Errata for `Algebra: Chapter 0'

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 at p.49, Exercise 1.8.)

This list is bound to grow forever. (149 items, and counting.) The contribution of many readers is hereby gratefully acknowledged.

Last updated: 11/06/11.

- **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, 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:

    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.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* $f_1 = f_2\sigma$.

- **Chapter II**

- **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:

The reader should check carefully that $\mathbb{Z}/n\mathbb{Z}$ consists of exactly n elements, namely

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

- **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,

- 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.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.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.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.72, top:

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

---

- 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:

- $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) \,|\, \det(M) = 1\}$;

- 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.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.

- 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.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.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, bottom:

    (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.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.131, middle:

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

- 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.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 4.10:

  - 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.160, bottom:

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

- 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 $\mathrm{Hom}_{R\text{-Mod}}(R, M) \cong M$ as R-modules.

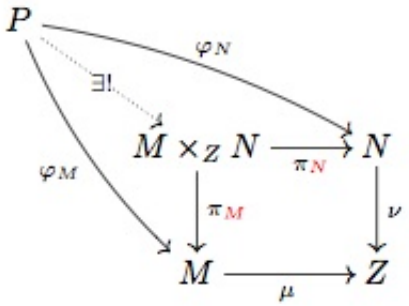
- p.163, Exercise 5.6:

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 element of G has necessarily infinite order. Alternative hint: The unique ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism.)

- 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, top half:



- 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:

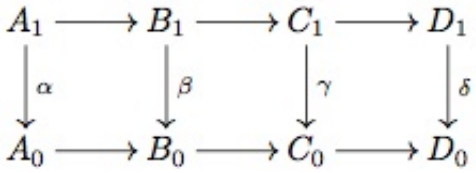
7.11. ▷ Let

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

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:**

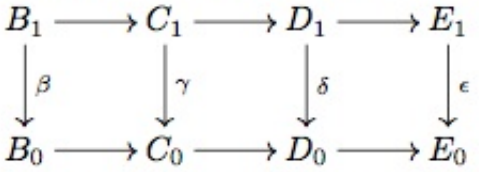
7.12. ¬ Practice your diagram chasing skills by proving the 'four-lemma': if



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



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:

$$(a_1, \dots, a_p)$$

such that $a_1 \cdots a_p = e$. We claim that $|S| = |G|^{p-1}$: indeed, once $a_1, \dots, a_{p-1}$ 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 $0 \le m < p$, act by $[m]$ on

$$(a_1, \dots, a_p)$$

by sending it to

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

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

(*) $$(a, \dots, a);$$

and note that $Z \neq \emptyset$, since $\{e, \dots, e\} \in Z$. Since $p \ge 2$ 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.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 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). [§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 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, 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.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.212, bottom:

It is worth mentioning that *any* 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.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.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.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.237, Theorem 6.6:

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

- p.239, middle:

classification of finite abelian groups into account. Indeed, by Theorem 6.6

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

for some positive integers $1 < d_1 \mid \cdots \mid d_s$. But if $s > 1$, then $|G| > d_s$ and $d_s g = 0$

- 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.*

- **Chapter V**
  - 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.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.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:

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

- p.258, top half:

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

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

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.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.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.274, proof of Lemma 4.15:

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

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

- **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.281, top:

root of f with *multiplicity* r if $(x-a)^r$ divides f and $(x-a)^{r+1}$ does *not* divide f.

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

5.1. ¬ Let $f(x) \in \mathbb{C}[x]$ prove that a 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 6.3:

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.301, third bullet:

  - 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 6.12:

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]

- **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.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.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 $(q_1), \ldots, (q_n) \subseteq R$, 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.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.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

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

- **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.397, Exercise 1.8:**

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

- 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.411, top:

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

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

- 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.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.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.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:

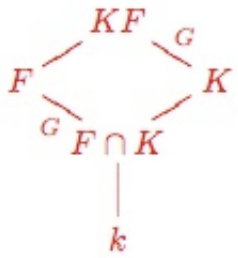
(1) $\Longleftrightarrow$ (2) by Theorem 4.8; (2) $\Longrightarrow$ (3) by Corollary 5.20. (3) $\Longleftrightarrow$ (4) follows from Proposition 6.5, applied to the extension $F^{\mathrm{Aut}_k(F)} \subseteq F$: by Proposition 6.5, we have

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

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) $\Longrightarrow$ (2) by Lemma 6.6.

- p.464, middle:

Pictorially,



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

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

- p.472, top:

$$\begin{aligned} s_1(t_1, t_2, t_3) &= t_1 + t_2 + t_3, \\ s_2(t_1, t_2, t_3) &= t_1t_2 + t_1t_3 + t_2t_3, \\ s_3(t_1, t_2, t_3) &= t_1t_2t_3. \end{aligned}$$

- p.476, bottom:

Proof. Assume $\mathrm{Aut}_k(F)$ is solvable. Let M be a common multiple of the order of the cyclic quotients, and let ζ be a primitive M-th root of 1 in an algebraic closure $\bar{k}$ 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 $\mathrm{Aut}_{k(\zeta)\cap F}(F)$. It follows that $\mathrm{Aut}_{k(\zeta)}(F(\zeta))$ is solvable, since $\mathrm{Aut}_{k(\zeta)\cap F}(F)$ is a subgroup of $\mathrm{Aut}_k F$ and the latter is solvable by assumption. (See the comment following Corollary IV.3.13.)

- 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.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.522, Exercise 3.15:

3.15. Let $f : R \to S$ be a ring homomorphism, and assume that the functor $f_* : S\text{-Mod} \to R\text{-Mod}$ 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; in particular, $f_* \circ g_*(S) \cong S$ as an R-module. Prove that this implies that g is injective. (If $a \in \ker g$, prove that a is in the annihilator of $f_* \circ g_*(S)$.)
- 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

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

- p.526, top half:

Now assume that

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

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

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

- 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.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.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.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?

- **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.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.580, top row of the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_1 & \xrightarrow{\sigma} & M_1 \times_{N_1} (\ker \nu) & \xrightarrow{\beta_1'} & \ker \nu & \longrightarrow & 0 \\ & & \| & & \swarrow \; \downarrow & & \downarrow & & \end{array}$$

- 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.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 $h_X = \operatorname{Hom}_{\mathsf{A}}(\_, X)$.

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

---

- p.602, Exercise 3.1:

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

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

- p.614, top:

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:

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.651, bottom:

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