Midterm

November 3, 2024

There are 6 parts and 4 questions in each part, 20 points each part and 120 points in total. You have 120 minutes to write your answer.

1. (20 points) Let R be a commutative ring with identity.

   (i) (5 points) An element $a \in R$ is called a *nilpotent* element if there exists a positive integer n such that $a^n = 0$. Now we collect all nilpotent elements of R into a set, i.e. $N = \{a \in R | a^n = 0, \text{ for some } n \in \mathbb{Z}_+\}$.

   Prove that N is an ideal of R. This ideal N is called the nilradical of R.

   (ii) (5 points) Recall the definition of *prime ideal*: Let R be a commutative ring with identity. An ideal $P \neq (1)$ of R is called a *prime ideal* if for any $a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$. We can prove the alternative definition of nilradical N, that is: The nilradical N of R is the intersection of all prime ideals of R.

   Step 1: Let $\mathcal{P}$ be the intersection of all prime ideals of R. Prove that if $f \in R$ is not nilpotent, then there exists a prime ideal P of R such that $f \notin P$. In the other word, if $a \in \mathcal{P}$, then a must be a nilpotent element.

   Question: Finish step 2, i.e., prove that if b is a nilpotent element then $b \in \mathcal{P}$.

   (iii) (5 points) An element $x \in R$ is called a *unit* if there exists an element $y \in R$ such that $xy = 1$. A maximal ideal is an ideal that is not contained in any other proper ideal. Let M be a maximal ideal of R. If you take the qoutient R/M then you get a field. All non-unit elements contained in some maximal ideal. Just compare the definition with "maximal subgroup", "maximal ideal" is also not unique in general. But the intersection of all maximal ideals is unique. This intersection is called the *Jacobson radical* of R, denoted by J.

   Prove: $\forall u \in J$, $1 - uv$ is a unit in R for all $v \in R$.

   (iv) (5 points) Prove: The other direction of (iii), that is, if $1 - uv$ is a unit in R for all $v \in R$ then $u \in J$. (Hint: If $u \notin M$ for some maximal ideal M then what can you say about $M + (u)$?)

2. (20 points) As we learned from our class, Let $F = \mathbb{Q}$ be a field, then $F[x]/(x^2 - 2)$ is also a field since $x^2 - 2$ is irreducible over $\mathbb{Q}$. And you can regard $F[x]/(x^2 - 2)$ as a 2-dimensional vector space over $\mathbb{Q}$ with basis $\{1, x\}$. Consider one root of $x^2 - 2$, which is $\sqrt{2}$, maps x to $\sqrt{2}$ then you get $F[x]/(x^2 - 2) \simeq F(\sqrt{2}) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. For a field extension $F \subset E$, the degree of the extension $[E : F]$ is the dimension of E as a vector space over F.

   This lemma may be useful: Let $f(x)$ be a polynomial with integer coefficients, and let $g(x)$ be a divisor of $f(x)$, i.e. $\exists h(x)$ such that $f(x) = g(x)h(x)$. If $g(x)$ is a primitive polynomial, then $h(x)$ is also a polynomial with integer coefficients. Primitive polynomial is a polynomial with integer coefficients such that all coefficients are coprime.

   (i) (5 points) Let $F \subseteq K \subseteq L$ be finite fields extensions. Prove: $[L : F] = [L : K][K : F]$.

(ii) (5 points) There exists three famous geometric problems posed by ancient Greeks, which are: *Doubling the Cube*, *Squaring the Circle*, and *Trisecting the Angle*. It's also known as "Impossibility of compass and straightedge construction". One lemma is proved that: If the element $\alpha \in \mathbb{R}$ is obtained from a field $\mathbb{Q}$ by a series of compass and straightedge constructions then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ for some integer $k \geqslant 0$.

Prove that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ so that doubling the cube is impossible.

(iii) (5 points) If an angle θ can be constructed, it is equivalent to $\cos\theta$ can be constructed.

Prove that $\cos 20°$ cannot be constructed by compass and straightedge. i.e. trisecting an (arbitary) angle is impossible. (Hint: $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$).

(iv) (5 points) As we all known, π is a transcendental number, which means it is not a root of any polynomial equation with rational coefficients.

Prove that $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is not finite. i.e. Squaring the circle is impossible.

3. (20 points) Recall the definition of group action we learned in our class:

Definition. Let G be a group and Ω be a set. We say that G acts on Ω if

(a) each element of G is a bijection from Ω to Ω;

(b) $\forall \omega \in \Omega$, $\omega^1 = \omega$;

(c) $\forall \omega \in \Omega$ and $g, h \in G$ we have $\omega^{gh} = (\omega^g)^h$.

We denote this action by $G \curvearrowright \Omega$.

Suppose G is a finite group acting on a set Ω, where $x, y \in G$ and $\alpha, \beta \in \Omega$.

(i) (5 points) Prove that two orbits $\Delta_\alpha = \{\omega \in \Omega | \alpha^g = \omega, g \in G\}$ and $\Delta_\beta = \{\omega \in \Omega | \beta^g = \omega, g \in G\}$ are equal or disjoint.

