Modern Algebra Preliminary Exam
Practice Problems

Department of Mathematics
University of Houston

The purpose of this list of problems is to help students practice for the Modern Algebra prelim. Some of the actual prelim problems may be entirely different from those on this list, and they will depend on the particular instructor who writes the exam. Therefore, students planning to take the exam should either take the prelim course for the corresponding year, or speak with the instructor to clarify which specific topics will and will not be covered.

Problem 1: Let p be a prime number. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Also, show by an explicit example that this need not be the case if p is not a prime.

Problem 2:

(a) Show that if $n \geq m$, then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-2)\dots(n-m+1)}{m}.$$

(b) Find all numbers n such that S_7 contains an element of order n.

Problem 3: Show that if $n \geq 4$, then the number of permutations in S_n which are the product of two disjoint 2-cycles is

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

Problem 4: Prove that S_4 does not contain a subgroup isomorphic to Q_8.

Problem 5: Let H be a subgroup of order 2 in G.

(a) Show that $\mathrm{N}_G(H) = \mathrm{C}_G(H)$

(b) If $\mathrm{N}_G(H) = G$, then show that $H \leqslant \mathrm{Z}(G)$

(c) Prove that A_5 cannot have a normal subgroup of order 2.

Problem 6: Consider

$$H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : \ a, b, c \in F \right\}$$

Then $H(F)$ is a group of order $|F|^3$ under matrix multiplication, called Heisenberg Group over F.

(a) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(b) Prove that every non-identity element of the group $H(\mathbb{R})$ has infinite order.

(c) Find the center $\mathrm{Z}(H(F))$ of group $H(F)$ and prove that $\mathrm{Z}(H(F))$ is isomorphic to the group $(H, +)$.

Problem 7: If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Show by an explicit example that this may not be true if ϕ is only assumed to be a homomorphism.

Problem 8: Let $G = \{z \in \mathbb{C} \colon z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$, the map from G to itself defined by $z \mapsto z^k$, is a surjective homomorphism. Also show that it is not an isomorphism.

Problem 9: Let p be a prime and $G = \mathbb{Z}_p \times \mathbb{Z}_p$. Determine the order of $\mathrm{Aut}(G)$, the group of automorphisms of G.

Problem 10: Let A be a non-empty set, let k be a positive integer with $k \leq |A|$, and let B be the set of all subsets of A with cardinality k. The symmetric group S_A acts on B by

$$\sigma.\{a_1, a_2, ..., a_k\} = \{\sigma(a_1), \sigma(a_2), ..., \sigma(a_k)\}.$$

(a) Prove that this is a group action.

(b) Describe explicitly how the elements (1 2) and (1 2 3) act on the six $2-$element subsets of $\{1, 2, 3, 4\}$.

Problem 11: Let H be a subset of group G.

(a) Show if H is non-empty, finite and closed under multiplication then it satisfies the subgroup criterion.

(b) Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

Problem 12:

(a) Let G be an Abelian group. Prove that $\{g \in G : \ |g| < \infty\}$ is a subgroup of G.

(b) Show by an explicit example that this may not be true if G is not Abelian.

(c) Find an example of a group G for which the subset of elements of infinite order together with the identity is not a subgroup of G.

Problem 13: Give an example of a group G and an integer $n \in \mathbb{Z}$ for which $\{g \in G \colon g^n = 1\}$ is not a subgroup of G.

Problem 14: Let H be a subgroup of a group G. Show that

(a) $H \leq \mathrm{N}_G(H)$. Also give an example to show that this is not necessarily true if H is not a subgroup of G.

(b) $H \leq \mathrm{C}_G(H)$ if and only if H is Abelian.

Problem 15: Let G and H be groups and $\phi \colon G \to H$ be a homomorphism. Let E be a subgroup of H. Prove that $\phi^{-1}(E) \leqslant G$. Additionally, if $E \trianglelefteq H$, prove that $\phi^{-1}(E) \trianglelefteq G$. Deduce that $\mathrm{Ker}(\phi) \trianglelefteq G$.

