Exercises from *Abstract Algebra* by I. N. Herstein

Exercise 2.1.18 If G is a finite group of even order, show that there must be an element $a \neq e$ such that $a = a^{-1}$.

Exercise 2.1.21 Show that a group of order 5 must be abelian.

Exercise 2.1.26 If G is a finite group, prove that, given $a \in G$, there is a positive integer n, depending on a, such that $a^n = e$.

Exercise 2.1.27 If G is a finite group, prove that there is an integer $m > 0$ such that $a^m = e$ for all $a \in G$.

Exercise 2.2.3 If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i, prove that G is abelian.

Exercise 2.2.5 Let G be a group in which $(ab)^3 = a^3 b^3$ and $(ab)^5 = a^5 b^5$ for all $a, b \in G$. Show that G is abelian.

Exercise 2.2.6c Let G be a group in which $(ab)^n = a^n b^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that $\left(aba^{-1}b^{-1}\right)^{n(n-1)} = e$.

Exercise 2.3.17 If G is a group and $a, x \in G$, prove that $C\left(x^{-1}ax\right) = x^{-1}C(a)x$

Exercise 2.3.19 If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.

Exercise 2.3.16 If a group G has no proper subgroups, prove that G is cyclic of order p, where p is a prime number.

Exercise 2.3.21 If A, B are subgroups of G such that $b^{-1}Ab \subset A$ for all $b \in B$, show that AB is a subgroup of G.

Exercise 2.3.22 If A and B are finite subgroups, of orders m and n, respectively, of the abelian group G, prove that AB is a subgroup of order mn if m and n are relatively prime.

Exercise 2.3.28 Let M, N be subgroups of G such that $x^{-1}Mx \subset M$ and $x^{-1}Nx \subset N$ for all $x \in G$. Prove that MN is a subgroup of G and that $x^{-1}(MN)x \subset MN$ for all $x \in G$.

Exercise 2.3.29 If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.

Exercise 2.4.8 If every right coset of H in G is a left coset of H in G, prove that $aHa^{-1} = H$ for all $a \in G$.

Exercise 2.4.26 Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a 1-1 mapping of S onto T.

Exercise 2.4.32 Let G be a finite group, H a subgroup of G. Let $f(a)$ be the least positive m such that $a^m \in H$. Prove that $f(a) \mid o(a)$, where $o(a)$ is an order of a.

Exercise 2.4.36 If $a > 1$ is an integer, show that $n \mid \varphi(a^n - 1)$, where ϕ is the Euler φ-function.

Exercise 2.5.23 Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.

Exercise 2.5.30 Suppose that $|G| = pm$, where $p \nmid m$ and p is a prime. If H is a normal subgroup of order p in G, prove that H is characteristic.

Exercise 2.5.31 Suppose that G is an abelian group of order $p^n m$ where $p \nmid m$ is a prime. If H is a subgroup of G of order p^n, prove that H is a characteristic subgroup of G.

Exercise 2.5.37 If G is a nonabelian group of order 6, prove that $G \simeq S_3$.

Exercise 2.5.43 Prove that a group of order 9 must be abelian.

Exercise 2.5.44 Prove that a group of order p^2, p a prime, has a normal subgroup of order p.

Exercise 2.5.52 Let G be a finite group and φ an automorphism of G such that $\varphi(x) = x^{-1}$ for more than three-fourths of the elements of G. Prove that $\varphi(y) = y^{-1}$ for all $y \in G$, and so G is abelian.

Exercise 2.6.15 If G is an abelian group and if G has an element of order m and one of order n, where m and n are relatively prime, prove that G has an element of order mn.

Exercise 2.7.3 Let G be the group of nonzero real numbers under multiplication and let $N = \{1, -1\}$. Prove that $G/N \simeq$ positive real numbers under multiplication.

Exercise 2.7.7 If φ is a homomorphism of G onto G' and $N \triangleleft G$, show that $\varphi(N) \triangleleft G'$.

Exercise 2.8.7 If G is a group with subgroups A, B of orders m, n, respectively, where m and n are relatively prime, prove that the subset of G, $AB = \{ab \mid a \in A, b \in B\}$, has mn distinct elements.

Exercise 2.8.12 Prove that any two nonabelian groups of order 21 are isomorphic.

Exercise 2.8.15 Prove that if $p > q$ are two primes such that $q \mid p - 1$, then any two nonabelian groups of order pq are isomorphic.

Exercise 2.9.2 If G_1 and G_2 are cyclic groups of orders m and n, respectively, prove that $G_1 \times G_2$ is cyclic if and only if m and n are relatively prime.

Exercise 2.10.1 Let A be a normal subgroup of a group G, and suppose that $b \in G$ is an element of prime order p, and that $b \notin A$. Show that $A \cap (b) = (e)$.

Exercise 2.11.6 If P is a p-Sylow subgroup of G and $P \triangleleft G$, prove that P is the only p-Sylow subgroup of G.

Exercise 2.11.7 If $P \triangleleft G$, P a p-Sylow subgroup of G, prove that $\varphi(P) = P$ for every automorphism φ of G.

