

# Exercises from *Algebra* by Michael Artin

**Exercise 2.2.9** Let  $H$  be the subgroup generated by two elements  $a, b$  of a group  $G$ . Prove that if  $ab = ba$ , then  $H$  is an abelian group.

*Proof.* Since  $a$  and  $b$  commute, for any  $g, h \in H$  we can write  $g = a^i b^j$  and  $h = a^k b^l$ . Then  $gh = a^i b^j a^k b^l = a^k b^l a^i b^j = hg$ . Thus  $H$  is abelian.  $\square$

**Exercise 2.3.2** Prove that the products  $ab$  and  $ba$  are conjugate elements in a group.

*Proof.* We have that  $(a^{-1})ab(a^{-1})^{-1} = ba$ .  $\square$

**Exercise 2.4.19** Prove that if a group contains exactly one element of order 2, then that element is in the center of the group.

*Proof.* Let  $x$  be the element of order two. Consider the element  $z = y^{-1}xy$ , we have:  $z^2 = (y^{-1}xy)^2 = (y^{-1}xy)(y^{-1}xy) = e$ . So:  $z = x$ , and  $y^{-1}xy = x$ . So:  $xy = yx$ . So:  $x$  is in the center of  $G$ .  $\square$

**Exercise 2.8.6** Prove that the center of the product of two groups is the product of their centers.

*Proof.* We have that  $(g_1, g_2) \cdot (h_1, h_2) = (h_1, h_2) \cdot (g_1, g_2)$  if and only if  $g_1 h_1 = h_1 g_1$  and  $g_2 h_2 = h_2 g_2$ .  $\square$

**Exercise 2.11.3** Prove that a group of even order contains an element of order 2.

*Proof.* Pair up if possible each element of  $G$  with its inverse, and observe that

$$g^2 \neq e \iff g \neq g^{-1} \iff \text{there exists the pair } (g, g^{-1})$$

Now, there is one element that has no pairing: the unit  $e$  (since indeed  $e = e^{-1} \iff e^2 = e$ ), so since the number of elements of  $G$  is even there must be at least one element more, say  $e \neq a \in G$ , without a pairing, and thus  $a = a^{-1} \iff a^2 = e$   $\square$

**Exercise 3.2.7** Prove that every homomorphism of fields is injective.

*Proof.* Suppose  $f(a) = f(b)$ , then  $f(a - b) = 0 = f(0)$ . If  $u = (a - b) \neq 0$ , then  $f(u)f(u^{-1}) = f(1) = 1$ , but that means that  $0f(u^{-1}) = 1$ , which is impossible. Hence  $a - b = 0$  and  $a = b$ .  $\square$

**Exercise 3.5.6** Let  $V$  be a vector space which is spanned by a countably infinite set. Prove that every linearly independent subset of  $V$  is finite or countably infinite.

*Proof.* Let  $A$  be the countable generating set, and let  $U$  be an uncountable linearly independent set. It can be extended to a basis  $B$  of the whole space. Now consider the subset  $C$  of elements of  $B$  that appear in the  $B$ -decompositions of elements of  $A$ . Since only finitely many elements are involved in the decomposition of each element of  $A$ , the set  $C$  is countable. But  $C$  also clearly generates the vector space  $V$ . This contradicts the fact that it is a proper subset of the basis  $B$  (since  $B$  is uncountable).  $\square$

**Exercise 3.7.2** Let  $V$  be a vector space over an infinite field  $F$ . Prove that  $V$  is not the union of finitely many proper subspaces.

