} \subseteq F$, it follows that $k = F^{\mathrm{Aut}_k(F)}$ if and only if $|\mathrm{Aut}_k(F)| = [F : k]$. (4) $\implies$ (2) by Lemma 6.6.

- p.464, middle:

Pictorially,



- p.465, bottom:

are in F, and F is generated by them; therefore F is the splitting field of the separable (since $\mathrm{char}\, k$ does not divide m) polynomial $x^m - c$ over k; hence (Theorem 6.9, part (1)) $k \subseteq F$ is Galois. Note that since $F = k(\delta)$ has degree m over k, and δ is a root of $x^m - c$, it follows that the polynomial $x^m - c$ is irreducible.

- **p.466, Exercise 6.2:**

6.2. Prove that quadratic extensions in characteristic$\neq 2$ are Galois.

- p.472, top:

$$s_1(t_1,t_2,t_3) = t_1 + t_2 + t_3,$$
$$s_2(t_1,t_2,t_3) = t_1t_2 + t_1t_3 + t_2t_3,$$
$$s_3(t_1,t_2,t_3) = t_1t_2t_3.$$

- p.474, top:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

- p.475, proof of Lemma 7.11:

For the converse, assume $f(x)$ is solvable by radicals. A formula for a root t_1

- p.476-7, Proof of Proposition 7.14:

Proof. Assume $\mathrm{Aut}_k(F)$ is solvable. Let M be a common multiple of the orders of the cyclic quotients, and let ζ be a primitive M-th root of 1 in an algebraic closure $\overline{k}$ of k. The splitting field $k(\zeta)$ of $x^M - 1$ over k is Galois over k ($x^M - 1$ is separable since k has characteristic 0). By Proposition 6.17, the extension $k(\zeta) \subseteq F(\zeta)$ is also Galois, with Galois group isomorphic to $\mathrm{Aut}_{k(\zeta)\cap F}(F)$. As $k(\zeta) \cap F$ is Galois over k (Exercise 6.13), this subgroup is normal, and it follows (Proposition IV.3.4, Corollary IV.3.13) that $\mathrm{Aut}_{k(\zeta)}(F(\zeta))$ is solvable and its cyclic quotients are among those for $\mathrm{Aut}_k(F)$. In particular, $k(\zeta) \subseteq F(\zeta)$ has enough roots of 1, and hence it is radical, by Lemma 7.13. So is $k \subseteq F(\zeta)$, since $k \subseteq k(\zeta)$ is itself trivially radical. This proves that $k \subseteq F$ is contained in a radical extension, hence in a Galois radical extension by Lemma 7.10.

Conversely, assume that $k \subseteq F$ is Galois and contained in a radical Galois extension $k \subseteq L$. Let M be a common multiple of the orders of the cyclic factors in this extension, and let ζ be a primitive M-th root of 1. The composite $L(\zeta)$ is Galois and radical over $k(\zeta)$ (Proposition 6.17 and Exercise 7.5); further, it has enough roots of 1.

- p.478, third paragraph:

To begin with, recall that an element of $\mathrm{Aut}_k(F)$ must send roots of a polynomial $f(x) \in k[x]$ to roots of the same polynomial, and if $f(x)$ is irreducible and F is its splitting field, then there are automorphisms of F sending any root of $f(x)$ to any other root (Proposition 1.5, Lemma 4.2). This observation may be rephrased as follows:

- p.481, Exercise 7.11:

$$f_n(x) := (x^2+2)\cdot x\cdot (x-2)\cdots (x-2(n-4))\cdot (x-2(n-3))$$

-

Chapter VIII

- p.489, top:

> Thus, K-Aff is defined in such a way that the functor $K\text{-Aff}^{op} \to K\text{-Alg}$ that maps an affine algebraic set S to its coordinate ring $K[S]$ is an equivalence of the *opposite* category of K-Aff with the subcategory of reduced, commutative, finite-type K-algebra.

- p.490, bottom:

> The 'dual notion' to limit is the *colimit* of a functor $\mathscr{F} : \mathsf{I} \to \mathsf{C}$. The colimit is an object C of C, endowed with morphisms $\gamma_I : \mathscr{F}(I) \to C$ for all objects I of I, such that $\gamma_I = \gamma_J \circ \mathscr{F}(\alpha)$ for all $\alpha : I \to J$ and that C is *initial* with respect to this requirement.

