Algebra I exercises

David Pierce

January 2, 2014
Matematik Bölümü
Mimar Sinan Güzel Sanatlar Üniversitesi
http://mat.msgsu.edu.tr/

Many exercises here are adaptations of exercises from Hungerford [3]. In that case, a reference is given.

The notation $\mathbb{N} = \{1, 2, 3, \dots\}$ and $\omega = \{0, 1, 2, \dots\}$ is used. If A and B are sets, then the set of functions from A to B is denoted by B^A.

Unless otherwise noted, the signature of groups is $\{\mathrm{e}, {}^{-1}, \cdot\}$. Thus, if $\mathfrak{G}$ is a group, this means $\mathfrak{G}$ is the structure $(G, \mathrm{e}^{\mathfrak{G}}, {}^{-1^{\mathfrak{G}}}, \cdot^{\mathfrak{G}})$. Usually we can abbreviate this as $(G, \mathrm{e}, {}^{-1}, \cdot)$. This group is an expansion of the monoid $(G, \mathrm{e}, \cdot)$ and the semigroup $(G, \cdot)$.

Exercise 1 (I.1.2)**.** If A is a set and $\mathfrak{G}$ is a group, show that the set G^A expands to a group in which $\cdot$ is given by

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Exercise 2 (I.1.3)**.** (a) Find a set A and a subset B of A^A such that

[i] B is closed under functional composition,

[ii] B contains a right identity with respect to composition,

[iii] every element of B has a left inverse with respect to this right identity, but

[iv] the semigroup $(B, \circ)$ does not expand to a group.

(b) Same problem, with "left" and "right" interchanged.

Exercise 3 (I.1.7)**.** The **Euclidean Algorithm** is a way to find the greatest common divisor $\gcd(a, b)$ of two integers a and b, not both 0; it is established in the first two propositions of Book VII of Euclid's *Elements* [1]. By means of the algorithm, we can find integral solutions to the equation

$$ax + by = \gcd(a, b).$$

Given a positive integer n, we let $\mathbb{Z}/n\mathbb{Z}$ denote the set of congruence-classes of integers *modulo* n. In the first section of his *Disquisitiones Arithmeticae* (published when he was 23), Gauss [2] shows in effect that

- the map taking an integer to its congruence-class is a bijection from $\{0, \ldots, n-1\}$ to $\mathbb{Z}/n\mathbb{Z}$, and
- the usual ring-structure on $\mathbb{Z}$ induces a ring-structure on $\mathbb{Z}/n\mathbb{Z}$.

Let us take all of the foregoing as proved.

(a) Prove **Euclid's Lemma** (which is Proposition VII.30 of the *Elements*): If p is prime, and $p \mid ab$, show that p divides a or b.
(b) Show that n is prime if and only if the set $\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}$ is closed under multiplication. (Of course 0 here means literally the set of multiples of n.)
(c) If p is prime, show that the semigroup $(\mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}, \cdot)$ expands to a group.

Exercise 4 (I.1.14)**.** Let p be a prime number, and let $\mathbb{Z}/p\mathbb{Z} \smallsetminus \{0\}$ be denoted by ${\mathbb{Z}_p}^{\times}$. We may identify this set with $\{1, \ldots, p-1\}$.

(a) Prove that 1 and $p-1$ are the only solutions of $x^2 = 1$ in ${\mathbb{Z}_p}^{\times}$.
(b) Prove $(p-2)! = 1$ in ${\mathbb{Z}_p}^{\times}$.
(c) Obtain **Wilson's Theorem,** namely $(p-1)! \equiv -1 \pmod{p}$.
(d) Let $\mathfrak{G}$ be a finite group. **Cauchy's Theorem** is that, if $|G|$ is a multiple of p, then G contains a nontrivial solution (that is, a solution other than e) of $x^p = \mathrm{e}$. Prove this in case $p = 2$. (Use the idea of the proof of Wilson's Theorem. In fact our proof of Cauchy's Theorem is going to use a generalization of this idea.)

Exercise 5 (I.1.9)**.** Let p be a prime.

(a) Show that $\{x/y \colon p \nmid y\}$ is the universe of a subgroup of $(\mathbb{Q}, +)$.

(b) Show that $\{x/p^n : n \in \omega\}$ is the universe of a subgroup of $(\mathbb{Q}, +)$.