*Proof.* If  $V$  is the set-theoretic union of  $n$  proper subspaces  $W_i$  ( $1 \leq i \leq n$ ), then  $|F| \leq n - 1$ . *Proof.* We may suppose no  $W_i$  is contained in the union of the other subspaces. Let  $u \in W_i$ ,  $u \notin \bigcup_{j \neq i} W_j$  and  $v \notin W_i$ . Then  $(v + Fu) \cap W_i = \emptyset$  and  $(v + Fu) \cap W_j$  ( $j \neq i$ ) contains at most one vector since otherwise  $W_j$  would contain  $u$ . Hence

$$|v + Fu| = |F| \leq n - 1.$$

Corollary: Avoidance lemma for vector spaces. Let  $E$  be a vector space over an infinite field. If a subspace is contained in a finite union of subspaces, it is contained in one of them.  $\square$

**Exercise 6.1.14** Let  $Z$  be the center of a group  $G$ . Prove that if  $G/Z$  is a cyclic group, then  $G$  is abelian and hence  $G = Z$ .

*Proof.* We have that  $G/Z(G)$  is cyclic, and so there is an element  $x \in G$  such that  $G/Z(G) = \langle xZ(G) \rangle$ , where  $xZ(G)$  is the coset with representative  $x$ . Now let  $g \in G$ . We know that  $gZ(G) = (xZ(G))^m$  for some  $m$ , and by definition  $(xZ(G))^m = x^mZ(G)$ . Now, in general, if  $H \leq G$ , we have by definition too that  $aH = bH$  if and only if  $b^{-1}a \in H$ . In our case, we have that  $gZ(G) = x^mZ(G)$ , and this happens if and only if  $(x^m)^{-1}g \in Z(G)$ . Then, there's a  $z \in Z(G)$  such that  $(x^m)^{-1}g = z$ , and so  $g = x^mz$ .

$g, h \in G$  implies that  $g = x^{a_1} z_1$  and  $h = x^{a_2} z_2$ , so

$$\begin{aligned} gh &= (x^{a_1} z_1) (x^{a_2} z_2) \\ &= x^{a_1} x^{a_2} z_1 z_2 \\ &= x^{a_1+a_2} z_2 z_1 \\ &= \dots = (x^{a_2} z_2) (x^{a_1} z_1) = hg. \end{aligned}$$

Therefore,  $G$  is abelian.  $\square$

**Exercise 6.4.2** Prove that no group of order  $pq$ , where  $p$  and  $q$  are prime, is simple.

*Proof.* If  $|G| = n = pq$  then the only two Sylow subgroups are of order  $p$  and  $q$ . From Sylow's third theorem we know that  $n_p \mid q$  which means that  $n_p = 1$  or  $n_p = q$ . If  $n_p = 1$  then we are done (by a corollary of Sylow's theorem) If  $n_p = q$  then we have accounted for  $q(p-1) = pq - q$  elements of  $G$  and so there is only one group of order  $q$  and again we are done.  $\square$

**Exercise 6.4.3** Prove that no group of order  $p^2q$ , where  $p$  and  $q$  are prime, is simple.

*Proof.* We may as well assume  $p < q$ . The number of Sylow  $q$ -subgroups is  $1 \pmod q$  and divides  $p^2$ . So it is  $1, p$ , or  $p^2$ . We win if it's  $1$  and it can't be  $p$ , so suppose it's  $p^2$ . But now  $q \mid p^2 - 1$ , so  $q \mid p + 1$  or  $q \mid p - 1$ . Thus  $p = 2$  and  $q = 3$ . But we know no group of order  $36$  is simple.  $\square$

**Exercise 6.4.12** Prove that no group of order  $224$  is simple.

*Proof.* The following proves there must exist a normal Sylow  $2$ -subgroup of order  $32$ . Suppose there are  $n_2 = 7$  Sylow  $2$ -subgroups in  $G$ . Making  $G$  act on the set of these Sylow subgroups by conjugation (Mitt wrote about this but on the set of the other Sylow subgroups, which gives no contradiction), we get a homomorphism  $G \rightarrow S_7$  which must be injective if  $G$  is simple (why?).