Problem 16: Calculate the number of Abelian groups of order 2000, up to isomorphism.

Problem 17: Construct 2 non-isomorphic groups of order 21.

Problem 18: Construct two non-isomorphic, non-Abelian groups of order 27. Prove that they are non-Abelian and non-isomorphic to one another.

Problem 19: Let G be a finite group with $|G| = 2024$. Prove that there exists $a \in G$ such that $a \neq e$ and $a * a = e$.

Problem 20: Let G be a finite group and suppose that H and K are subgroups of G such that $\gcd(|H|, |K|) = 1$. Prove that $H \cap K = \{e\}$.

Problem 21: Let $m, n \in \mathbb{N}$. Prove that the group $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic iff $\gcd(m, n) = 1$.

Problem 22: Let G and K be groups and $\phi : G \to K$ a homomorphism. Prove that for every $a \in G$, if a has finite order, then $\phi(a)$ has finite order and $o(\phi(a)) \,|\, o(a)$.

Problem 23: Let G and K be groups and $\phi : G \to K$ a homomorphism. Prove that ϕ is injective if and only if $o(\phi(a)) = o(a)$ for every $a \in G$.

Problem 24: Prove that $\{(1, 2), (1, 2, \cdots, n)\}$ is a generating set for S_n.

Problem 25: Prove that the center of S_n is trivial for every $n \geq 3$.

Problem 26: Prove that the map $\phi : S_n \to \mathbb{Z}_2$ defined by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases}$$

is a homomorphism.

Problem 27: Let G be a finite group with $|G| = n$. Let S be a subset of G with $|S| > \frac{n}{2}$. Prove that $G = \{ab : a, b \in S\}$.

Problem 28: Prove that any subgroup of a cyclic group is cyclic.

Problem 29: For a given set A, denote by S_A the group of all bijective functions from A to A with the composition as the binary operation. Prove that for any sets A and B, if $|A| = |B|$, then $S_A \cong S_B$.

Problem 30: Prove that $\mathbb{R}$ is not finitely generated.

Problem 31: Prove that $\mathbb{Q}$ is not finitely generated.

Problem 32: Let $H \leqslant G$. On the left coset space G/H define the operation

$$aH * bH = abH.$$

Prove that $*$ is a well-defined binary operation if and only if H is normal in G.

Problem 33: Given two subsets $A, B \subseteq G$, denote $A \bullet B = \{ab : a \in A \text{ and } b \in B\}$. Let $H \leqslant G$. Prove that H is normal in G iff for every $x, y \in G$, the set $xH \bullet yH$ is a left coset of H in G.

Problem 34: Let $H \leqslant G$, and let $*$ and $\bullet$ be the operations as defined above. Prove that H is normal in G iff for every $x, y \in G$

$$xH * yH = xH \bullet yH.$$

Problem 35: Suppose that S is a non-empty subset of G such that $aSa^{-1} \subset S$ for all $a \in G$. Prove that $\langle S \rangle$ is normal in G.

Problem 36: Let G' be the subgroup generated by the set $\{aba^{-1}b^{-1} : a, b \in G\}$. Prove that

(a) $G' \trianglelefteq G$.

(b) The quotient group G/G' is Abelian.

(c) If $H \trianglelefteq G$ is such that G/H is Abelian, then $G' \subseteq H$.

Problem 37: A subgroup $H \leq G$ is said to be a *characteristic subgroup* of G if $\alpha(H) \subseteq H$ for all $\alpha \in \mathrm{Aut}(G)$. Prove that

(a) Every characteristic subgroup of G in normal in G.

(b) $Z(G)$ and G' are characteristic subgroups of G.

(c) If $H \trianglelefteq G$ and K is a characteristic subgroup of H, then $K \trianglelefteq G$.

Problem 38: Let $H \trianglelefteq G$ and let $\alpha \in \mathrm{Aut}(G)$ be such that $\alpha(H) \subset H$. Prove that there exists $\beta \in \mathrm{Aut}(G/H)$ such that $\pi \circ \alpha = \beta \circ \pi$, where $\pi : G \to G/H$ is the canonical quotient map.