Exercise 6 (I.1.11). (a) Show that each of the following conditions defines the same class of groups:

[i] $xy = yx$ (that is, the group is abelian).
[ii] $(xy)^2 = x^2y^2$.
[iii] $(xy)^{-1} = x^{-1}y^{-1}$.
[iv] $(xy)^n = x^ny^n$ for all n in $\mathbb{Z}$.
[v] $\bigwedge_{i\in 3}(xy)^{n+i} = x^{n+i}y^{n+i}$ for some n in $\mathbb{Z}$.

(b) Show that possibly $(xy)^n = x^ny^n$ and $(xy)^{n+1} = x^{n+1}y^{n+1}$, although $xy = yx$ may fail.

Exercise 7 (I.1.13). Every group satisfying the identity $x^2 = \mathrm{e}$ is abelian.

Exercise 8 (I.1.15). Prove:

(a) Every *finite* semigroup with left and right cancellation ($xy = xz \Rightarrow y = z$ and $yx = zx \Rightarrow y = z$) expands to a group.
(b) There is an infinite semigroup with left and right cancellation that does not expand to a group.

Exercise 9. (a) Show that semigroup may have a left identity that is not a right identity.
(b) If a semigroup has a left identity and a right identity, show that they are equal.
(c) In a monoid, show that there is exactly one left identity, and this is a right identity.
(d) Find monoids $\mathfrak{M}$ and $\mathfrak{N}$ such that

$$(M, \cdot) \subseteq (N, \cdot), \qquad \text{but} \qquad (M, \mathrm{e}, \cdot) \nsubseteq (N, \mathrm{e}, \cdot).$$

(e) Find a chain $\mathfrak{M}_0 \subseteq \mathfrak{M}_1 \subseteq \mathfrak{M}_2 \subseteq \cdots$ of semigroups that expand to monoids, although the union $\bigcup_{k\in\omega} \mathfrak{M}_k$ does not.

Remark. This problem yields the following model-theoretic conclusions. A monoid is a structure $(M, \mathrm{e}, \cdot)$ such that

- $(M, \cdot)$ is a semigroup satisfying the axiom

$$\exists x\, \forall y\, (x \cdot y = y \wedge y \cdot x = y),$$

- e satisfies the formula
$$\forall y\ x \cdot y = y.$$

In this case e is the *only* element of M that satisfies this formula. Thus for every formula $\varphi(\vec{x})$ in the signature $\{\mathrm{e}, \cdot\}$ of monoids, there is a formula $\varphi^*(\vec{x})$ in the signature $\{\cdot\}$ of semigroups such that every monoid satisfies

$$\forall \vec{x}\ \big(\varphi(\vec{x}) \Leftrightarrow \varphi^*(\vec{x})\big).$$

One obtains φ^* from φ by replacing every equation $\mathrm{e} \cdot x = y$ with the formula $\exists z\ (z \cdot x = y \wedge \forall u\ z \cdot u = u)$, and so forth. However:

- Not every function from one monoid to another that is a homomorphism of semigroups is a homomorphism of monoids.
- The theory of semigroups that expand to monoids cannot be axiomatized by $\forall\exists$ sentences.

Exercise 10 (I.2.9)**.** If f is a homomorphism from a group $\mathfrak{G}$ to a group $\mathfrak{H}$, and $\mathfrak{K} < \mathfrak{H}$, show that

(a) $\operatorname{im}(f)$ is the universe of a subgroup of $\mathfrak{H}$ (briefly, $\operatorname{im}(f) < H$),
(b) $f^{-1}(K)$ is the universe of a subgroup of $\mathfrak{G}$ (*i.e.* $f^{-1}(K) < G$),
(c) $\ker(f)$ is the universe of a subgroup of $\mathfrak{G}$ (*i.e.* $\ker(f) < G$),
(d) f is injective if and only if $\ker(f) = \{\mathrm{e}^{\mathfrak{G}}\}$.

Exercise 11 (I.2.2)**.** Show that a group $\mathfrak{G}$ is abelian if and only if the permutation $x \mapsto x^{-1}$ of G is an automorphism of $\mathfrak{G}$.

Exercise 12. In a monoid, show that, if an element has a left inverse and a right inverse, then these are equal.

