Exercises from *Abstract Algebra* by David Dummit and Richard Foote

Exercise 1.1.2a Prove the the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$ is not commutative.

Exercise 1.1.3 Prove that the addition of residue classes $\mathbb{Z}/n\mathbb{Z}$ is associative.

Exercise 1.1.4 Prove that the multiplication of residue class $\mathbb{Z}/n\mathbb{Z}$ is associative.

Exercise 1.1.5 Prove that for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

Exercise 1.1.15 Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

Exercise 1.1.16 Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

Exercise 1.1.17 Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

Exercise 1.1.18 Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

Exercise 1.1.20 For x an element in G show that x and x^{-1} have the same order.

Exercise 1.1.22a If x and g are elements of the group G, prove that $|x| = \left|g^{-1}xg\right|$.

Exercise 1.1.22b Deduce that $|ab| = |ba|$ for all $a, b \in G$.

Exercise 1.1.25 Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

Exercise 1.1.29 Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

Exercise 1.1.34 If x is an element of infinite order in G, prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.

Exercise 1.3.8 Prove that if $\Omega = \{1, 2, 3, \ldots\}$ then S_Ω is an infinite group

Exercise 1.6.4 Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Exercise 1.6.11 Let A and B be groups. Prove that $A \times B \cong B \times A$.

Exercise 1.6.17 Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Exercise 1.6.23 Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian.

Exercise 1.7.5 Prove that the kernel of an action of the group G on a set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.

Exercise 1.7.6 Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

Exercise 2.1.5 Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Exercise 2.1.13 Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

Exercise 2.4.4 Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Exercise 2.4.13 Prove that the multiplicative group of positive rational numbers is generated by the set $\left\{\frac{1}{p} \mid p \text{ is a prime}\right\}$.

Exercise 2.4.16a A subgroup M of a group G is called a maximal subgroup if $M \neq G$ and the only subgroups of G which contain M are M and G. Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

Exercise 2.4.16b Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

Exercise 2.4.16c Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only $H = \langle x^p \rangle$ for some prime p dividing n.

Exercise 3.1.3a Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian.

Exercise 3.1.22a Prove that if H and K are normal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Exercise 3.1.22b Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

Exercise 3.2.8 Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Exercise 3.2.11 Let $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume G is finite).

Exercise 3.2.16 Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if p is a prime then $a^p \equiv a (\bmod p)$ for all $a \in \mathbb{Z}$.

Exercise 3.2.21a Prove that $\mathbb{Q}$ has no proper subgroups of finite index.

Exercise 3.3.3 Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either $K \leq H$, or $G = HK$ and $|K : K \cap H| = p$.

Exercise 3.4.1 Prove that if G is an abelian simple group then $G \cong Z_p$ for some prime p (do not assume G is a finite group).

Exercise 3.4.4 Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.

Exercise 3.4.5a Prove that subgroups of a solvable group are solvable.

Exercise 3.4.5b Prove that quotient groups of a solvable group are solvable.

Exercise 3.4.11 Prove that if H is a nontrivial normal subgroup of the solvable group G then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.

Exercise 4.2.8 Prove that if H has finite index n then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

Exercise 4.2.9a Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G.

Exercise 4.2.14 Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

Exercise 4.3.5 If the center of G is of index n, prove that every conjugacy class has at most n elements.

Exercise 4.3.26 Let G be a transitive permutation group on the finite set A with $|A| > 1$. Show that there is some $\sigma \in G$ such that $\sigma(a) \neq a$ for all $a \in A$.

Exercise 4.3.27 Let $g_1, g_2, \ldots, g_r$ be representatives of the conjugacy classes of the finite group G and assume these elements pairwise commute. Prove that G is abelian.

Exercise 4.4.2 Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic.

Exercise 4.4.6a Prove that characteristic subgroups are normal.

Exercise 4.4.6b Prove that there exists a normal subgroup that is not characteristic.

Exercise 4.4.7 If H is the unique subgroup of a given order in a group G prove H is characteristic in G.

Exercise 4.4.8a Let G be a group with subgroups H and K with $H \leq K$. Prove that if H is characteristic in K and K is normal in G then H is normal in G.

Exercise 4.5.1a Prove that if $P \in \mathrm{Syl}_p(G)$ and H is a subgroup of G containing P then $P \in \mathrm{Syl}_p(H)$.

Exercise 4.5.13 Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

Exercise 4.5.14 Prove that a group of order 312 has a normal Sylow p-subgroup for some prime p dividing its order.

Exercise 4.5.15 Prove that a group of order 351 has a normal Sylow p-subgroup for some prime p dividing its order.

Exercise 4.5.16 Let $|G| = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

Exercise 4.5.17 Prove that if $|G| = 105$ then G has a normal Sylow 5 -subgroup and a normal Sylow 7-subgroup.

Exercise 4.5.18 Prove that a group of order 200 has a normal Sylow 5-subgroup.

Exercise 4.5.19 Prove that if $|G| = 6545$ then G is not simple.

Exercise 4.5.20 Prove that if $|G| = 1365$ then G is not simple.

Exercise 4.5.21 Prove that if $|G| = 2907$ then G is not simple.

Exercise 4.5.22 Prove that if $|G| = 132$ then G is not simple.

Exercise 4.5.23 Prove that if $|G| = 462$ then G is not simple.

Exercise 4.5.28 Let G be a group of order 105. Prove that if a Sylow 3-subgroup of G is normal then G is abelian.

Exercise 4.5.33 Let P be a normal Sylow p-subgroup of G and let H be any subgroup of G. Prove that $P \cap H$ is the unique Sylow p-subgroup of H.

