Algebra Qualifying Exam Solutions

(Accuracy Not Guaranteed)

Hui Sun

May 6, 2025

Contents

Warning 0.1. I cannot do Nakayama lemma questions.

Warning 0.2. I cannot do some of other questions either.

Chapter 1

Fall 2024

Problem 1.1. Let p be prime and G a nonabelian group of order $2p$. Compute the number of conjugacy classes of elements of G.

Problem 1.2. Recall that a commutative ring R is *Artinian* if every descending chain of ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$ is eventually constant. Show that if R is an Artinian integral domain, then R is a field.

Problem 1.3. Let K be a field and $f(x) \in K[x]$ an irreducible polynomial. Suppose given a finite extension L of K of degree prime to the degree of $f(x)$. Show that $f(x)$ is irreducible over L.

Problem 1.4. Determine $m, n \in \mathbb{Z} \setminus \{0\}$ such that fields $\mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{n})$ are isomorphic.

Problem 1.5. Prove that any two dimensional faithful complex representation of a non-commutative group is irreducible.

Problem 1.6. Let A, B be linear operators on a finite dimensional vector space V over a field of characteristic 0 such that $A^3 = B^2$ are the identity and $AB = BA^2$. Prove that if U is an invariant under A, B subspace of V then there exists an invariant under A, B subspace W of V such that $V = U \oplus W$.

Chapter 2

Fall 2023

3,6

Problem 2.1. For any positive integer n, denote by A_n the group of even permutations on a set of cardinality n.

(i) Let G be a simple group with a proper subgroup H of index n. Suppose that the order of G is at least 3. Prove that there exists an injective homomorphism from G to A_n.

(ii) Prove that A_6 has no subgroup of order 120. [Hint: You may use the fact that A_n is simple for $n \geq 5$.]

Proof. (i) We note that G has an action on the cosets $g_i H$, since $[G : H] = n$, this is a transitive action that permutes n elements, thus there is a map

$$\rho : G \to S_n$$

since G is simple, we know $\ker(\rho) = \{e\}$, i.e.,

$$G \cong \mathrm{im}(\rho)$$

It suffices to show that $\mathrm{im}(\rho)$ is contained in A_n, suppose not, then $\mathrm{im}(\rho) \cap A_n$ is a subgroup of index 2 in $\mathrm{im}(\rho)$, hence is normal in $\mathrm{im}(\rho)$, this is a contradiction again to the fact that G is simple. This shows that $\mathrm{im}(\rho) \subset A$, and ρ is faithful, thus G embeds into A_n.

(ii) Using (i), suppose there is a subgroup H of order 120 of A_6, since A_6 is simple, then $[A_6 : H] = 3$, we know there exists an injective homomorphism from A_6 to A_3, which is a contradiction.

□

Problem 2.2. Answer the following questions and justify your answers.

(i) Is $X^2 + Y^2 + 1$ irreducible in the polynomial ring $\mathbb{C}[X, Y]$?

(ii) Is $X^2 + 3X + 2$ irreducible in the formal power series ring $\mathbb{Z}[[X]]$?

Proof. (i) It is irreducible. We see

$$X^2 + Y^2 + 1 = X^2 + (Y - i)(Y + i)$$

since $(Y - i)$ is irreducible in $\mathbb{C}[Y]$, i.e., prime in $\mathbb{C}[Y]$, we apply generalized Eisenstein,

$$X^2 + Y^2 + 1 \text{ is irreducible in } (\mathbb{C}[Y])[X]$$

and we are done by observing $\mathbb{C}[Y][X] = \mathbb{C}[X, Y]$.

(ii) It is also irreducible. We can proceed directly with the definition, since

$$X^2 + 3X + 2 = (X + 2)(X + 1)$$

and $(X + 1)$ is a unit in $\mathbb{Z}[[X]]$, hence it is irreducible. (Alternatively, f is a unit if the constant term $f(0)$ is a unit, thus suppose

$$f = gh$$

then $g(0)h(0) = f(0)$. If $f(0)$ is irreducible, it implies either $g(0)$ or $h(0)$ is a unit, which implies either g or h is a unit, hence f irreducible.)