Exercise 2.11.22 Show that any subgroup of order p^{n-1} in a group G of order p^n is normal in G.

Exercise 3.2.21 If σ, τ are two permutations that disturb no common element and $\sigma\tau = e$, prove that $\sigma = \tau = e$.

Exercise 3.2.23 Let σ, τ be two permutations such that they both have decompositions into disjoint cycles of cycles of lengths $m_1, m_2, \ldots, m_k$. Prove that for some permutation $\beta, \tau = \beta\sigma\beta^{-1}$.

Exercise 3.3.2 If σ is a k-cycle, show that σ is an odd permutation if k is even, and is an even permutation if k is odd.

Exercise 3.3.9 If $n \geq 5$ and $(e) \neq N \subset A_n$ is a normal subgroup of A_n, show that N must contain a 3-cycle.

Exercise 4.1.19 Show that there is an infinite number of solutions to $x^2 = -1$ in the quaternions.

Exercise 4.1.28 Show that $\{x \in R \mid \det x \neq O\}$ forms a group, G, under matrix multiplication and that $N = \{x \in R \mid \det x = 1\}$ is a normal subgroup of G.

Exercise 4.1.29 If $x \in R$ is a zero-divisor, show that $\det x = 0$, and, conversely, if $x \neq 0$ is such that $\det x = 0$, then x is a zero-divisor in R.

Exercise 4.1.34 Let T be the group of matrices A with entries in the field $\mathbb{Z}_2$ such that $\det A$ is not equal to 0. Prove that T is isomorphic to S_3, the symmetric group of degree 3.

Exercise 4.2.5 Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is commutative.

Exercise 4.2.6 If $a^2 = 0$ in R, show that $ax + xa$ commutes with a.

Exercise 4.2.9 Let p be an odd prime and let $1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b}$, where a, b are integers. Show that $p \mid a$.

Exercise 4.3.1 If R is a commutative ring and $a \in R$, let $L(a) = \{x \in R \mid xa = 0\}$. Prove that $L(a)$ is an ideal of R.

Exercise 4.3.4 If I, J are ideals of R, define $I+J$ by $I+J = i + j \mid i \in I, j \in J$. Prove that $I + J$ is an ideal of R.

Exercise 4.3.25 Let R be the ring of 2×2 matrices over the real numbers; suppose that I is an ideal of R. Show that $I = (0)$ or $I = R$.

Exercise 4.4.9 Show that $(p-1)/2$ of the numbers $1, 2, \ldots, p-1$ are quadratic residues and $(p-1)/2$ are quadratic nonresidues $\mod p$.

Exercise 4.5.12 If $F \subset K$ are two fields and $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$, show that they are relatively prime in $K[x]$.

Exercise 4.5.16 Let $F = \mathbb{Z}_p$ be the field of integers $\mod p$, where p is a prime, and let $q(x) \in F[x]$ be irreducible of degree n. Show that $F[x]/(q(x))$ is a field having at exactly p^n elements.

Exercise 4.5.23 Let $F = \mathbb{Z}_7$ and let $p(x) = x^3 - 2$ and $q(x) = x^3 + 2$ be in $F[x]$. Show that $p(x)$ and $q(x)$ are irreducible in $F[x]$ and that the fields $F[x]/(p(x))$ and $F[x]/(q(x))$ are isomorphic.

Exercise 4.5.25 If p is a prime, show that $q(x) = 1 + x + x^2 + \cdots x^{p-1}$ is irreducible in $Q[x]$.

Exercise 4.6.2 Prove that $f(x) = x^3 + 3x + 2$ is irreducible in $Q[x]$.

Exercise 4.6.3 Show that there is an infinite number of integers a such that $f(x) = x^7 + 15x^2 - 30x + a$ is irreducible in $Q[x]$.

Exercise 5.1.8 If F is a field of characteristic $p \neq 0$, show that $(a + b)^m = a^m + b^m$, where $m = p^n$, for all $a, b \in F$ and any positive integer n.

Exercise 5.2.20 Let V be a vector space over an infinite field F. Show that V cannot be the set-theoretic union of a finite number of proper subspaces of V.

Exercise 5.3.7 If $a \in K$ is such that a^2 is algebraic over the subfield F of K, show that a is algebraic over F.

Exercise 5.3.10 Prove that $\cos 1^\circ$ is algebraic over $\mathbb{Q}$.

Exercise 5.4.3 If $a \in C$ is such that $p(a) = 0$, where $p(x) = x^5 + \sqrt{2}x^3 + \sqrt{5}x^2 + \sqrt{7}x + \sqrt{11}$, show that a is algebraic over $\mathbb{Q}$ of degree at most 80.

Exercise 5.5.2 Prove that $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

Exercise 5.6.3 Let $\mathbb{Q}$ be the rational field and let $p(x) = x^4 + x^3 + x^2 + x + 1$. Show that there is an extension K of Q with $[K : Q] = 4$ over which $p(x)$ splits into linear factors.

Exercise 5.6.14 If F is of characteristic $p \neq 0$, show that all the roots of $x^m - x$, where $m = p^n$, are distinct.