Problem 39: Let G and K be groups and $\psi : G \to K$ a homomorphism. Prove or disprove the following statements.

(a) If $H \trianglelefteq G$, then $\psi(H) \trianglelefteq K$.

(b) If $L \trianglelefteq K$, then $\psi^{-1}(L) \trianglelefteq G$.

Problem 40: Prove that every finitely generated Abelian group is a quotient of $\mathbb{Z}^n$ for some $n \in \mathbb{N}$.

Problem 41: For the given group G and the generating set S for G in each of the following parts, find the cardinality of the set $B_S(n) = \{g \in G : |g|_S \leq n\}$, where

$$|g|_S := \min\{n \in \mathbb{N} : \exists s_1, s_2, \ldots, s_n \in S \text{ such that } g = s_1 s_2 \cdots s_n\},$$

is the word length of g with respect to the generating set S.

(a) $G = \mathbb{Z}$ and $S = \{-1, 1\}$

(b) $G = \mathbb{Z}$ and $S = \{-2, -1, 1, 2\}$

(c) $G = \mathbb{Z} \times \mathbb{Z}$ and $S = \{(1, 0), (0, 1), (-1, 0), (0, -1)\}$

(d) $G = F_2 = \langle a, b \rangle$ and $S = \{a^{-1}, a, b, b^{-1}\}$

Definitions for Problems 42 and 43: An action of a group G on a set X is said to be

(i) *faithful* if for every non-trivial $g \in G$, there exists $x \in X$ such that $gx \neq x$.

(ii) *free* if for every non-trivial $g \in G$ and every $x \in X$ we have $gx \neq x$.

Problem 42: Let G be a group and H a subgroup of G. For each of the following actions, determine whether the action is faithful, free, both or neither.

(a) The action of G on G by left multiplication.

(b) The action of G on G by conjugation.

(c) The action of G on G/H by left multiplication.

(d) The action of G on the set X of all subgroups of G by conjugation.

Problem 43: For each of the following actions, determine whether the action is faithful or not.

(a) The canonical action of S_n on $\{1, 2, \ldots, n\}$.

(b) The action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$ by matrix multiplication.

(c) The action of $\mathbb{Z}$ on the unit circle S^1, given by rotations $k \cdot x := R_{2\pi k\theta}$, $\forall k \in \mathbb{Z}, x \in S^1$, for a fixed $0 < \theta < 1$.

(d) The action of $\mathrm{GL}_2(\mathbb{R})$ on the the set X of all lines in $\mathbb{R}^2$ passing through the origin.

Problem 44: Prove that an action of the group G on a set X is transitive if and only if it is conjugate to the canonical action of G on the coset space G/H for some subgroup $H \leq G$.

Problem 45: Let G be a group, and let $x \in G$. Consider the action of G on G by conjugation. What is the stabilizer subgroup G_x.

Problem 46: Let G be a group, H a subgroup of G, and $x \in G$. Consider the action G on G/H by left multiplication. What are the stabilizer subgroup and the orbit of the point $xH \in G/H$.

Problem 47: Consider the action of $\mathbb{Z}$ on S^1 as in part (c) of Problem 43 above, in the case $\theta = \frac{3}{8}$. For an arbitrary point $x \in S^1$, find the stabilizer subgroup and the orbit of x.

Problem 48: Let G be a group.

(a) Denote $\mathrm{Inn}(G) := \{\phi_g : g \in G\}$ for the set of all inner automorphisms of G. Prove that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

(b) Prove that the map $\Phi : G \to \mathrm{Inn}(G)$ defined by $\Phi(g) = \phi_g$ is a (surjective) group homomorphism, and find the kernel of Φ.

Problem 49: Prove or disprove: If $K \trianglelefteq H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$.

Problem 50: Let G be a group and let G' be the subgroup generated by the set $\{aba^{-1}b^{-1} : a, b \in G\}$. Prove that

(a) $G' \trianglelefteq G$.

(b) The quotient group G/G' is Abelian.

(c) If $H \trianglelefteq G$ is such that G/H is Abelian, then $G' \subseteq H$.