Exercise 13. Let $\mathbb{H}$ be the abelian group $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$. We use the notation

$$(1,0,0,0) = 1, \qquad (0,1,0,0) = \mathbf{i},$$
$$(0,0,1,0) = \mathbf{j}, \qquad (0,0,0,1) = \mathbf{k}.$$

More generally, we let

$$(x,0,0,0) = x, \qquad (0,x,0,0) = x\mathbf{i},$$
$$(0,0,x,0) = x\mathbf{j}, \qquad (0,0,0,x) = x\mathbf{k}.$$

Thus every element (x, y, z, w) of $\mathbb{H}$ can be written as $x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$. We define a *multiplication* (that is, an operation that distributes in both senses over addition) by these rules:

$$\begin{aligned}
\mathbf{i}\cdot x &= x\mathbf{i}, & \mathbf{j}\cdot x &= x\mathbf{j}, & \mathbf{k}\cdot x &= x\mathbf{k},\\
\mathbf{i}^2 &= -1, & \mathbf{j}^2 &= -1, & \mathbf{k}^2 &= -1,\\
\mathbf{i}\cdot\mathbf{j} &= \mathbf{k}, & \mathbf{j}\cdot\mathbf{k} &= \mathbf{i}, & \mathbf{k}\cdot\mathbf{i} &= \mathbf{j},\\
\mathbf{j}\cdot\mathbf{i} &= -\mathbf{k}, & \mathbf{k}\cdot\mathbf{j} &= -\mathbf{i}, & \mathbf{i}\cdot\mathbf{k} &= -\mathbf{j}.
\end{aligned}$$

So now $\mathbb{H}$ is a (possibly non-associative) ring.

(a) Show that multiplication on $\mathbb{H}$ is associative, so that $(\mathbb{H}, 1, \cdot)$ is a monoid. There are several possible approaches to this, including the following. (So the real challenge of this problem is to find the most efficient approach to it.)

[i] One can show directly

$$\begin{aligned}
&\big((x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}) \cdot (y_0 + y_1\mathbf{i} + y_2\mathbf{j} + y_3\mathbf{k})\big) \cdot\\
&\quad\cdot (z_0 + z_1\mathbf{i} + z_2\mathbf{j} + z_3\mathbf{k}) = (x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}) \cdot\\
&\qquad\cdot \big((y_0 + y_1\mathbf{i} + y_2\mathbf{j} + y_3\mathbf{k}) \cdot (z_0 + z_1\mathbf{i} + z_2\mathbf{j} + z_3\mathbf{k})\big).
\end{aligned}$$

[ii] Letting $\mathbf{e}_0 = 1$, $\mathbf{e}_1 = \mathbf{i}$, $\mathbf{e}_2 = \mathbf{j}$, and $\mathbf{e}_3 = \mathbf{k}$, one can first observe that

$$\begin{aligned}
&\left(\left(\sum_{n<4} x_n\mathbf{e}_n\right) \cdot \sum_{n<4} x_n\mathbf{e}_n\right) \cdot \sum_{n<4} x_n\mathbf{e}_n\\
&\qquad\qquad = \sum_{m<4}\sum_{n<4}\sum_{r<4} x_m y_n z_r \big((\mathbf{e}_m \cdot \mathbf{e}_n) \cdot \mathbf{e}_r\big)
\end{aligned}$$

and

$$\begin{aligned}
&\left(\sum_{n<4} x_n\mathbf{e}_n\right) \cdot \left(\left(\sum_{n<4} x_n\mathbf{e}_n\right) \cdot \sum_{n<4} x_n\mathbf{e}_n\right)\\
&\qquad\qquad = \sum_{m<4}\sum_{n<4}\sum_{r<4} x_m y_n z_r \big(\mathbf{e}_m \cdot (\mathbf{e}_n \cdot \mathbf{e}_r)\big).
\end{aligned}$$

Also, the definition of multiplication is unaffected by the permutations $(1\ 2\ 3)$ and $(1\ 3\ 2)$ of the set $\{1, 2, 3\}$ of indices of the $\mathbf{e}_n$.

[iii] One can observe $x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} = x + y\mathbf{i} + (z + w\mathbf{i}) \cdot \mathbf{j}$, and the elements $x + y\mathbf{i}$ can be considered as elements of the field $\mathbb{C}$. If now $z \in \mathbb{C}$, we have $\mathbf{j} \cdot z = \bar{z}\mathbf{j}$.

