There are 3 areas, each consisting of 4 problems. Each problem is worth 10 points. Best 3 problems out of each area will determine your score.

1. Group Theory

Problem 1.1. How many elements of order 15 are there in $S_8$? Find the centralizer (not just its order) of $(1, 2, 3)(4, 5, 6, 7, 8)$ in $S_8$.

Solution: Any element of order 15 is a product of a 3-cycle and a 5-cycle in $S_8$. There are therefore $m = \binom{8}{3} \cdot 2 \cdot 5! / 5$ such elements.

Since all elements of order 15 are conjugate to $\sigma = (1, 2, 3)(4, 5, 6, 7, 8)$, the orbit of $(1, 2, 3)(4, 5, 6, 7, 8)$ under conjugation has size $m$. The centralizer $C$ of $\sigma$ is the stabilizer of $\sigma$ under conjugation, and it has therefore size $8! / m = 15$.

The subgroup $H$ generated by $\sigma$ is of order 15. Since $\sigma^k \sigma = \sigma \sigma^k$, we see that $H \leq C$, and thus, in fact, $C = H$. □

Problem 1.2. Let $G$ be a non-abelian group of order $p^3$, where $p$ is a prime. Show that $Z(G) = G'$ is a subgroup of order $p$, and that $G/Z(G) = \mathbb{Z}_p \times \mathbb{Z}_p$.

Solution: Fact 1: $p$-groups are nilpotent

Fact 2: nilpotent groups have nontrivial center

Fact 3: If $H$ is a group such that $H/Z(H)$ is cyclic then $H$ is commutative.

Fact 4: In a group $H$, $H'$ is the smallest normal subgroup such that $G/G'$ is abelian.

Since $G$ is nilpotent, it has nontrivial center, i.e., $|Z(G)| = p, p^2, p^3$. But $|Z(G)| = p^3$ implies $Z(G) = G$, a contradiction. Hence $|Z(G)| = p, p^2$. When $|Z(G)| = p^2$ then $|G/Z(G)| = p$ and hence $G/Z(G)$ is cyclic, a contradiction using Fact 3. Thus $|Z(G)| = p$. Then $G/Z(G)$ is of order $p^2$, not cyclic by Fact 3. Thus $G/Z(G)$ is the only other group of order $p^2$, namely $\mathbb{Z}_p \times \mathbb{Z}_p$.

Now, $G/Z(G) = \mathbb{Z}_p \times \mathbb{Z}_p$ is abelian, and hence $G' \leq Z(G)$. This leaves us with $G' = 1$ or $G' = Z(G)$, since $|Z(G)| = p$. But $G' = 1$ implies that $G/G' = G$ is abelian, a contradiction. □

Problem 1.3. Show that every group of order 1995 = 3 · 5 · 7 · 19 is solvable. (Hint: First show that such a group has a normal subgroup of order 19.)

Solution: Denote by $r_p(G)$ the number of Sylow $p$-subgroups of a group $G$.

Let $G$ be the group in question. Since $r_{19}(G) \equiv 1 \pmod{19}$ and $r_{19}(G) \leq 3 \cdot 5 \cdot 7 = 105$, the possibilities are 1, 20, 39, 58, 77, 96. But non of these divides 105, except 1. Hence there is a unique, thus normal Sylow 19-subgroup $H$. Now, $H \cong \mathbb{Z}_{19}$ is solvable, and $K = G/H$ is of order 105. It suffices to show that $K$ is solvable.

By counting, the choices for $r_7(K)$ are 1 or 15, and the choices for $r_5(K)$ are 1 or 21. Assume that $r_7(K) = 15$ and $r_5(K) = 21$. Any two distinct Sylow 7-subgroups intersect trivially (being isomorphic to $\mathbb{Z}_7$), and thus their union covers $15 \cdot (7 - 1) = 90$ elements of order 7. Similarly, the union of all Sylow 5-subgroups covers $21 \cdot (5 - 1) = 84$ elements of order 5. But $90 + 84 > 105$, a contradiction. Thus either $r_7(K) = 1$ or $r_5(K) = 1$. □
Assume that \( r_7(K) = 1 \). Then \( K \) has a normal subgroup \( N \) of order 7 (hence solvable), and \( F = K/N \) is of order \( 3 \cdot 5 \). Thus \( F \) has a unique Sylow 5-subgroup \( S \) (solvable), and since \( F/S \) is of order 3, it is also solvable.