Problem 51: A subgroup $H \leqslant G$ is said to be a *characteristic subgroup* of G if $\alpha(H) \subseteq H$ for all $\alpha \in \mathrm{Aut}(G)$. Prove that

(a) Every characteristic subgroup of G in normal in G.

(b) $Z(G)$ and G' are characteristic subgroups of G.

(c) If $H \trianglelefteq G$ and K is a characteristic subgroup of H, then $K \trianglelefteq G$.

Problem 52: Let H and K be normal subgroups of G and $H \leqslant K$. Show that K/H is a normal subgroup of G/H, and $G/K \cong (G/H)/(K/H)$.

Problem 53: Prove that every finitely generated Abelian group is a quotient of $\mathbb{Z}^n$ for some $n \in \mathbb{N}$.

Problem 54: Let G and K be groups and $\phi : G \to K$ a homomorphism. Prove that for every $a \in G$, if a has finite order, then $\phi(a)$ has finite order and $o(\phi(a)) \,|\, o(a)$.

Problem 55: Let $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $K = \mathrm{Aut}(H)$, and let $\varphi : K \to K$ be the identity map, $\varphi(k) = k$ for all $k \in K$. Prove that $H \rtimes_\varphi K \cong S_4$.

Problem 56: The group $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ can be written using generators and relations as

$$G = \langle x, y \mid x^4 = y^4 = 1, xy = yx \rangle.$$

Given this presentation, let $\overline{G} = G/\langle x^2 y^2 \rangle$.

(a) Show that $|\overline{G}| = 8$.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{x}^a \overline{y}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Prove that $\overline{G} \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

Problem 57: Let N be a finite subgroup of a group G.

(a) Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$

(b) Show that $N_G(N) = \{g \in G \colon gNg^{-1} \subseteq N\}$

(c) Show by an example that (b) need not be true if N is not finite.

Problem 58: Let A be an Abelian group and let D be the diagonal subgroup

$$D = \{(a, a) | a \in A\} \leqslant A \times A.$$

(a) Prove that $D \trianglelefteq A \times A$ and $\frac{A \times A}{D} \cong A$.

(b) Prove that this result is still be true for all non-Abelian groups A, or give a counterexample to show that it is not.

Problem 59:

(a) Let p be a prime number, let G be a finite Abelian group, and let H be a subgroup of G. Prove that H has index p in G if and only if it is the kernel of surjective homomorphism

$$\varphi : G \to \mathbb{Z}/p\mathbb{Z}.$$

(b) Give an example to show that the conclusion of (a) is not true in general if G is not assumed to be Abelian.

(c) Using part (a), calculate the number of subgroups of index 5 in the group

$$G = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Problem 60: Let F be a field of order q and let $n \in \mathbb{N}$. Use the First Isomorphism Theorem to prove that

$$|\mathrm{GL}_n(F) : \mathrm{SL}_n(F)| = q - 1.$$

Problem 61: Prove that $\mathrm{Z}(\mathrm{SL}_2(\mathbb{F}_3)) = \{\pm I\}$, and that

$$\mathrm{SL}_2(\mathbb{F}_3)/\mathrm{Z}(\mathrm{SL}_2(\mathbb{F}_3)) \cong A_4.$$

Problem 62: Suppose that M and N are normal subgroups of G and that $G = MN$. Prove that

$$G/(M \cap N) \cong G/M \times G/N.$$

Problem 63: Suppose that A is a finite Abelian group, that p is a prime number, and that $\varphi : A \to A$ is the map defined by $\varphi(a) = a^p$. If $H, K \leqslant G$ are defined by

$$H = \varphi(A) \quad \text{and} \quad K = \ker(\varphi),$$

prove that $A/H \cong K$.

Problem 64: Prove that if G is a group then the index $|G : \mathrm{Z}(G)|$ is not a prime number.

Problem 65: Let p be an odd prime number. Recall that, for $k \in \mathbb{N}$, an integer g is called a *primitive root modulo* p^k if

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times = \langle g \rangle.$$

Suppose that g is a primitive root modulo p. Prove that g or $g + p$ is a primitive root modulo p^k, for all $k \in \mathbb{N}$.