- p.492, bottom:

> for all objects X of C and Y of D. (More precisely, there should be a natural isomorphism of 'bifunctors' $\mathsf{C}^{op} \times \mathsf{D} \to \mathsf{Set}$: $\mathrm{Hom}_{\mathsf{C}}(\_, \mathscr{G}(\_)) \tilde{\to} \mathrm{Hom}_{\mathsf{D}}(\mathscr{F}(\_), \_)$.)

- p.495, bottom:

> is exact, then
>
> $$\mathscr{G}(A) \xrightarrow{\mathscr{G}(\varphi)} \mathscr{G}(B) \xrightarrow{\mathscr{G}(\psi)} \mathscr{G}(C) \longrightarrow 0$$
>
> is also exact. ⌟

- **p.496, Exercise 1.5:**

1.5. For F a field, denote by F^* the group of nonzero elements of F, with multiplication. The assignment $\mathsf{Fld} \to \mathsf{Grp}$ mapping F to F^* and a homomorphism of fields $\varphi : k \to F$ (i.e., a field extension[8]) to the restriction $\varphi|_{k^*} : k^* \to F^*$ is clearly a covariant functor. On the other hand, we can consider the category Fld_k^f of *finite* extensions of a fixed field k. Prove that the assignment $F \mapsto F^*$ on objects, together with the prescription associating with every $F_1 \subseteq F_2$ the *norm* $N_{F_1 \subseteq F_2} : F_2^* \to F_1^*$ (cf. Exercise VII.1.12), gives a *contravariant* functor $\mathsf{Fld}_k^f \to \mathsf{Grp}$.

State and prove an analogous statement for the *trace* (cf. Exercise VII.1.13).

- p.497, Exercise 1.7:

1.7. ▷ Define a topology on $\operatorname{Spec} R$ by declaring the closed sets to be the sets $V(I)$, where $I \subseteq R$ is an ideal and $V(I)$ denotes the set of prime ideals *containing* I.

- p.497, Exercise 1.9:

Prove that the assignment $X \mapsto h_X := \operatorname{Hom}_{\mathsf{C}}(\_, X)$ (cf. §1.2) defines a covariant functor $\mathsf{C} \to \mathsf{Set}^{\mathsf{C}^{op}}$. (Define the action on morphisms in the natural way.) [1.11, IX.1.11]

- p.497, Exercise 1.11:

1.11. (Cf. Exercise 1.9.) Let C be a small category. A contravariant functor $\mathsf{C} \to \mathsf{Set}$ is *representable* if it is naturally isomorphic to a functor h_X (cf. §1.2). In this case, X 'represents' the functor. Prove that C is equivalent to the subcategory of representable functors in $\mathsf{Set}^{\mathsf{C}^{op}}$. (Hint: Yoneda; see Exercise 1.10.)

- p.498, Exercise 1.12:

1.12. Let C, D be categories, and let $\mathscr{F} : \mathsf{C} \to \mathsf{D}$, $\mathscr{G} : \mathsf{D} \to \mathsf{C}$ be functors. Prove that $\mathscr{F}$ is left-adjoint to $\mathscr{G}$ if and only if, for every object Y in D, the object $\mathscr{G}(Y)$ represents the functor $h_Y \circ \mathscr{F}$ ('naturally' in Y).

- p.505, Corollary 2.6:

$$(M_1 \oplus M_2) \otimes_R N \cong (M_1 \otimes_R N) \oplus (M_2 \otimes_R N).$$

- p.509, bottom half:

so we can define

$$\operatorname{Tor}_i^R(M, N) := H_i(M_\bullet \otimes_R N).$$

For example, according to this definition $\operatorname{Tor}_0^R(M, N) \cong M \otimes_R N$ (Exercise 2.14),

- p.521, Exercise 3.9:

3.9. Let $f : R \to S$ be a ring homomorphism, and let M be an R-module. Prove that the extension $f^*(M)$ satisfies the following universal property: if N is an S-module and $\varphi : M \to N$ is an R-linear map, then there exists a unique S-linear map $\tilde{\varphi} : f^*(M) \to N$ making the diagram

---

- p.522, Exercise 3.15:

3.15. Let $f : R \to S$ be a ring homomorphism, and assume that the functor $f_* : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$ is an equivalence of categories.