[iv] As a ring, $\mathbb{H}$ embeds in the associative ring of 2×2 matrices over $\mathbb{C}$ under the map

$$x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} \mapsto \begin{pmatrix} x + y\mathbf{i} & z + w\mathbf{i} \\ -z + w\mathbf{i} & x - y\mathbf{i} \end{pmatrix}.$$

[v] As a ring, $\mathbb{H}$ embeds in the associative ring of 4×4 matrices over $\mathbb{R}$ under the map

$$x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} \mapsto \begin{pmatrix} x & y & z & w \\ -y & x & -w & z \\ -z & w & x & -y \\ -w & -z & y & x \end{pmatrix}.$$

(b) The semigroup $(\mathbb{C} \smallsetminus \{0\}, \cdot)$ is a group because

$$(x + y\mathbf{i})(x - y\mathbf{i}) = x^2 + y^2,$$

so that (assuming $x + y\mathbf{i} \neq 0$)

$$(x + y\mathbf{i})\Big(\frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}\mathbf{i}\Big) = 1.$$

Find an operation $h \mapsto \bar{h}$ on $\mathbb{H}$ such that

$$h \mapsto h \cdot \bar{h} \colon \mathbb{H} \smallsetminus \{0\} \to \mathbb{R} \smallsetminus \{0\}.$$

Then show that $(\mathbb{H} \smallsetminus \{0\}, \cdot)$ is a group.

Remark. Consequently $\mathbb{H}$ (as a structure in the signature $\{0, -, +, 1, \cdot\}$) is a **division ring.**

Exercise 14 (I.2.4)**.** (a) Show that the elements $(0\ 1\ 2\ 3)$ and $(0\ 3)$ generate a subgroup, called $\mathrm{Dih}(4)$, of $\mathrm{Sym}(3)$ of order 8. One way to do this is to consider the given elements as permutations of the vertices of a square.

(b) Show that $\mathrm{Dih}(4)$ is not isomorphic to the subgroup Q_8 of $\mathbb{H} \smallsetminus \{0\}$ generated by $\mathbf{i}$ and $\mathbf{j}$.

Exercise 15 (I.2.12)**.** Find all (a, b) in $\mathbb{Z} \oplus \mathbb{Z}$ such that, for some (c, d) in $\mathbb{Z} \oplus \mathbb{Z}$,

$$\mathbb{Z} \oplus \mathbb{Z} = \langle (a, b), (c, d) \rangle.$$

It may be useful to consider $x(a, b) + y(c, d)$ as the matrix product

$$(x\ y) \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then the information in Exercise 3 will be useful.

Exercise 16. In the most general sense, an **algebra** is a structure with no distinguished relations, but only operations. Suppose $\mathfrak{A}$ is an algebra with universe A. A **congruence-relation** on $\mathfrak{A}$ is an equivalence-relation $\sim$ on A such that for all n in ω, for all distinguished n-ary operations f of $\mathfrak{A}$,

$$x_0 \sim y_0 \land \cdots \land x_{n-1} \sim y_{n-1} \implies f(\vec{x}) = f(\vec{y}).$$

In this case there is an n-ary operation $\tilde{f}$ on $A/{\sim}$ given by

$$\tilde{f}([x_0], \ldots, [x_{n-1}]) = f(x_0, \ldots, x_{n-1}).$$

(In particular, $\tilde{f}$ exists automatically when $n = 0$.) If indeed $\sim$ is a congruence-relation on $\mathfrak{A}$, then there is a quotient algebra $\mathfrak{A}/{\sim}$ whose universe is $A/{\sim}$ and whose distinguished operations are just these $\tilde{f}$.

Suppose $\sim$ is a congruence-relation on a semigroup $(G, \cdot)$, so that there is an operation on $G/{\sim}$ given by

$$[x][y] = [xy].$$

(a) Show that $(G, \cdot)/{\sim}$ is a semigroup.
(b) If $(G, \cdot)$ expands to a group, show that $\sim$ is a congruence-relation on this group, and the quotient of the group by $\sim$ is a group.
(c) If $n \in \mathbb{N}$, we define $\equiv$ on $\mathbb{Z}$ by

$$x \equiv y \iff n \mid x - y.$$

Show that $\equiv$ is a congruence-relation on $\mathbb{Z}$ as a ring. (This was taken for granted in Exercise 3.)

Exercise 17 (I.3.3)**.** The only big theorem used by this exercise is the Lagrange Theorem, that the order of a subgroup divides the order of the group. Suppose G is a group of order pq, where p and q are distinct prime numbers. Prove the following.

(a) If a and b are in G and $\operatorname{ord}(a) = p = \operatorname{ord}(b)$, then either $\langle a \rangle = \langle b \rangle$ or $\langle a \rangle \cap \langle b \rangle = \langle\ \rangle$.
(b) G has an element of order p or q.
(c) $G = \langle a, b \rangle$ for some a and b in G.
(d) If G is abelian, then G is cyclic.

