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. □

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

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

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: $z^2 = \left(y^{-1}xy\right)^2 = \left(y^{-1}xy\right)\left(y^{-1}xy\right) = e$. So: $z = x$, and $y^{-1}xy = x$. So: $xy = yx$. So: x is in the center of G. □

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 $g_2 h_2 = h_2 g_2$. □

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

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

Now, there is one element that has no pairing: the unit e (since indeed $e = e^{-1} \Longleftrightarrow e^2 = e$), 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 $a = a^{-1} \Longleftrightarrow a^2 = e$ □

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 $f(u)f\left(u^{-1}\right) = f(1) = 1$, but that means that $0f\left(u^{-1}\right) = 1$, which is impossible. Hence $a - b = 0$ and $a = b$. □

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.

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.

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 $G = Z$.

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. □

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 mod 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. □

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 $G \to S_7$ 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?) □

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

Exercise 6.8.4 Prove that the group generated by x, y, z with the single relation $yxyz^{-2} = 1$ is actually a free group.

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.

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

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

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.

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

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

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

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 $\mathbb{Z}$.

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 $\mathbb{Q}$.

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

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

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

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

Exercise 11.12.3 Prove that if $x^2 \equiv -5$ (modulo 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).

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

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