Exercise 5.4.2 Prove that a subgroup H of G is normal if and only if $[G, H] \leq H$.

Exercise 7.1.2 Prove that if u is a unit in R then so is $-u$.

Exercise 7.1.11 Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

Exercise 7.1.12 Prove that any subring of a field which contains the identity is an integral domain.

Exercise 7.1.15 A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

Exercise 7.2.2 Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be an element of the polynomial ring $R[x]$. Prove that $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$.

Exercise 7.2.4 Prove that if R is an integral domain then the ring of formal power series $R[[x]]$ is also an integral domain.

Exercise 7.2.12 Let $G = \{g_1, \ldots, g_n\}$ be a finite group. Prove that the element $N = g_1 + g_2 + \ldots + g_n$ is in the center of the group ring RG.

Exercise 7.3.16 Let $\varphi : R \to S$ be a surjective homomorphism of rings. Prove that the image of the center of R is contained in the center of S.

Exercise 7.3.28 Prove that an integral domain has characteristic p, where p is either a prime or 0.

Exercise 7.3.37 An ideal N is called nilpotent if N^n is the zero ideal for some $n \geq 1$. Prove that the ideal $p\mathbb{Z}/p^m\mathbb{Z}$ is a nilpotent ideal in the ring $\mathbb{Z}/p^m\mathbb{Z}$.

Exercise 7.4.27 Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R then $1 - ab$ is a unit for all $b \in R$.

Exercise 8.1.12 Let N be a positive integer. Let M be an integer relatively prime to N and let d be an integer relatively prime to $\varphi(N)$, where φ denotes Euler's φ-function. Prove that if $M_1 \equiv M^d \pmod{N}$ then $M \equiv M_1^{d'} \pmod{N}$ where d' is the inverse of d mod $\varphi(N)$: $dd' \equiv 1 \pmod{\varphi(N)}$.

Exercise 8.2.4 Let R be an integral domain. Prove that if the following two conditions hold then R is a Principal Ideal Domain: (i) any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and (ii) if $a_1, a_2, a_3, \ldots$ are nonzero elements of R such that $a_{i+1} \mid a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

Exercise 8.3.4 Prove that if an integer is the sum of two rational squares, then it is the sum of two integer squares.

Exercise 8.3.5a Let $R = \mathbb{Z}[\sqrt{-n}]$ where n is a squarefree integer greater than 3. Prove that $2, \sqrt{-n}$ and $1 + \sqrt{-n}$ are irreducibles in R.

Exercise 8.3.6a Prove that the quotient ring $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

Exercise 8.3.6b Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \bmod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

Exercise 9.1.6 Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.

Exercise 9.1.10 Prove that the ring $\mathbb{Z}\left[x_1, x_2, x_3, \ldots\right] / \left(x_1 x_2, x_3 x_4, x_5 x_6, \ldots\right)$ contains infinitely many minimal prime ideals (cf. exercise.9.1.36 of Section 7.4).

Exercise 9.3.2 Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.

Exercise 9.4.2a Prove that $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.2b Prove that $x^6 + 30x^5 - 15x^+ 6x - 120$ is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.2c Prove that $x^4 + 4x^3 + 6x^2 + 2x + 1$ is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.2d Prove that $\frac{(x+2)^p - 2^p}{x}$, where p is an odd prime, is irreducible in $\mathbb{Z}[x]$.

Exercise 9.4.9 Prove that the polynomial $x^2 - \sqrt{2}$ is irreducible over $\mathbb{Z}[\sqrt{2}]$. You may assume that $\mathbb{Z}[\sqrt{2}]$ is a U.F.D.

Exercise 9.4.11 Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

Exercise 11.1.13 Prove that as vector spaces over $\mathbb{Q}, \mathbb{R}^n \cong \mathbb{R}$, for all $n \in \mathbb{Z}^+$.

Exercise 11.3.3bi Let S be any subset of V^* for some finite dimensional space V. Define Ann $(S) = \{v \in V \mid f(v) = 0$ for all $f \in S\}$. Let W_1 and W_2 be subspaces of V^*. Prove that $\operatorname{Ann}(W_1 + W_2) = \operatorname{Ann}(W_1) \cap \operatorname{Ann}(W_2)$.

Exercise 11.3.3bii Let S be any subset of V^* for some finite dimensional space V. Define Ann $(S) = \{v \in V \mid f(v) = 0$ for all $f \in S\}$. Let W_1 and W_2 be subspaces of V^*. Prove that $\operatorname{Ann}(W_1 \cap W_2) = \operatorname{Ann}(W_1) + \operatorname{Ann}(W_2)$.

Exercise 11.3.3c Let S be any subset of V^* for some finite dimensional space V. Define Ann $(S) = \{v \in V \mid f(v) = 0$ for all $f \in S\}$. Let W_1 and W_2 be subspaces of V^*. Prove that $W_1 = W_2$ if and only if $\operatorname{Ann}(W_1) = \operatorname{Ann}(W_2)$

Exercise 11.3d Let S be any subset of V^* for some finite dimensional space V. Define Ann $(S) = \{v \in V \mid f(v) = 0 \text{ for all } f \in S\}$. Prove that the annihilator of S is the same as the annihilator of the subspace of V^* spanned by S.

Exercise 11.3f Let S be any subset of V^* for some finite dimensional space V. Define Ann $(S) = \{v \in V \mid f(v) = 0 \text{ for all } f \in S\}$. Assume V is finite dimensional. Prove that if W^* is any subspace of V^* then $\dim \operatorname{Ann}(W^*) = \dim V - \dim W^*$