(ii) (5 points) If $\forall \alpha, \beta \in \Omega$, there exists $x \in G$ s.t. $\alpha^x = \beta$, then we call this group action $G \curvearrowright \Omega$ is transitive. **Now suppose $G \curvearrowright \Omega$ is transitive for question (ii), (iii) and (iv).**

Prove that for all $\alpha, \beta \in \Omega$, the stabilizers $G_\alpha = \{x \in G | \alpha^x = \alpha\}$ and $G_\beta = \{x \in G | \beta^x = \beta\}$ are conjugate subgroups. i.e. There exists $g \in G$ s.t. $G_\alpha = g^{-1} G_\beta g$.

(iii) (5 points) Prove that $\forall \alpha \in \Omega$, $[G : G_\alpha] = |\Omega|$.

(iv) (5 points) Recall the definition of regular and semiregular actions:
Definition. A group action $G \curvearrowright \Omega$ is called *semiregular* if $G_\alpha = \{1\}$ for all $\alpha \in \Omega$. A group action $G \curvearrowright \Omega$ is called *regular*, if G is both transitive and semiregular on Ω.
Prove that $G \curvearrowright \Omega$ is regular if and only if $|G| = |\Omega|$.

4. (20 points) Let G be a finite group. Let p be a prime number where $p \mid |G|$.

As we learned in class, the Sylow 3rd Theorem tells us if n_p denotes the number of p-Sylow subgroups of a group G, then n_p divides $|G|$ and $n_p \equiv 1 \pmod p$. Let $Syl_p(G) = \{all\ Sylow\ p-subgroups\ of\ G\}$ then $|Syl_p(G)| = n_p$. Now we try to prove a stronger version of the theorem:

Stronger Sylow 3rd Theorem: $n_p \equiv 1 \pmod{p^e}$, where $p^e = min[S : S \cap T]$, where $S \in Syl_p(G)$ and T runs through $Syl_p(G)$, $T \neq S$.

For any $S \in Syl_p(G)$, let S act on $Syl_p(G)$ by conjugation. That is, for any $s \in S$ and $P \in Syl_p(G)$, define $P^s := s^{-1}Ps$.

(i) (5 points) For any two Sylow subgroups S and P, prove that the stabilizer of P in the group action $S \curvearrowright Syl_p(G)$ is $S \cap P$.

(ii) (5 points) Finish the proof of the stronger Sylow 3rd Theorem.

(iii) (5 points) Prove that if $|G| = pq$ where p and q are distinct primes, then G is not simple.

(iv) (5 points) Prove that if $|G| = p^a q$ where p and q are distinct primes and a is a positive integer, and for any $S, T \in Syl_p(G)$ we have $S \cap T = \{e\}$ then G is not simple.

5. (20 points) Recall the fundamental theorem of finite abelian groups.

Theorem. *For every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. Formally, let G be a finite abelian group of order $n > 1$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then:*

(a) $G \simeq A_1 \times A_2 \times \cdots \times A_k$ where $|A_i| = p_i^{\alpha_i}$;

(b) For each A_i, $A_i \simeq Z_{p_i^{\beta_1}} \times Z_{p_i^{\beta_2}} \times \cdots \times Z_{p_i^{\beta_t}}$ where $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha_i$.

Using this theorem, answer the following questions.

(i) (5 points) Let G be a abelian group of order 72, find all the possible isomorphism classes of G.

(ii) (5 points) Find the number of cyclic subgroups of order 4 of the following group: $G = Z_2 \times Z_4 \times Z_8 \times Z_{16}$.

(iii) (5 points) Find the number of non-cyclic subgroups of order 4 of the following group: $G = Z_2 \times Z_4 \times Z_8 \times Z_{16}$.

(iv) (5 points) Write the automorphism group of following groups respectively: Z_{27}, Z_{16}, Z_{72}, $Z_2 \times Z_2$, Z_p^d.

6. (20 points) In our class, we proved the simplicity of $A_n (n \geq 5)$ by discussing the form of cycles. Here, we will prove the simplicity of $A_n (n \geq 5)$ by induction on n. First, suppose we have already proven the simplicity of A_5. Next, assume that A_{n-1} is simple. Now we will prove that A_n is simple.

(i) (5 points) Using Sylow theorem, show that A_4 is not simple. (Hint: Consider the order of A_4.)

(ii) (5 points) Let $G = A_n$ with $n \geq 6$. Prove that a proper normal subgroup H is semiregular on $\{1, \cdots, n\}$. (Hint: Consider the natural action of G on $\{1, 2, \dots n\}$. By induction hypothesis, the point stabilizer $G_i \simeq A_{n-1}$ is simple.)

(iii) (5 points) For any non-identity $\tau \in H$, define r as the longest length of a disjoint cycle in τ. Show that $r < 3$. (Hint: If $r \geq 3$ construct τ_1 and τ_2 such that $\tau_1(i) = \tau_2(i)$ for some $i \in \{1, \cdots, n\}$.)

(iv) (5 points) Prove that H does not exists. (Hint: Note any non-identity $\tau \in H$ is a product of disjoint cycles of length 2.)