- Prove that there is a homomorphism of rings $\overline{g} : S \to \mathrm{End}_{\mathsf{Ab}}(R)$ such that the composition $R \to S \to \mathrm{End}_{\mathsf{Ab}}(R)$ is the homomorphism realizing R as a module over itself (that is, the homomorphism studied in Proposition III.2.7).
- Use the facts that S is commutative and f_* is fully faithful to deduce that $\overline{g}(S)$ is isomorphic to R. Deduce that f has a left-inverse $g : S \to R$.
- Therefore, $f_* \circ g_*$ is naturally isomorphic to the identity; and it follows that $g_* \circ f_*(S) \cong S$ as an S-module. Prove that this implies that g is injective. (If $a \in \ker g$, prove that a is in the annihilator of $g_* \circ f_*(S)$.)
- Conclude that f is an isomorphism.

Two rings are *Morita equivalent* if their categories of left-modules are equivalent. The result of this exercise is a (very) particular case of the fact that two *commutative* rings are Morita equivalent if and only if they are isomorphic. In fact, this more general statement is perhaps easier (!) to prove than the particular case worked out in this exercise. The reader can verify that if R is a commutative ring, then it is isomorphic to the endomorphism ring of the *identity functor* on R-Mod. It follows that if R-Mod is equivalent to S-Mod, then R and S must be isomorphic. The commutativity is crucial in this statement: for example, it can be shown that any ring R is Morita equivalent to the ring of matrices[17] $\mathcal{M}_{n,n}(R)$, for all $n > 0$.

- p.525, bottom:

uniquely through an R-linear map

$$\overline{\varphi_I} : \bigwedge^{\ell}_R(M) \to R,$$

- p.526, top half:

Now assume that

$$\sum_{1\le j_1<\cdots<j_\ell\le r} \lambda_{j_1\ldots j_\ell}\, e_{j_1}\wedge\cdots\wedge e_{j_\ell} = 0;$$

then with $I = (i_1,\ldots,i_\ell)$

$$\lambda_{i_1\ldots i_\ell} = \overline{\varphi_I}\left(\sum_{1\le j_1<\cdots<j_\ell\le r} \lambda_{j_1\ldots j_\ell}\, e_{j_1}\wedge\cdots\wedge e_{j_\ell} = 0\right) = \overline{\varphi_I}(0) = 0.$$

- p.527, top half:

Similarly to the alternating case, if $e_1,\ldots,e_r$ generate M, then the *symmetric* power $\mathbb{S}^\ell_R(M)$ is generated by the (images[20] of) all tensors

$$e_{i_1}\otimes\cdots\otimes e_{i_\ell}$$

with $1\le i_1\le\cdots\le i_\ell\le r$. In this case all $\mathbb{S}^\ell_R(M)$ are, in general, nonzero.

- p.529, (iv)=>(ii):

(iv) $\Longrightarrow$ (ii): Let $\varphi : S\to T$ be a graded homomorphism, and assume $I = \ker\varphi$. Let $s = \sum_i s_i \in \ker\varphi$, with $s_i\in S_i$. Then $\sum_i \varphi(s_i) = 0$ in T, and $\varphi(s_i)$ is homogeneous of degree i for all i. It follows that $\varphi(s_i) = 0$ for all i, that is, each $s_i\in\ker\varphi = I$, implying (ii). □

- p.529, middle:

The conventional grading of a polynomial ring is not the only option: we could decide to grade $k[x,y]$ by placing constants in degree 0 and assigning degree 1 to the indeterminate x and degree 2 to y. With such a grading, the ideal $(y-x^2)$ *is* homogeneous. ⌟

- p.532, Exercise 4.3:

4.3. Let I be the ideal (x, y) in $k[x, y]$; so every element of I may be written (of course, not uniquely) in the form $fx+gy$ for some polynomials $f, g \in k[x, y]$. Define a function $\varphi : I \times I \to k$ by prescribing

$$\varphi(f_1x + g_1y, f_2x + g_2y) := f_1(0,0)g_2(0,0) - f_2(0,0)g_1(0,0).$$

- Prove that φ is well-defined.
- Prove that φ is $k[x, y]$-bilinear and alternating.
- Prove that $\bigwedge^2_{k[x,y]}(I) \neq 0$.

Note that I has rank 1 as a $k[x, y]$-module; if it were free, its second exterior power would have to vanish by Lemma 4.3.