Exercise 18 (I.3.5, 9)**.** (a) Find an infinite group generated by two elements, each of which has finite order. You can use the example of the subgroup of $\operatorname{Sym}(\mathbb{C}^{\times})$ generated by the elements

$$\tau \mapsto \frac{-1}{\tau}, \qquad \tau \mapsto \frac{-1}{\tau + 1}.$$

(b) Show that no group as in (a) can be abelian.
(c) Find an infinite group containing nontrivial elements of finite order, but generated by two elements, each having infinite order. You can let $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ be the group.

Exercise 19 (I.3.6)**.** Given n in $\mathbb{N}$, describe all subgroups of $\mathbb{Z}/n\mathbb{Z}$. (What are their orders? What are their generators? Are they cyclic?)

Exercise 20 (I.4.2)**.** Find all cosets (in terms of their elements) of $\langle(0\ 1)\rangle$ and of $\langle(0\ 1\ 2)\rangle$ in $\operatorname{Sym}(3)$.

Exercise 21 (I.4.5)**.** Find all groups of order 4 (up to isomorphism). Lagrange's Theorem and Exercise 7 may be useful.

Exercise 22. An **automorphism** of a group is an isomorphism from the group to itself. The set of automorphisms of a group G can be denoted by $\operatorname{Aut}(G)$.

(a) Show that $\operatorname{Aut}(G) < \operatorname{Sym}(G)$. (The first G is the group; the second, the set. Strictly one would write $\operatorname{Aut}(G, \cdot) < \operatorname{Sym}(G)$.)
(b) Find $\operatorname{Aut}(\mathbb{Z}/4\mathbb{Z})$.
(c) Find $\operatorname{Aut}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$.

Exercise 23 (I.5.6)**.** Show that there is a homomorphism $x \mapsto f_x$ from a group G to $\mathrm{Aut}(G)$ given by

$$f_x(y) = xyx^{-1}.$$

Exercise 24 (I.5.7)**.** If $H < G$, show that, under either of the following two conditions, $H \lhd G$.

(a) H is finite and is the only subgroup of G of its order.
(b) $[G : H]$ is finite, and H is the only subgroup of G having this index in G.

Exercise 25 (I.5.10, 11)**.** (a) Show that the relation $\lhd$ of being a normal subgroup is not transitive. You can use subgroups of $\mathrm{Dih}(4)$ for an example.
(b) Show that if $K < H$ and $H \lhd G$ and H is cyclic, then $K \lhd G$.

Exercise 26 (I.6.4)**.** Show $\mathrm{Sym}(n) = \langle (0\ 1\ \cdots\ n-1), (0\ 1) \rangle$.

Exercise 27 (I.6.11)**.** Find all normal subgroups of $\mathrm{Dih}(n)$.

Exercise 28. Suppose $(G_i : i \in I)$ is a family of groups, and for each i in I, $H_i \lhd G_i$. Show

$$\prod_{i\in I} H_i \lhd \prod_{i\in I} G_i, \qquad \prod_{i\in I} G_i \Big/ \prod_{i\in I} H_i \cong \prod_{i\in I} \frac{G_i}{H_i}.$$

Exercise 29 (I.9.3)**.** For any set A, let $\mathrm{F}(A)$ be the free group on A. If $A \subseteq B$, show that $\mathrm{F}(B)/\langle\langle A \rangle\rangle$ is a free group.

Exercise 30. Describe the groups

(a) $\langle a, b \mid a^7, b^3, a^2ba^6b^2 \rangle$,

(b) $\langle a, b \mid a^7, b^3, a^3ba^6b^2 \rangle$.

Exercise 31 (II.1.11)**.** Show that $(\mathbb{Q}^+, \cdot)$ is a free abelian group.

Exercise 32. How many nonisomorphic abelian groups have order p^n?

Exercise 33 (II.4.9)**.** If G is not abelian, then $G/\,\mathrm{C}(G)$ is not cyclic.

Exercise 34 (II.4.14)**.** If p is a prime dividing $|G|$, and

$$1 < \frac{|G|}{p} \leqslant p,$$

then G is not simple.

Exercise 35 (II.5.11)**.** In a simple group of order 168, how many elements have order 7?

Exercise 36.

(a) Find the smallest nonabelian group.
(b) Find the smallest nonabelian soluble group.
(c) Find the smallest nonabelian soluble group that is not nilpotent.