Problem 66: Let $N = 6! = 720$. Calculate the number of elements of order 2 in $(\mathbb{Z}/N\mathbb{Z})^\times$, the multiplicative group of invertible residue classes modulo N.

Problem 67: Let p be an odd prime number and let $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ be defined by

$$\varphi(a) = \begin{cases} 1 & \text{if } a = b^2 \text{ for some } b \in (\mathbb{Z}/p\mathbb{Z})^\times, \\ -1 & \text{otherwise.} \end{cases}$$

(a) Prove that φ is a homomorphism.

(b) Prove the $-1 \in \ker(\varphi)$ if and only if $p = 1 \bmod 4$.

Problem 68: The *exponent* of a group G is defined to be the smallest positive integer $n \in \mathbb{N}$ with the property that, for all $g \in G$ $g^n = e$, or ∞ if no such n exists.

(a) Prove that any finite group has finite exponent.

(b) Give an example of an infinite group with finite exponent.

(c) Prove of disprove the following statement: A finite group of exponent n always contains an element of order n.

Problem 69: Let p be an odd prime and let P be a p-group.

(a) Prove that if every subgroup of P is normal then P is Abelian.

(b) Give an example to show that the result in (a) is not true for $p = 2$.

Problem 70: Let G be a non-trivial finite group and p a prime. Suppose that every subgroup $H \neq G$ has index divisible by p. Prove that the center of G has order divisible by p.

Problem 71: Let p be a prime and n a positive integer with $n < p^2$. Find (with proof) a Sylow p-subgroup of the symmetric group S_n.

Problem 72: Let $\mathbb{F}$ be a field and let $\mathbb{F}^\times$ denote the group of non-zero elements of $\mathbb{F}$. Show that every finite subgroup of $\mathbb{F}^\times$ is cyclic.

Problem 73: Let x be a nilpotent element of the commutative ring R.

(a) Prove that x is either zero or zero-divisor.

(b) Prove that rx is nilpotent for all $r \in R$.

(c) Prove that $1 + x$ is a unit in R.

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

Problem 74: A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$.

(a) Let X be a non-empty set and let $P(X)$ be the set of all subsets of X (the power set of X). Define addition and multiplication on $P(X)$ by

$A + B = (A - B) \cup (B - A)$ and $A \times B = A \cap B$. Show that $P(X)$ is a Boolean ring with an identity.

(b) Prove that every Boolean ring is commutative.

(c) Prove that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$.

Problem 75: Let R and S be non-zero rings with identity and denote their respective identities by 1_R and 1_S. Let $\phi : R \to S$ be a non-zero homomorphism of rings.

(a) Prove that if S is an integral domain then $\phi(1_R) = 1_S$.

(b) Show by an example that (a) need not be true if S is not an integral domain.

(c) Prove that if $\phi(1_R) \neq 1_S$, then $\phi(1_R)$ is a zero divisor in S.

(d) Prove that if $\phi(1_R) = 1_S$, then $\phi(u)$ is a unit in S and $\phi(u^{-1}) = \phi(u)^{-1}$ for each unit u of R.

Problem 76:

(a) Let I be an ideal of R and let S be a subring of R. Prove that $I \cap S$ is an ideal of S.

(b) Show by an example that not every ideal of a subring S of a ring R need be of the form $I \cap S$ for some ideal I of R.

Problem 77: Assume R is a commutative ring. Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be an element of the polynomial ring $R[x]$.

(a) Prove that $P(x)$ is a unit in $R[x]$ iff a_0 is a unit and $a_1, a_2, ..., a_n$ are nilpotent in R.

(b) Prove that $P(x)$ is nilpotent in $R[x]$ iff $a_0, a_1, ..., a_n$ are nilpotent elements of R.

Problem 78: Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

(b) Prove that IJ is the ideal contained in $I \cap J$.

(c) Give an example where $IJ \neq I \cap J$.

(d) Prove that if R is commutative and if $I + J = R$, then $IJ = I \cap J$.