The case \( r_5(K) = 1 \) is analogous.

**Problem 1.4.** We say that an abelian group \( G \) has property \( P \) iff the following holds: for every subgroup \( H \) of \( G \), \( G/H \) is isomorphic to a subgroup of \( G \).

Let \( G \) be a finitely generated abelian group. Show that \( G \) has property \( P \) if and only if \( G \) is finite.

Solution: By the fund. thm. for fin. gen. abelian groups we have \( G = (\mathbb{Z})^n \times \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_m^{r_m}} \), where \( n \geq 0 \), \( m \geq 0 \), \( r_i \geq 0 \) and \( p_i \) are primes, not necessarily distinct. Clearly, \( G \) is finite iff \( n = 0 \).

Assume \( G \) is finite. Let \( H \) be a subgroup of \( G \). Then \( G/H \) is finite abelian group of order \( |G|/|H| \). The order of \( G/H \) is \( p_1^{s_1} \cdots p_m^{s_m} \) for some \( s_i \leq r_i \). It is then easy to adjust the factors of \( G \) for each prime \( p_i \) to obtain the group of desired order.

Assume \( G \) is infinite, say \( G = \mathbb{Z} \times K \) (where \( K \) could still be infinite). Let \( p \) be a prime that is not equal to any \( p_i \). Let \( H = p\mathbb{Z} \times K \). Then \( G/H \cong \mathbb{Z}_p \). Since \( G \) has no elements of order \( p \), we are done.

**2. Rings**

**Problem 2.1.** Let \( R \) be a commutative ring with 1. Let us call an ideal \( I \) of \( R \) irreducible if it is NOT possible to write \( I = I_1 \cap I_2 \), where \( I_1, I_2 \) are proper ideals of \( R \) properly containing \( I \).

(i) Let \( 0 \neq x \in R \). Show that there is an ideal \( I_x \) of \( R \) maximal with respect to the property that \( x \notin I_x \).

(ii) Show that the ideal \( I_x \) from part (i) is irreducible.

(iii) Show that every prime ideal \( P \) of \( R \) is irreducible.

Solution: (i) Let \( S = \{ I \leq R, I \text{ proper; } x \notin I \} \). Since \( 0 \in S \), \( S \) is not empty. When \( I_0 \leq I_1 \leq I_2 \leq \cdots \) is a chain of ideals of \( S \), then \( I = \bigcup I_i \) is a proper ideal of \( R \) (since \( 1 \notin I \)), and it does not contain \( x \) (easy). By Zorn’s lemma, \( S \) has a maximal element, and that’s our \( I_x \).

(ii) Assume \( I_x = I \cap J \) in the forbidden way. Since \( I \) properly contains \( I_x \) and \( I_x \) is maximal, we have \( x \in I \). Similarly, \( x \in J \). But then \( x \in I \cap J \), a contradiction.

(iii) Let \( P = I \cap J \) in the forbidden way. Let \( r \in I \setminus P, s \in J \setminus P \). Then \( rs \in I \), \( rs \in P \). This is a contradiction with \( P \) being prime.

**Problem 2.2.** (i) Let \( R = \mathbb{Z}[\sqrt{-11}] = \{ m + n\sqrt{-11}; m, n \in \mathbb{Z} \} \). Find all units of \( R \). Show that \( R \) possesses an element that is irreducible but not prime.

(ii) Now let \( R = \mathbb{Z}[\sqrt{7}] \), and let \( Q \) be the field of fractions of \( R \). Show that the polynomial \( x^2 - x - 4 \) is irreducible in \( R \) but not in \( Q \).

Solution: (i) The map \( N : R \to \mathbb{Z} \) defined by \( m + n\sqrt{-11} \mapsto m^2 + 11n^2 \) is multiplicative. When \( u \in R \) is a unit, there is \( v \) such that \( uv = 1 \). Then \( N(u)N(v) = N(1) = 1 \). Thus \( N(u) = 1 \). Hence \( U(R) = \{ 1, -1 \} \).