- p.533, Exercise 4.12:

4.12. (Cf. Exercise 4.11.) Prove the 'weak homogeneous Nullstellensatz': if k is algebraically closed and $I \subseteq k[x_0, \ldots, x_n]$ is a homogeneous ideal, then $\mathscr{V}(I) = \emptyset$ if and only if $\sqrt{I}$ is either $k[x_0, \ldots, x_n]$ or the irrelevant ideal $(x_0, \ldots, x_n)$. (Translate this into a question about $\mathbb{A}^{n+1}_k$.)

- p.535, Exercise 4.22:

$$d_r(e_{i_1} \wedge \cdots \wedge e_{i_r}) = \sum_{j=1}^{r} (-1)^{j-1} a_{i_j} e_{i_1} \wedge \cdots \wedge \hat{e_{i_j}} \wedge \cdots \wedge e_{i_r},$$

- p.538, Proof of Proposition 5.5:

$$\mathrm{Hom}_R(M, F) \cong \mathrm{Hom}_R(M, R^n) \cong \mathrm{Hom}_R(M, R)^n \cong \mathrm{Hom}_R(M, R) \otimes_R R^n \cong M^\vee \otimes_R F,$$

- p.540, bottom:

As P is free, $P \cong F^R(S) \cong R^{\oplus S}$ for some set S. Choosing (arbitrarily!) preimages in N of the standard basis vectors $\mathbf{e}_s \in R^{\oplus S}$ gives a set-function $S \to N$, extending to an R-linear map $\rho : P \to N$ by the universal property of free modules:

$$0 \longrightarrow M \xrightarrow{\mu} N \underset{\rho}{\overset{\nu}{\rightleftarrows}} P \longrightarrow 0\,.$$

- p.542, top:

remember that *dualizing kills torsion* (over integral domains). Practice this by working out Exercise 5.11.

- p.542, middle:

  By Proposition 5.16, $M^{\vee\vee}$ is torsion-free over integral domains. In fact, the double-dual construction is a standard way to 'clean up' a module, removing its torsion.

- p.543, Exercise 5.3:

  To show $\ker\beta \subseteq \operatorname{im}\alpha$, choose $N = B/\operatorname{im}(\alpha)$.) Remember that the converse does not hold, since in general $\operatorname{Hom}_R(\_, N)$ is not exact. What extra hypothesis on α would guarantee the exactness of (*) for all N?

- p.544, Exercise 5.12:

  $\omega : M \to M^{\vee\vee}$ defined in §5.5. [§5.5]

- p.544, Exercise 5.13:

  (canonical) isomorphism ω defined in §5.5. [§5.5]

- p.546, Lemma 6.2:

  An R-module Q is injective *if and only if for all monomorphisms of R-modules*

- p.547, middle:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \frac{\mathbb{Z}}{(2)} \longrightarrow 0$$

- p.549, bottom:

  Consider the set E of pairs $(\widetilde{L}, \tilde{q})$, where $\widetilde{L}$ ranges over the submodules of M containing L and $\tilde{q} : \widetilde{L} \to Q$ extends q: $\tilde{q}|_L = q$. Then E is nonempty, since $(L, q) \in E$, and we can define a partial order on E by prescribing that $(\widetilde{L}', \tilde{q}') \preceq (\widetilde{L}'', \tilde{q}'')$ if $\widetilde{L}' \subseteq \widetilde{L}''$ and $\tilde{q}''$ extends $\tilde{q}'$. It is clear that every chain has an upper bound (take the union of the corresponding $\widetilde{L}$), so by Zorn's lemma there exists a maximal extension $(\widetilde{L}, \tilde{q})$, and we are done if we can prove that $\widetilde{L} = M$.

- p.550, Proof of Lemma 6.9:

Proof. By adjunction (Lemma 3.5),

$$\mathrm{Hom}_R(\_, f^!(Q)) \cong \mathrm{Hom}_S(f_*(\_), Q)$$

as functors R-Mod $\to$ Ab. Since f_* is exact (Proposition 3.6) and $\mathrm{Hom}_S(\_, Q)$ is exact by hypothesis, $\mathrm{Hom}_R(\_, f^!(Q))$ must be exact. This is precisely the statement. □

- p.554, beginning of Section 6.5:

6.5. $\mathbf{Ext}^*_{\mathbb{Z}}(G, \mathbb{Z})$. We will attempt to convince the reader that computing Ext modules is not too unreasonable, by discussing the computation of $\mathrm{Ext}^*_{\mathbb{Z}}(G, \mathbb{Z})$ for an arbitrary finitely generated abelian group G.