Problem 79: Let $\phi : R \to S$ be a homomorphism of commutative rings.

(a) Prove that if P is a prime ideal of S then either $\phi^{-1}(P) = R$ or $\phi^{-1}(P)$ is a prime ideal of R.

(b) Prove that if M is a maximal ideal of S and ϕ is surjective then $\phi^{-1}(M)$ is a maximal ideal of R.

(c) Give an example to show that (b) need not be true if ϕ is not surjective.

Problem 80: Let $R = C([0,1])$ be the ring of continuous real valued functions on the interval $[0,1]$. Prove that the set $A_{1/2} = \{f \in R : f(1/2) = 0\}$ is an ideal in R, and that the quotient ring $R/A_{1/2}$ is ring isomorphic to $\mathbb{R}$.

Problem 81: Let R be the rings of all continuous functions on $\mathbb{R}$. For each $c \in \mathbb{R}$, let M_c be the maximal ideal $\{f \in R : \ f(c) = 0\}$.

(a) Let I be the collection of functions $f(x)$ in R with compact support. Prove that I is an ideal of R that is not a prime ideal.

(b) Let M be a maximal ideal of R containing I (properly). Prove that $M \neq M_c$ for any $c \in \mathbb{R}$.

Problem 82: Let R be a ring with identity $1 \neq 0$. Assume a is an idempotent in R (i.e. that $a^2 = a$), and that $ar = ra$ for all $r \in R$.

(a) Prove that Ra and $R(1-a)$ are two sided ideals of R and that

$$R \cong Ra \times R(1-a).$$

(b) If R is a finite Boolean ring, prove that

$$R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}.$$

Problem 83: Let $R = \mathbb{Z}[\sqrt{-n}]$, where n is a squarefree integer greater than 3.

(a) Prove that 2, $\sqrt{-n}$, and $1 + \sqrt{-n}$ are irreducible elements in R.

(b) Prove that R is not a UFD.

(c) Give an explicit ideal in R that is not principal.

Problem 84: Let R be a commutative ring. Prove that if R contains a prime ideal P with no zero divisors, then R is an integral domain.

Problem 85: Let R be an integral domain with quotient field F and let $p(x)$ be monic polynomial in $R[x]$. Assume that

$$p(x) = a(x)b(x),$$

where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of degree smaller than that of $p(x)$.

(a) Prove that if $a(x) \notin R[x]$ then R is not a UFD.

(b) Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

Problem 86: Let R be the subring of $\mathbb{C}$ defined by

$$R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\},$$

and let $I \subseteq R$ be the principal ideal $I = (1 + \sqrt{-5})$.

(a) Find a complete set of distinct representatives for the quotient ring R/I.

(b) Prove that I is not a prime ideal.

Problem 87: Let R be the subring of $\mathbb{R}$ defined by

$$R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\},$$

and let $I \subseteq R$ be the principal ideal $I = (3)$.

(a) Prove that R/I is a field, and compute its cardinality.

(b) Find a generator for the multiplicative group $(R/I)^\times$.

Problem 88: Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$.

(a) Prove that $F[x]/(f(x))$ has q^n elements.

(b) Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

(c) Use the above results to explicitly construct a field of order 49.

(d) Prove that the multiplicative group of the field constructed in part (c) is cyclic, by explicitly demonstrating a generator for the group.

Problem 89: Find all commutative rings R with 1 such that R has a unique maximal ideal and such that the only units of R are 1 and -1.

Problem 90: Prove that an ideal I of a commutative ring R is prime if and only if R/I is an integral domain.

Problem 91: Prove that if R is a PID then every non-zero prime ideal in R is maximal.

Problem 92: Prove that $R[x]$ is a PID if and only if R is a field.

Problem 93: Prove that $\mathbb{Z}[\sqrt{-3}]$ is an integral domain but not a unique factorization domain.

Problem 94: A proper ideal P of a commutative ring R is prime if $ab \in P$ implies that either $a \in P$ or $b \in P$. Prove that every nonzero prime ideal in a principal ideal domain is maximal.