But this cannot be since then we would embed  $G$  into  $S_7$ , which is impossible since  $|G| \nmid 7! = |S_7|$  (why?)  $\square$

**Exercise 6.8.1** Prove that two elements  $a, b$  of a group generate the same subgroup as  $bab^2, bab^3$ .

*Proof.* Let  $H = \langle bab^2, bab^3 \rangle$ . It is clear that  $H \subset \langle a, b \rangle$ . Note that  $(bab^2)^{-1}(bab^3) = b$ , therefore  $b \in H$ . This then implies that  $b^{-1}(bab^2)b^{-2} = a \in H$ . Thus  $\langle a, b \rangle \subset H$ .  $\square$

**Exercise 6.8.6** Let  $G$  be a group with a normal subgroup  $N$ . Assume that  $G$  and  $G/N$  are both cyclic groups. Prove that  $G$  can be generated by two elements.

**Exercise 10.1.13** An element  $x$  of a ring  $R$  is called nilpotent if some power of  $x$  is zero. Prove that if  $x$  is nilpotent, then  $1 + x$  is a unit in  $R$ .

*Proof.* If  $x^n = 0$ , then

$$(1 + x) \left( \sum_{k=0}^{n-1} (-1)^k x^k \right) = 1 + (-1)^{n-1} x^n = 1.$$

□

**Exercise 10.2.4** Prove that in the ring  $\mathbb{Z}[x]$ ,  $(2) \cap (x) = (2x)$ .

*Proof.* Let  $f(x) \in (2x)$ . Then there exists some polynomial  $g(x) \in \mathbb{Z}$  such that

$$f(x) = 2xg(x)$$

But this means that  $f(x) \in (2)$  (because  $xg(x)$  is a polynomial), and  $f(x) \in (x)$  (because  $2g(x)$  is a polynomial). Thus,  $f(x) \in (2) \cap (x)$ , and

$$(2x) \subseteq (2) \cap (x)$$

On the other hand, let  $p(x) \in (2) \cap (x)$ . Since  $p(x) \in (2)$ , there exists some polynomial  $h(x) \in \mathbb{Z}[x]$  such that

$$p(x) = 2h(x)$$

Furthermore,  $p(x) \in (x)$ , so

$$p(x) = xh_2(x)$$

So,  $2h(x) = xh_2(x)$ , for some  $h_2(x) \in \mathbb{Z}[x]$ . This means that  $h(0) = 0$ , so  $x$  divides  $h(x)$ ; that is,

$$h(x) = xq(x)$$

for some  $q(x) \in \mathbb{Z}[x]$ , and

$$p(x) = 2xq(x)$$

Thus,  $p(x) \in (2x)$ , and

$$(2) \cap (x) \subseteq (2x)$$

Finally,  $(2) \cap (x) = (2x)$ , as required. □

**Exercise 10.6.7** Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

*Proof.* Let  $I$  be some nonzero ideal. Then there exists some  $z \in \mathbb{Z}[i]$ ,  $z \neq 0$  such that  $z \in I$ . We know that  $z = a + bi$ , for some  $a, b \in \mathbb{Z}$ . We consider three cases: 1. If  $b = 0$ , then  $z = a$ , so  $z \in \mathbb{Z} \cap I$ , and  $z \neq 0$ , so the statement of the exercise holds. 2. If  $a = 0$ , then  $z = ib$ . Since  $z \neq 0$ , we conclude that  $b \neq 0$ . Since  $I$  is an ideal in  $\mathbb{Z}[i]$ , and  $i \in \mathbb{Z}[i]$ , we conclude that  $iz \in I$ . Furthermore,

$iz = -b \in \mathbb{Z}$ . Thus,  $iz$  is a nonzero integer which is in  $I$ . 3. Let  $a \neq 0$  and  $b \neq 0$ . Since  $I$  is an ideal and  $z \in I$ , we conclude that  $z^2 \in I$ ; that is,

$$(a + bi)^2 = a^2 - b^2 + 2abi \in I$$

Furthermore, since  $-2a \in \mathbb{Z}[i]$ , and  $z \in I$  and  $I$  is an ideal,  $-2az \in I$ ; that is,

$$-2az = -2a(a + bi) = -2a^2 - 2abi \in I$$

Since  $I$  is closed under addition,

$$(a^2 - b^2 + 2abi) + (-2a^2 - 2abi) \in I \implies -a^2 - b^2 \in I$$

Notice that  $-a^2 - b^2 \neq 0$  since  $a^2 > 0$  and  $b^2 > 0$ , so  $-a^2 - b^2 < 0$ . Furthermore, it is an integer. Thus, we have found a nonzero integer in  $I$ .  $\square$

**Exercise 10.4.6** Let  $I, J$  be ideals in a ring  $R$ . Prove that the residue of any element of  $I \cap J$  in  $R/IJ$  is nilpotent.