□

Problem 2.3. Denote by $\mathrm{SL}_2(\mathbb{C})$ the special linear group over the complex number field, i.e., the group of all 2×2 complex matrices with determinant 1. Prove the following statements.

(i) $\mathrm{SL}_2(\mathbb{C})$ is generated by elements of the forms

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

where $a \in \mathbb{C}$, and

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$$

where $b \in \mathbb{C}$.

(ii) $\mathrm{SL}_2(\mathbb{C})$ is equal to its own commutator subgroup.

Problem 2.4. Prove that the quotient ring $\mathbb{Z}[\sqrt{2}]/(3)$ is a field.

Proof. Since $\mathbb{Z}[\sqrt{2}]/(3)$ is finite, it is a field iff it is an integral domain. Hence it suffices to see that (3) is a prime ideal in $\mathbb{Z}[\sqrt{3}]$. □

Problem 2.5. Compute the Galois group of the splitting field of the polynomial $X^4 - 3$ over $\mathbb{Q}$.

Proof. The Galois extension generated by this polynomial is

$$\mathbb{Q}(\sqrt[4]{3}, i)$$

Thus the Galois group has order 8, i.e., a 2-Sylow subgroup of S_4, hence it must be isomorphic to D_8. □

Problem 2.6. Compute the character table for the dihedral group D_5.

Chapter 3

Fall 2019

3,5

Problem 3.1. Let $\mathbb{F}_q$ be a field with $q \neq 9$ elements and a be a generator of the cyclic group $\mathbb{F}_q^*$. Show that $\mathrm{SL}_2(\mathbb{F}_q)$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

Proof. I will not do all the computation here, but here are a list of matrices one can get using these generators:

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

where t is any element in $\mathbb{F}_q$. And one can essentially show that these generate all the upper triangular matrices in $\mathrm{SL}_2(\mathbb{F}_q)$, i.e.,

$$\left\{ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} : x, y \in \mathbb{F}_q \right\}$$

and one can show that any matrix in $\mathrm{SL}_2(\mathbb{F}_q)$ is a product of $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and upper triangular matrices, then done. □

Problem 3.2. Let p, q be two prime numbers such that $p|q-1$. Prove that:

(a) there exists an integer $r \not\equiv 1 \mod q$ such that $r^p \equiv 1 \mod q$;

(b) there exists (up to an isomorphism) only one noncommutative group of order pq.

Proof. (a) We want to find there exists $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ such that $r \neq 1$ such that $r^p \equiv 1 \mod q$. If $p \mid (q-1)$, then there exists an element of order p in the group $(\mathbb{Z}/q\mathbb{Z})^\times$ by Cauchy's theorem, i.e., $r^p \equiv 1 \mod q$.

(b) We must have $q > p$ then $n_q = 1$, and we can write

$$G = N \otimes_\theta P$$

where N is a normal q-subgroup and P is a Sylow p-subgroup. We note that

$$\theta : 1 \mapsto r$$

where r is an element of order p, which exists by (a). And the group is described as

$$G = \langle g, h : g^q = h^p = e : hgh^{-1} = g^r \rangle$$

This group is unique because the elements $g \mapsto g^r$ where r is any element wth order p forms a subgroup in $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$, thus they define isomorphic strucutres of G.

□

Problem 3.3. Let F, L be extensions of a field K. Suppose that F/K is finite. Show that there exists an extension E/K such that there are monomorphisms of F into E and of L into E which are identical on K.

Problem 3.4. Find all irreducible representations of a finite p-group over a field of characteristic p.