Consider \( r = 1 + \sqrt{-11} \). Note that \( N(r) = 12 = 2 \cdot 2 \cdot 3 \). Now, it is easy to see that there are no elements of norm 3 in \( R \), so \( r \) is irreducible. Since \( r(1 - \sqrt{-11}) = 12 \), \( r \) divides 12 = 3 \cdot 4. But \( r \) does not divide 3 (compare norms) nor 4 (again compare norms). Thus \( r \) is not prime.
(ii) Let \( f(x) = x^2 - x - 4 \). We have \( f(m + n\sqrt{17}) = m^2 + 2mn\sqrt{17} + 17n^2 - m - n\sqrt{17} - 4 \). Assume \( f(m + n\sqrt{17}) = 0 \). Since \( \sqrt{17} \) is irrational, we must have \( 2mn - n = 0 \) and \( m^2 + 17n^2 - m - 4 = 0 \). When \( n = 0 \) in the first equation, the second equation reduces to \( m^2 - m - 4 = 0 \), i.e., \( m = (1 \pm \sqrt{17})/2 \). This shows that \( f(x) \) factors in \( \mathbb{Q} \). It also shows that \( f(x) \) does not factor in \( R \) (because we have already found 2 roots).

**Problem 2.3.** Give an example of each of the following, if possible. Explain!

(i) A non-commutative domain that is not a division ring.
(ii) A finite non-commutative ring.
(iii) A unique factorization domain that is not a principal ideal domain.
(iv) A non-commutative domain that is not a division ring.
(v) A unique factorization domain that is not a principal ideal domain.

Solution: (i) \( \mathbb{H}[x] \), (ii) \( M_2(GF(p)) \), (iii) \( F[x, y] \) where \( F \) is a field, (iv) does not exist by Wedderburn Theorem.

**Problem 2.4.** Let \( R \) be a commutative ring with ideals \( A, B \). Let \( f : R \to R/A \times R/B \) be defined by \( f(r) = (r + A, r + B) \).

(i) Show that \( f \) is a homomorphism of rings.
(ii) Show that \( f \) is surjective if and only if \( A + B = R \).

Solution: (i) is routine.

(ii) Assume that \( f \) is surjective. Then for all \( r \in R \) there is \( t \in R \) such that \( f(t) = (r + A, B) \). Thus \( t + A = r + A, t + B = B \). Thus \( t - r = a \in A, t \in B \). Thus \( r = -a + t \in A + B \).

Conversely, assume that \( A + B = R \). Let \( r, s \in R \). Then \( r = ra + rb, s = sa + sb \) where \( ra, sa \in A, rb, sb \in B \). Thus \( (r + A, s + B) = (r + A, sa + B) \). Then \( f(rb + sa) = (rb + sa + A, rb + sa + B) = (r + A, s + B) \).

3. Fields and Galois Theory

**Problem 3.1.** Construct a field \( F \) of order 9. Explicitly construct isomorphism of vector spaces between \( \mathbb{Z}_3 \times \mathbb{Z}_3 \) and \( F \). Explicitly construct isomorphism of groups between a group \( G \) of order 8 and \( F^* \).

Solution: Need irreducible polynomial of degree 2 over \( \mathbb{Z}_3 \), and \( f(x) = x^2 + 1 \) does the job: \( f(0) = 1, f(1) = 2, f(2) = 4 + 1 = 2 \). Let \( F = \mathbb{Z}_3[x]/(f(x)) = \{ax + b; a, b \in \mathbb{Z}_3 \} \). The isomorphism between vector spaces is \( (a, b) \mapsto ax + b \). We need a primitive element. Try \( x + 1; (x + 1)^2 = x^2 + 2x + 1 = 2x, (x + 1)^3 = 2x(x + 1) = 2x^2 + 2x = 2x - 2, (x + 1)^4 = (2x - 2)(x + 1) = 2(x^2 - 1) = 2(-2) = -4 = -1 \). Hence \( x + 1 \) is a primitive element. Let \( G = \langle a \rangle, a^8 = 1 \). Then \( a^1 \mapsto (x + 1)^i \) is the needed isomorphism.

**Problem 3.2.** Let \( F = \mathbb{Q}, E = \mathbb{Q}(i, \sqrt{7}) \).

(i) Show that \( F \subset E \) is a Galois extension.

(ii) Find the isomorphism type of the Galois group \( \text{Gal}(E/F) \) and describe all its elements.