Problem 95: Suppose that R is a subring of a commutative ring S and that R is of finite index n in S. Let m be an integer that is relatively prime to n. Prove that the natural map $R/mR \to S/mS$ is a ring isomorphism.

Problem 96: Let $R = \mathbb{Q}[x, y]$ be the ring of polynomials in two variables with rational coefficients.

(a) Give an example of a maximal ideal of R that is proper (i.e. $\neq \{0\}, \neq R$), or prove that no such ideal exists.

(b) Give an example of a principal ideal of R that is proper (i.e. $\neq \{0\}, \neq R$), or prove that no such ideal exists.

Problem 97: Two elements in an arbitrary ring are called *relatively prime* if the only elements dividing both are units. Let A and B be principal ideal domains such that $A \subseteq B$. Suppose that p and q are relatively prime elements in A. Show that p and q are also relatively prime in B.

Problem 98: Let R be an integral domain.

(a) Show that a polynomial of degree d in $R[x]$ has at most d roots.

(b) Give an example to show that this is not true in general if R is not assumed to be an integral domain.

Problem 99: Suppose that $N \geq 3$ is an odd number with $N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1 < \cdots < p_k$ are prime numbers and $a_1, \ldots, a_k \in \mathbb{N}$. Compute the number of solutions $x \bmod N$ to the equation

$$x^3 - 3x^2 + 2x = 0 \bmod N.$$

Problem 100:

(a) Let p be a prime number with $p = 1 \bmod 4$. Prove that there are exactly two solutions to the equation $x^2 = -1 \bmod p$. You may use the fact that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

(b) Suppose that $N = p_1 p_2 \cdots p_k$, where $p_1 < \cdots < p_k$ are prime numbers satisfying $p_i = 1 \bmod 4$ for each $1 \leq i \leq k$. Calculate the number of elements of order 4 in $(\mathbb{Z}/N\mathbb{Z})^\times$.

Problem 101: Show that $p(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Problem 102: Consider $f(x) = x^5 - ax - 1 \in \mathbb{Z}[x]$. Find the values of $a \in \mathbb{Z}$ so that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Problem 103:

(a) Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) Determine the degree of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

(c) Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

Problem 104: Let p be a prime

(a) Determine the elements of the Galois group of $x^p - 2$.

(b) Determine all the subfields of the splitting field of $x^p - 2$.

(c) Prove that the Galois group of $x^p - 2$ is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$, $a \neq 0$.

Problem 105:

(a) Prove that $f(x) = x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.

(b) Show that there are roots α_1, α_2 of $f(x)$ such that if $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Then $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.

(c) Prove that the splitting field of $f(x)$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

Problem 106: Let $\mathbb{F}_9$ be finite field with 9 elements. Let $\sigma_9 = (\sigma_3)^2$, where σ_3 is the Frobenius automorphism $x \to x^3$.

(a) Prove that σ_9 fixes $\mathbb{F}_9$.

(b) Prove that every finite extension of $\mathbb{F}_9$ of degree n is the splitting field of $x^{9^n} - x$ over $\mathbb{F}_9$, hence is unique.

(c) Prove that every finite extension of $\mathbb{F}_9$ of degree n is cyclic with σ_9 as the generator.

(d) Prove that the subfields of the unique extension of $\mathbb{F}_9$ of degree n are in bijective correspondence with the divisors d of n.

Problem 107: Prove that if K/F is a finite extension of fields then K/F is algebraic. Show that the converse is not true, in general.

Problem 108: Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Find an element $\alpha \in K$ for which $K = \mathbb{Q}(\alpha)$.

Problem 109: Give an example of a degree 4 extension of $\mathbb{Q}$ with exactly 2 distinct embeddings into $\mathbb{R}$.

Problem 110: Suppose L/K is a finite, separable, field extension with $[L : K] = n$, and let $\sigma_1, \ldots, \sigma_n$ be the distinct embeddings of L into $\overline{K}$ which fix K. Prove that if $\alpha \in L$ and $\sigma_i(\alpha) = \alpha$ for all $1 \leq i \leq n$, then $\alpha \in K$.