- p.555, first display:

of M by N, that is, of exact sequences

$$0 \longrightarrow N \longrightarrow E \longrightarrow M \longrightarrow 0$$

modulo a suitable isomorphism relation (cf. §IV.5.2). For example, the direct sum

---

- p.555, Exercise 6.5:

6.5. Prove that the dual of a finitely generated projective module is projective. Prove that finitely generated projective modules are reflexive (that is, isomorphic to their biduals).

- p.557, Exercise 6.22, last bullet:

  - Prove that $e(\epsilon(\mathscr{E}))$ is isomorphic to $\mathscr{E}$ and that $\epsilon(e(\kappa)) = \kappa$.

-

Chapter IX

- p.563, bottom:

First assume $\varphi : A \to B$ is a monomorphism with a kernel $\iota : K \to A$. In particular, $\varphi \circ \iota : K \to A \to B$ is the zero-morphism; therefore $\iota = 0$ by Lemma 1.3. What about K? If $\zeta : Z \to A$ is any morphism such that the composition $Z \to$

- p.563, Lemma 1.5:

Lemma 1.5. *Let $\varphi : A \to B$ be a morphism in an additive category. If φ has a kernel, then φ is a monomorphism if and only if $0 \to A$ is its kernel. If φ has a cokernel, then φ is an epimorphism if and only if $B \to 0$ is its cokernel.*

- **p.567, bottom:**

diagram is supposed to indicate). The fibered product may be constructed in this context, just as in the particular case of R-Mod, as the kernel of the difference of the two morphisms

$$A \times B \underset{\varphi \circ \rho_A}{\overset{\psi \circ \rho_B}{\rightrightarrows}} C$$

where ρ_A, ρ_B are the morphisms making $A \times B$ a product. The reader will prove that these 'fiber squares' preserve kernels, in the sense that $\ker \varphi = \psi' \circ \ker \varphi'$ (Exercise 1.16).

- p.568, bottom:

Proposition 1.12. *In an abelian category, finite products and coproducts coincide.*

As it happens, this fact is already true in *additive* categories, and the argument for this more general claim is (even) more straightforward than what follows. Here we will quickly review the ingredients going into a proof that the morphism (π_A, π_B) is a *monomorphism*. Similar arguments, proving that the same morphism is an epimorphism, will be left to the reader.

In the process, we recover for these objects all the properties we expect on the basis of our experience with R-Mod. Doing it 'with arrows' requires a bit of practice but is not particularly difficult.

- $\pi_B : A \amalg B \to B$ is the cokernel of $i_A : A \to A \amalg B$:

- p.569, middle:

Indeed, i_A is a monomorphism since $A \xrightarrow{i_A} A \amalg B \xrightarrow{\pi_A} A$ is the identity; hence it is a kernel (definition of abelian category!); hence it is the kernel of its cokernel (Lemma 1.8).

- p.574, Exercise 1.8:

$$0 \longrightarrow \mathrm{Hom}_A(Z, K) \longrightarrow \mathrm{Hom}_A(Z, A) \longrightarrow \mathrm{Hom}_A(Z, B)$$

- p.575, top:

- Let $\varphi : A \to B$ be a morphism in A. If φ has a cokernel, prove that φ is an epimorphism if and only if $B \to 0$ is its cokernel. (Cf. Lemma 1.5.)

- p.575, Exercise 1.14:

1.14. Let T be a topological space. Recall that a *presheaf* on T with values in a category A is a contravariant functor from a certain category associated with T to A (Example VIII.1.5). Define the *category* of A-valued presheaves on T. Prove that presheaves on T with values in an abelian category form an abelian category. (Hint: Exercise 1.11.)

- p.580, top row of the diagram:

$$0 \longrightarrow L_1 \xrightarrow{\sigma} M_1 \times_{N_1} (\ker \nu) \xrightarrow{\beta_1'} \ker \nu \longrightarrow 0$$

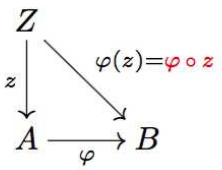
- p.580, bottom half:

Since $\operatorname{coker} \lambda$ plays the role of kernel in the bottom row and $\tau \circ \epsilon' : \ker \nu \to N_0$ is the zero-morphism (because $\tau \circ \epsilon' \circ \beta_1' = \tau \circ \epsilon = 0$ and β_1' is an epimorphism), ϵ' must factor through $\operatorname{coker} \lambda$, finally yielding

---

- p.582, top:

of B: simply compose morphisms, i.e.,



- p.584, bottom:

Now we will proceed to verify all the miracles we have advertised. In the following, the symbol $\sim$ will stand for the equivalence relation defined above[8]; thus, two morphisms $z_1 : Z_1 \to A$, $z_2 : Z_2 \to A$ determine the same 'element' of $\hat{A}$ if and only if $z_1 \sim z_2$.