Exercise 37 (II.7.8)**.**

(a) Find all n such that $\mathrm{Dih}(n)$ is nilpotent.
(b) For such n, find the groups $\mathrm{C}_k(\mathrm{Dih}(n))$.
(c) Find all m such that $\mathrm{Dih}(m)$ is soluble.
(d) For such m, find the groups $(\mathrm{Dih}(m))^{(k)}$.

Exercise 38. In a commutative ring, by definition, a proper ideal P is prime if and only if, for all x and y in the ring,

$$xy \in P \ \& \ x \notin P \implies y \in P.$$

Prove that the proper ideal P is prime if and only if, for all all ideals I and J,

$$IJ \subseteq P \ \& \ I \nsubseteq P \implies J \subseteq P.$$

Here

$$IJ = (\{xy \colon x \in I \ \& \ y \in J\}).$$

Proof. The sufficiency of the given condition follows because

$$(xy) = (x)(y),$$
$$x \in P \iff (x) \subseteq P.$$

For necessity, suppose P is prime, and $IJ \subseteq P$, but $I \nsubseteq P$. Then some element x of I is not in P. For all y in J, we have $xy \in IJ$, so $xy \in P$, and therefore $y \in P$. Thus $J \subseteq P$. □

Exercise 39. Given a commutative ring R with an ideal I, show that every ideal of R/I is of the form J/I for some ideal J of I.

Proof. Say K is an ideal of R/I. Let $J = \{x \in R\colon x + I \in K\}$. For all x, y, and r in R, if $x + I$ and $y + I$ are in K, then

$$(x + I) - (y + I) \in K, \qquad\qquad (r + I)(x + I) \in K,$$

and therefore $x - y \in J$ and $rx \in J$. Thus J is an ideal of R. Moreover, since $x + I \in K \iff x \in J$, and $x \in J \iff x + I \in J/I$, we have $K = J/I$. □

Exercise 40. Let R be a commutative ring with proper ideal I.

(a) If R is an integral domain, must R/I be an integral domain?
(b) If R is a unique factorization domain (UFD) and R/I is an integral domain, must R/I be a UFD?
(c) If R is a principal ideal domain (PID) and R/I is a unique factorization domain, must R/I be a PID?
(d) If R is a field, must R/I be a field?

Note: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Exercise 41 (III.2.21)**.** If $n \in \mathbb{N}$, find all prime ideals and all maximal ideals of $\mathbb{Z}_n$.

Proof. By Exercise 40, $\mathbb{Z}_n$ is a PID. Every ideal (k) of $\mathbb{Z}_n$ is equal to (d), where $d = \gcd(k, n)$: this is because the equation $kx + ny = d$ is soluble. Thus every quotient of $\mathbb{Z}_n$ is $\mathbb{Z}_n/(d)$ for some divisor d of n; and this quotient is isomorphic to $\mathbb{Z}_d$. This is an integral domain if and only if d is prime, and in this case the domain is a field. Thus the prime ideals of $\mathbb{Z}_n$ are the ideals (p), where p is a prime factor of n; and these prime ideals are all maximal. □

Exercise 42 (III.1.11, 6.10)**.**

(a) Prove the Binomial Theorem: In every commutative ring, for every n in ω,

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i,$$

where

$$\binom{n}{i} = \frac{n!}{i! \cdot (n-i)!}.$$

(b) Let R be an integral domain with quotient field K. Thus, if $a \in R$ and $b \in R \smallsetminus (0)$, then $a/b \in K$. Assume a/b is an element c of R, and π is an irreducible of R such that $\pi \mid a$, but $\pi \nmid b$. Can you conclude that $p \mid c$?

(c) Let p be a prime number. If $0 < i < p$, prove

$$p \biggm| \binom{p}{i}.$$

(d) Prove the indentity

$$(x+y)^p = x^p + y^p$$

in all commutative rings having characteristic p.

(e) Prove that $x \mapsto x^p$ is an endomorphism of every commutative ring having characteristic p.

(f) For all n in ω, prove that $x \mapsto x^{p^n}$ is an endomorphism of every commutative ring having characteristic p.

(g) For all n in ω, prove the indentity

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

in all commutative rings having characteristic p.

(h) If $n \in \mathbb{N}$ and $0 < i < p^n$, prove

$$p \biggm| \binom{p^n}{i}.$$

(i) Prove the irreducibility over $\mathbb{Q}$ of the polynomial

$$1 + X + \cdots + X^{p-1}.$$

References

[1] Euclid. *Euclid's Elements.* Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, the Thomas L. Heath translation, edited by Dana Densmore.

[2] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986. Translated into English by Arthur A. Clarke, revised by William C. Waterhouse.

[3] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.