*Proof.* If  $x$  is in  $I \cap J$ ,  $x \in I$  and  $x \in J$ .  $R/IJ = \{r + ab : a \in I, b \in J, r \in R\}$ . Then  $x \in I \cap J \implies x \in I$  and  $x \in J$ , and so  $x^2 \in IJ$ . Thus

$$[x]^2 = [x^2] = [0] \text{ in } R/IJ$$

$\square$

**Exercise 10.4.7a** Let  $I, J$  be ideals of a ring  $R$  such that  $I + J = R$ . Prove that  $IJ = I \cap J$ .

*Proof.* We have seen that  $IJ \subset I \cap J$ , so it remains to show that  $I \cap J \subset IJ$ . Since  $I + J = (1)$ , there are elements  $i \in I$  and  $j \in J$  such that  $i + j = 1$ . Let  $k \in I \cap J$ , and multiply  $i + j = 1$  through by  $k$  to get  $ki + kj = k$ . Write this more suggestively as

$$k = ik + kj.$$

The first term is in  $IJ$  because  $k \in J$ , and the second term is in  $IJ$  because  $k \in I$ , so  $k \in IJ$  as desired.  $\square$

**Exercise 10.5.16** Let  $F$  be a field. Prove that the rings  $F[x]/(x^2)$  and  $F[x]/(x^2 - 1)$  are isomorphic if and only if  $F$  has characteristic 2.

**Exercise 10.7.6** Prove that the ring  $\mathbb{F}_5[x]/(x^2 + x + 1)$  is a field.

**Exercise 10.7.10** Let  $R$  be a ring, with  $M$  an ideal of  $R$ . Suppose that every element of  $R$  which is not in  $M$  is a unit of  $R$ . Prove that  $M$  is a maximal ideal and that moreover it is the only maximal ideal of  $R$ .

*Proof.* Suppose there is an ideal  $M \subset I \subset R$ . If  $I \neq M$ , then  $I$  contains a unit, thus  $I = R$ . Therefore  $M$  is a maximal ideal.

Suppose we have an arbitrary maximal ideal  $M'$  of  $R$ . The ideal  $M'$  cannot contain a unit, otherwise  $M' = R$ . Therefore  $M' \subset M$ . But we cannot have  $M' \subsetneq M \subsetneq R$ , therefore  $M = M'$ .  $\square$

**Exercise 11.2.13** If  $a, b$  are integers and if  $a$  divides  $b$  in the ring of Gauss integers, then  $a$  divides  $b$  in  $\mathbb{Z}$ .

*Proof.* Suppose  $a|b$  in  $\mathbb{Z}[i]$  and  $a, b \in \mathbb{Z}$ . Then  $a(x + yi) = b$  for  $x, y \in \mathbb{Z}$ . Expanding this we get  $ax + ayi = b$ , and equating imaginary parts gives us  $ay = 0$ , implying  $y = 0$ .  $\square$

**Exercise 11.3.1** Let  $a, b$  be elements of a field  $F$ , with  $a \neq 0$ . Prove that a polynomial  $f(x) \in F[x]$  is irreducible if and only if  $f(ax + b)$  is irreducible.

**Exercise 11.3.4** Prove that two integer polynomials are relatively prime in  $\mathbb{Q}[x]$  if and only if the ideal they generate in  $\mathbb{Z}[x]$  contains an integer.