Problem 111: Let p be a prime and let F be a field. Let K be a Galois extension of F whose Galois group is a p-group (i.e. the degree $[K : F]$ is a power of p). Such an extension is called a p-extension.

(a) Let L be a p-extension of K. Prove that the Galois closure of L over F is a p-extension of F.

(b) Give an example to show that (a) need not hold if $[K : F]$ is a power of p but K/F is not Galois.

Problem 112: Let K be the splitting field over $\mathbb{Q}$ of the polynomial $x^4 - 2$. Determine the Galois group of $K/\mathbb{Q}$ and explicitly compute all intermediate fields of the extension. Which of the intermediate fields are Galois over $\mathbb{Q}$?

Problem 113: For $n \in \mathbb{N}$ let $\xi_n = e^{2\pi i/n} \in \mathbb{C}$. Prove that $\mathbb{Q}(\xi_n)$ is a Galois extension of $\mathbb{Q}$ and that

$$\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

Problem 114: Suppose that K/F is an extension of *finite fields*, and let $\sigma_{K/F} : K \to K$ be the map defined by

$$\sigma_{K/F}(x) = x^{|F|}.$$

(a) Prove that $\sigma_{K/F}$ is a non-zero field homomorphism, and deduce from this that it is a bijection.

(b) Prove that $\sigma_{K/F} \in \mathrm{Aut}(K/F)$.

(c) Prove that the order of $\sigma_{K/F}$ in $\mathrm{Aut}(K/F)$ equals $[K : F]$, and conclude that

$$\mathrm{Gal}(K/F) \cong \langle \sigma_{K/F} \rangle.$$

Problem 115: Let p be a prime and let $q = p^{30}$. Compute the lattice of intermediate fields of the extension $\mathbb{F}_q/\mathbb{F}_p$.

Problem 116: Let $\xi_7 \in \mathbb{C}$ be a primitive 7^{th} root of unity.

(a) Compute the lattice of intermediate fields of the extension $\mathbb{Q}(\zeta_7)/\mathbb{Q}$.

(b) Write each intermediate field as a simple extension of $\mathbb{Q}$.

Problem 117: Let $\xi_{13} \in \mathbb{C}$ be a primitive 13^{th} root of unity.

(a) Describe explicitly the subfields of $\mathbb{Q}(\xi_{13})$ in the form of simple extension of $\mathbb{Q}$.

(b) Determine the minimal polynomials satisfied by the primitive generators of subfields in (a).

Problem 118: Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$.

(a) Prove that the Galois closure of F has Galois group either S_4, A_4 or the dihedral group D_8.

(b) Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.

Problem 119:

(a) Determine the Galois group over $\mathbb{Q}$ of the polynomial $x^4 + 8x^2 + 8x + 4$.

(b) Determine which of the subfields of this field are Galois over $\mathbb{Q}$.

(c) For the Galois fields in (b), determine a polynomial $f(x) \in \mathbb{Q}[x]$ for which they are the splitting field over $\mathbb{Q}$.

Problem 120: Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be elements of an extension field K of F, and assume that they are algebraic over F. Prove that $F(\alpha_1, \alpha_2, \ldots, \alpha_k) = F[\alpha_1, \alpha_2, \ldots, \alpha_k]$.

Problem 121:

(a) Find the minimal polynomial of $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$.

(b) Does the field $\mathbb{Q}(\sqrt{2} + \sqrt{5})$ contain any solution to $x^3 - 5$? Prove that your answer is correct.

Problem 122: Compute the Galois group of the polynomial $x^3 - 4x + 2$ over the field of rational numbers $\mathbb{Q}$, and over the field of real numbers $\mathbb{R}$.

Problem 123: Show that the field $\mathbb{Q}[\sqrt{2 + \sqrt{2}}]$ is Galois over $\mathbb{Q}$, and determine its Galois group.

Problem 124: Let K be a field extension of F of degree n and let $f(x) \in F[x]$ be an irreducible polynomial of degree $m > 1$. Show that if m is relatively prime to n, then f has no root in K.