- p.591, Exercise 2.17:

2.17. Upgrade the Yoneda lemma (Exercise VIII.1.10) to prove that every small abelian category A is equivalent to a full subcategory of the category F of Exercise 2.15, by means of the functor assigning to each object X in A the functor $h_X = \mathrm{Hom}_{\mathsf{A}}(\_, X)$.

Prove that this Yoneda embedding is *left*-exact and 'reflects exactness' in the

---

- p.596, proof of Lemma 3.4:

$$\mathrm{Hom}_{\mathsf{C}(\mathsf{A})}(M^\bullet, N^\bullet) \to \mathrm{Hom}_{\mathsf{A}}(H^i(M^\bullet), H^i(N^\bullet))$$

- p.596, first line following the proof of Lemma 3.4:

We can also view cohomology as a functor $\mathsf{C}(\mathsf{A}) \to \mathsf{C}(\mathsf{A})$, by placing each

---

- p.602, Exercise 3.1:

$$\cdots \xrightarrow{d^{-3}} M^{-2} \xrightarrow{d^{-2}} M^{-1} \longrightarrow \ker d^0 \longrightarrow A \longrightarrow 0 \longrightarrow \cdots,$$

$$\cdots \longrightarrow 0 \longrightarrow A \longrightarrow \mathrm{coker}\, d^{-1} \longrightarrow M^1 \xrightarrow{d^1} M^2 \xrightarrow{d^2} \cdots$$

- p.614, top:

Theorem 4.14. *Let $\mathscr{F} : \mathsf{A} \to \mathsf{B}$ be an additive functor between two abelian categories. If $L^\bullet$, $M^\bullet$ are homotopy equivalent complexes in $\mathsf{C}(\mathsf{A})$, then the cohomology complexes*

$$H^\bullet(\mathsf{C}(\mathscr{F})(L^\bullet)), \quad H^\bullet(\mathsf{C}(\mathscr{F})(M^\bullet))$$

are isomorphic.

- p.614, Exercise 4.5:

4.5. ▷ Let $\alpha_k^\bullet, \beta_k^\bullet : L_k^\bullet \to M_k^\bullet$, $k = 0, 1$, be morphisms of cochain complexes. Assume that $\alpha_0 \sim \beta_0$, $\alpha_1 \sim \beta_1$. Prove that $\alpha_0 \oplus \alpha_1 \sim \beta_0 \oplus \beta_1$ as morphisms $L_0^\bullet \oplus L_1^\bullet \to M_0^\bullet \oplus M_1^\bullet$. [§4.3]

- p.629, middle:

It is however clear that such resolutions exist *if* the category has enough projectives/injectives: if A has enough projectives, then given any object A of A there is a projective P^0 with an epimorphism $\pi : P^0 \to A$; and then a projective P^{-1} with an epimorphism $d^{-1} : P^{-1} \to \ker \pi$; and then a projective P^{-2} with an

---

- p.639, Exercise 6.4:

  Prove that $\mathscr{P} \circ \mathscr{I}$ is naturally *isomorphic* to the identity functor and that there is a natural *transformation* (not an isomorphism in general) $\mathscr{I} \circ \mathscr{P} \rightsquigarrow \mathrm{id}_{\mathsf{K}^-(\mathsf{A})}$ such that the composition $\mathscr{P} \circ (\mathscr{I} \circ \mathscr{P}) \rightsquigarrow \mathscr{P}$ is an isomorphism. [§7.1, §7.2]

- p.641, Exercise 6.13:

  6.13. ▷ (Cf. Exercise 6.2.) Let A be an abelian category with enough projectives, and let $\hat{\mathsf{A}}$ be the subcategory of $\mathsf{K}^-(\mathsf{P})$ whose objects have cohomology concentrated in degree 0. Choosing (arbitrarily) a projective resolution for every object A of A and lifting morphisms as in Proposition 6.5, we obtain a functor $\mathsf{A} \to \hat{\mathsf{A}}$; with notation as in §6.3, this is $\mathscr{P} \circ \iota$. It is clear that $H^0 \circ \mathscr{P} \circ \iota$ is the identity functor on A. Prove that there is a natural isomorphism from the identity functor on $\hat{\mathsf{A}}$ to $\mathscr{P} \circ \iota \circ H^0$. [§7.1]

- p.643, middle:

  This may be viewed as a nuisance. On the contrary, it is one of the main values of deriving categories and functors. Recasting an additive functor $\mathscr{F} : \mathsf{A} \to \mathsf{B}$ at

---

- p.644, Proposition 7.3, statement:

  Proposition 7.3. *The left-derived functor* $\mathsf{L}\mathscr{F}$ *satisfies the following universal property: There is a natural transformation* η: $\mathsf{L}\mathscr{F} \circ \mathscr{P}_{\mathsf{A}} \rightsquigarrow \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})$ *such that for every functor* $\mathscr{G} : \mathsf{K}^-(\mathsf{P}(\mathsf{A})) \to \mathsf{K}^-(\mathsf{P}(\mathsf{B}))$ *and every natural transformation* $\gamma : \mathscr{G} \circ \mathscr{P}_{\mathsf{A}} \rightsquigarrow \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})$, *there is a unique (up to natural isomorphism) natural transformation* $\mathscr{G} \rightsquigarrow \mathsf{L}\mathscr{F}$ *inducing a factorization of* γ *as follows:* $\mathscr{G} \circ \mathscr{P}_{\mathsf{A}} \rightsquigarrow \mathsf{L}\mathscr{F} \circ \mathscr{P}_{\mathsf{A}} \overset{\eta}{\rightsquigarrow} \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})$.

- p.644, Proposition 7.3, proof:

Proof. If we have done our homework (and in particular Exercise 6.4), then we have defined a certain natural transformation $\mathscr{I}_{\mathsf{A}} \circ \mathscr{P}_{\mathsf{A}} \rightsquigarrow \mathrm{id}_{K^-(\mathsf{A})}$; composing on the left by $\mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})$ defines a tranformation η as stated, since $\mathsf{L}\mathscr{F} = \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F}) \circ \mathscr{I}_{\mathsf{A}}$ by definition. Concretely, for every $L^\bullet$, $\eta_{L^\bullet} : \mathsf{L}\mathscr{F} \circ \mathscr{P}_{\mathsf{A}}(L^\bullet) = \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})(\mathscr{P}_{\mathsf{A}}(L^\bullet)) \to \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})(L^\bullet)$ is the morphism induced by the morphism $\mathscr{P}_{\mathsf{A}}(L^\bullet) \to L^\bullet$ associated with the chosen projective resolution.

Every natural transformation $\mathscr{G} \rightsquigarrow \mathsf{L}\mathscr{F}$ will induce a natural transformation γ as in the statement. We have to verify that every $\gamma : \mathscr{G} \circ \mathscr{P}_{\mathsf{A}} \rightsquigarrow \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F})$ is induced in this fashion, by one and only one (up to natural isomorphism) natural transformation $\mathscr{G} \rightsquigarrow \mathsf{L}\mathscr{F}$. The uniqueness follows because we can reconstruct the transformation $\mathscr{G} \rightsquigarrow \mathsf{L}\mathscr{F}$ from γ, by horizontally composing on the right by $\mathrm{id}_{\mathscr{I}_{\mathsf{A}}}$ (and again using Exercise 6.4, to obtain an isomorphism $\mathrm{id}_{K^-(\mathsf{P}(\mathsf{A}))} \cong \mathscr{P}_{\mathsf{A}} \circ \mathscr{I}_{\mathsf{A}}$):

$$\mathscr{G} \xrightarrow{\sim} \mathscr{G} \circ \mathscr{P}_{\mathsf{A}} \circ \mathscr{I}_{\mathsf{A}} \xrightarrow{\gamma \cdot \mathrm{id}_{\mathscr{I}_{\mathsf{A}}}} \mathscr{P}_{\mathsf{B}} \circ \mathsf{K}(\mathscr{F}) \circ \mathscr{I}_{\mathsf{A}} = \mathsf{L}\mathscr{F}.$$