**Exercise 11.4.1b** Prove that  $x^3 + 6x + 12$  is irreducible in  $\mathbb{Q}$ .

*Proof.* Apply Eisenstein's criterion with  $p = 3$ .  $\square$

**Exercise 11.4.6a** Prove that  $x^2 + x + 1$  is irreducible in the field  $\mathbb{F}_2$ .

*Proof.* If  $x^2 + x + 1$  were reducible in  $\mathbb{F}_2$ , its factors must be linear. But we neither have that  $0^2 + 0 + 1 = 1$  nor  $1^2 + 1 + 1 = 0$ , therefore  $x^2 + x + 1$  is irreducible.  $\square$

**Exercise 11.4.6b** Prove that  $x^2 + 1$  is irreducible in  $\mathbb{F}_7$

*Proof.* If  $p(x) = x^2 + 1$  were reducible, its factors must be linear. But no  $p(a)$  for  $a \in \mathbb{F}_7$  evaluates to 0, therefore  $x^2 + 1$  is irreducible.  $\square$

**Exercise 11.4.6c** Prove that  $x^3 - 9$  is irreducible in  $\mathbb{F}_{31}$ .

*Proof.* If  $p(x) = x^3 - 9$  were reducible, it would have a linear factor, since it either has a linear factor and a quadratic factor or three linear factors. We can then verify by brute force that  $p(x) \neq 0$  for  $x \in \mathbb{F}_31$ .  $\square$

**Exercise 11.4.8** Let  $p$  be a prime integer. Prove that the polynomial  $x^n - p$  is irreducible in  $\mathbb{Q}[x]$ .

*Proof.* Straightforward application of Eisenstein's criterion with  $p$ .  $\square$

**Exercise 11.12.3** Prove that if  $x^2 \equiv -5 \pmod{p}$  has a solution, then there is an integer point on one of the two ellipses  $x^2 + 5y^2 = p$  or  $2x^2 + 2xy + 3y^2 = p$ .

**Exercise 11.13.3** Prove that there are infinitely many primes congruent to  $-1$  (modulo 4).

*Proof.* First we show a lemma: if  $a \equiv 3 \pmod{4}$  then there exists a prime  $p$  such that  $p \mid a$  and  $p \equiv 3 \pmod{4}$ .

Clearly, all primes dividing  $a$  are odd. Suppose all of them would be  $\equiv 1 \pmod{4}$ . Then their product would also be  $a \equiv 1 \pmod{4}$ , which is a contradiction.

To prove the main claim, suppose that  $p_1, \dots, p_n$  would be all such primes. (In particular, we have  $p_1 = 3$ .) Consider  $a = 4p_2 \cdots p_n + 3$ . (Or you can take  $a = 4p_2 \cdots p_n - 1$ .) Show that  $p_i \nmid a$  for  $i = 1, \dots, n$ . (The case  $3 \nmid a$  is solved differently than the other primes - this is the reason for omitting  $p_1$  in the definition of  $a$ .) Then use the above lemma to get a contradiction.  $\square$

**Exercise 13.4.10** Prove that if a prime integer  $p$  has the form  $2^r + 1$ , then it actually has the form  $2^{2^k} + 1$ .

*Proof.* In particular, we have

$$\frac{x^a + 1}{x + 1} = \frac{(-x)^a - 1}{(-x) - 1} = 1 - x + x^2 - \cdots + (-x)^{a-1}$$

by the geometric sum formula. In this case, specialize to  $x = 2^{2^m}$  and we have a nontrivial divisor.  $\square$

**Exercise 13.6.10** Let  $K$  be a finite field. Prove that the product of the nonzero elements of  $K$  is  $-1$ .

*Proof.* Since we are working with a finite field with  $q$  elements, anyone of them is a root of the following polynomial

$$x^q - x = 0.$$

In particular if we rule out the 0 element, any  $a_i \neq 0$  is a root of

$$x^{q-1} - 1 = 0.$$

This polynomial splits completely in  $\mathbb{F}_q$  so we find

$$(x - a_1) \cdots (x - a_{q-1}) = 0$$

in particular

$$x^{q-1} - 1 = (x - a_1) \cdots (x - a_{q-1})$$

Thus  $a_1 \cdots a_{q-1} = -1$ .  $\square$