(iii) Draw the lattice of all intermediate fields \( F \subset K \subset E \) and describe all intermediate fields \( K \) as \( K = F(u) \) for some \( u \in E \).

Solution: I write \( Q \) instead of \( \mathbb{Q} \) here. We have \( Q \subseteq Q(\sqrt{7}) \subseteq Q(i, \sqrt{7}) \). Both extensions are of degree 2: as witnessed by \( x^2 - 7 \) and \( x^2 + 1 \). Thus \( E \) is the splitting field of \( f(x) = (x^2 - 7)(x^2 + 1) \), which is separable, and thus \( F \subseteq E \) is Galois. Let \( G \) be the Galois group. Since \( F \subseteq E \) is Galois, |\( G \)| = 4. We either have \( G = \mathbb{Z}_4 \) or
$G = \mathbb{Z}_2 \times \mathbb{Z}_2$. The latter is correct because both $Q(\sqrt{7})$ and $Q(i)$ are intermediate fields, and $\mathbb{Z}_4$ has only one intermediate subgroup. The automorphisms are $1$, $\sigma$, $\tau$, and $\sigma \tau$, where $\sigma(i) = i$, $\sigma(\sqrt{7}) = -\sqrt{7}$, $\tau(i) = -i$, $\tau(\sqrt{7}) = \sqrt{7}$. The intermediate field corresponding to $\langle \sigma \rangle$ is $Q(i)$. The intermediate field corresponding to $\tau$ is $Q(\sqrt{7})$. Which element is fixed by $\sigma \tau$? Well, $\sigma \tau(i \sqrt{7}) = i \sqrt{7}$. Thus the intermediate field corresponding to $\langle \sigma \tau \rangle$ is $Q(i \sqrt{7})$. □

**Problem 3.3.** (i) Show that every finite extension is algebraic.
(ii) Show that every simple algebraic extension is finite.
(iii) Assume that $F \subseteq E$ and $E \subseteq D$ are algebraic extensions. Must $F \subseteq D$ be algebraic?

**Solution:** (i) Assume $F \subseteq E$ is finite, say of dimension $n$. Let $e \in E$. Then $e, e^2, \ldots, e^{n+1}$ are linearly dependent, etc.

(ii) Let $F \subseteq F(u)$ be a simple algebraic extension. Then there is $f \in F[x]$ such that $f(u) = 0$. Then $|F(u) : F| = \deg m \leq \deg f < \infty$, where $m$ is the minimal polynomial for $u$.

(iii) It must be algebraic. Let $d \in D$. Since $E \subseteq D$ is algebraic, there are $e_i \in E$ such that $e(d) = 0$, where $e(x) = \sum_i e_i x^i$. Since each $e_i$ is algebraic over $F$ and since $d$ is algebraic over $E$, $F \subseteq F(e_1) \subseteq F(e_1, e_2) \subseteq \cdots \subseteq F(e_1, \ldots, e_n) \subseteq F(e_1, \ldots, e_n, d)$ is a chain of finite extensions. Hence $F \subseteq F(e_1, \ldots, e_n, d)$ is finite, thus algebraic by (i). This means that $d$ is algebraic over $F$. □

**Problem 3.4.** Let $A(\mathbb{Q}) = \{u \in \mathbb{C}; f(u) = 0 \text{ for some } f \in \mathbb{Q}[x]\}$. You can take for granted that $A(\mathbb{Q})$ is a field, called algebraic numbers. Show that:

(i) $A(\mathbb{Q}) = \{u \in \mathbb{C}; f(u) = 0 \text{ for some } f \in \mathbb{Z}[x]\}$,
(ii) $\mathbb{Q} \subseteq \mathbb{A}(\mathbb{Q})$ is an algebraic extension that is not finite. (Hint: Look at $2^{1/n}$ for arbitrarily large $n$.)
(iii) $A(\mathbb{Q})$ is countably infinite.

**Solution:** (i) clear denominators.

(ii) $x^n - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein. Hence $|\mathbb{Q}(2^{1/n}) : \mathbb{Q}| = n$. Since each $\mathbb{Q}(2^{1/n})$ is contained in $A(\mathbb{Q})$, we are done.

(iii) A bit of set theory does the job. There cannot be more roots than polynomials. Each polynomial has finitely many coefficients. Each coefficient is taken from a countable set. □