Concretely, for all $P^\bullet$ in $K^-(\mathsf{P}(A))$, the resolution morphism $\mu_{P^\bullet} : \mathscr{P}_A(P^\bullet) \to P^\bullet$ is an isomorphism in $K^-(\mathsf{P}(A))$; then (writing $P^\bullet$ for $\mathscr{I}_A(P^\bullet)$ for notation's sake)

$$\mathscr{G}(P^\bullet) \xrightarrow{\mathscr{G}(\mu_{P^\bullet}^{-1})} \mathscr{G} \circ \mathscr{P}_A(P^\bullet) \xrightarrow{\gamma_{P^\bullet}} \mathscr{P}_B \circ K(\mathscr{F})(P^\bullet) = \mathsf{L}\mathscr{F}(P^\bullet).$$

It is straightforward to verify that this natural transformation induces γ. □

- p.645, Remark 7.4:

Remark 7.4. The fact that there is a natural transformation $\mathscr{I} \circ \mathscr{P} \rightsquigarrow \mathrm{id}$ (Exercise 6.4), used in the proof of Proposition 7.3, has another interesting consequence. Let A, B, C be abelian categories, and let $\mathscr{F} : \mathsf{A} \to \mathsf{B}$, $\mathscr{G} : \mathsf{B} \to \mathsf{C}$ be additive functors. Assume that B and C have enough projectives, so that the derived functors

---

- p.645, middle:

7.3. Taking cohomology. The content of Proposition 7.3 is again in line with our main strategy: in moving from A to $\mathsf{D}^-(\mathsf{A})$, the left-derived functor $\mathsf{L}\mathscr{F}$ is the functor that preserves 'as much cohomological information as possible' regarding bounded-above complexes, in the sense that it is the closest one can get to extending $\mathscr{F} : \mathsf{A} \to \mathsf{B}$ to a functor $\mathsf{D}^-(\mathsf{A}) \to \mathsf{D}^-(\mathsf{B})$.

- p.651, bottom:

Now the long exact sequence of left-derived functors is an immediate consequence of the long exact cohomology sequence.

- p.655, middle:

is an abelian group carrying a *trivial* action of G; it is clear that the assignment $M \mapsto M^G$ defines a covariant functor $\cdot^G : G\text{-}\mathsf{Mod} \to \mathsf{Ab}$. Both G-Mod and Ab are abelian categories, and it takes a moment to realize that $\cdot^G$ is a left-exact

---

- p.661, hint to Exercise 7.15:

  (Hint: To efface $\mathsf{R}^i\mathscr{F}$ for $i > 0$, use injectives. To efface H^i for $i > 0$, stare at the sequence of complexes mentioned right before the statement of Proposition 4.1.)

- p.662, Example 8.2:

  Example 8.2. Let R be a commutative ring. Recall (Definition VIII.2.13) that an R-module M is *flat* if $\_ \otimes_R M$ is exact, or equivalently (by the symmetry of $\otimes$) if $M \otimes_R \_$ is exact. Flat modules are acyclic with respect to tensor products, in a very

---

- p.663, statement of Theorem 8.3:

  be a resolution of an object M of A, such that every object A^i is $\mathscr{F}$-acyclic. Then

---

- p.663, bottom:

  and taking cohomology:

  $$\mathsf{L}_{i-1}\mathscr{F}(K) \cong H^{-i}(\mathsf{C}(\mathscr{F})(A^\bullet)).$$

- p.668, Example 8.8:

  'first quadrant' example, let $L^\bullet$, resp., $M^\bullet$, be a complex in $\mathsf{C}^{\leq 0}(\mathsf{A})$, resp., $\mathsf{C}^{\geq 0}(\mathsf{A})$:

- p.674, Theorem 8.12, first bullet:

  - *Assume that (*) is a resolution of $N^\bullet$ in $\mathsf{C}^{\leq 0}(\mathsf{A}')$. Then $T^\bullet$ is quasi-isomorphic*

- p.687, middle:

  where $[e]$ denotes the class of $e \in \ker d$ in E'. (Since $\beta \circ \gamma(e) = d(e) = 0$, $\gamma(e) \in \ker \beta = \operatorname{im} \alpha = A'$.) All needed verifications (such as the independence on the representative e of $[e]$ in the third prescription) are straightforward, from the exactness of the given triangle.

- p.695, Exercise 9.2:

9.2. ▷ Let A be an abelian category, and suppose two complexes $L^\bullet$, $M^\bullet$ are connected by an 'upside-down roof' (a 'trough'?)