Proof. Let G any finite p-group. Let V be an irreducible representation over $\mathbb{F}_p$, consider the $[\mathbb{F}_p G]$-module W generated by any $v \in V \setminus \{0\}$. We see W is a finite-dimensional vector space over $\mathbb{F}_p$, i.e.,

$$|W| = p^d$$

for some $d \geq 1$. We consider the action of G on W, all the orbits of this action either has size 1 or is a power of p, since G is a p-group, by the class formula, let N be the number of nontrivial orbits of size 1,

$$|W| \equiv 1 + N \mod p \Rightarrow 1 + N \equiv 0 \mod p$$

Hence there exists at least one nontrivial orbit $\{v\}$ of size 1. We consider the vector space $\bar{W}$ generated by v over $\mathbb{F}_p$: it is one-dimensional vector space contained in V, invariant under G, since V is irreducible, we must have $V = \bar{W}$. The action of G on $\bar{W}$ is the trivial action, thus all irreducible representations of a finite p-group over $\mathbb{F}_p$ are trivial. □

Problem 3.5. How many two-sided ideals has the group algebra $\mathbb{C}[\mathrm{S}_3]$, where S_3 is the group of permutations of $\{1, 2, 3\}$?

Proof. By Artin-Wedderburn, $\mathbb{C}[S_3]$ can be decomposed into the following

$$\mathbb{C}[S_3] \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C})$$

We note that $n_1^2 + \cdots + n_k^2 = 6$, and each M_{n_i} corresponds to an irreducible representation of dimension n_i, hence we see

$$\mathbb{C}[S_3] = \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$$

Thus it has 3 two sided ideals. □

Chapter 4

Spring 2018

I cannot do 5.
2,3

Problem 4.1. Let F be a field of characteristic not equal to 2. Let D be the non-commutative algebra over F generated by elements i, j that satisfy the relations

$$i^2 = j^2 = 1, \quad ij = -ji.$$

Define $k = ij$.

(a) Verify that D is isomorphic to the algebra $M_2(F)$ of 2×2 matrices in such a way that

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, k \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(b) Write $q = x + yi + zj + uk$ for $x, y, z, u \in F$. Verify that the norm

$$N(q) = x^2 - y^2 - z^2 + u^2$$

corresponds to the determinant under the isomorphism of part (a).

(c) What does the involution $q \mapsto \bar{q} = x - yi - zj - uk$ on D correspond to on the matrix side?

Proof. (a) Let φ denote this map, it is clear that $\varphi(i)^2 = \varphi(j)^2 = I$, and $\varphi(ij) = \varphi(-ji) = \varphi(k)$. Thus it suffices to show that φ is a bijecction. Since D is generated by i, j and they each have other 2, then any element in D is of the form

$$ai + bj$$

where $a, b \in F$. Then we see φ is injective because

$$\varphi(ai + bj) = 0 \Rightarrow a = b = 0$$

To show φ is surjective, it suffices to see that $M_2(F)$ is generated by $\varphi(i), \varphi(j)$. Using the fact the generators of $M_2(F)$ are

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

We see that they can be generated using $\varphi(i), \varphi(j)$, hence also surjective.

(b) We see that

$$\varphi(q) = \begin{pmatrix} x + y & z + u \\ z - u & x - y \end{pmatrix}$$

Thus $N(q) = \det(\varphi(q))$.

(c) We see

$$\varphi(\overline{q}) = \begin{pmatrix} x-y & -(z+u) \\ -(z-u) & x+y \end{pmatrix}$$

This corresponds to taking the adjugate

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

□

Problem 4.2. Let R be a commutative ring. An R-module M is said to be finitely presented if there exists a right-exact sequence

$$R^m \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

for some non-negative integers m, n. Prove that any finitely generated projective R-module P is finitely presented.

Problem 4.3. Let R be the ring $\mathbb{Z}[\zeta_p]$, where p is a prime number and ζ_p denotes a primitive pth root of unity in $\mathbb{C}$. Prove that if an integer $n \in \mathbb{Z}$ is divisible by $1 - \zeta_p$ in R, then p divides n.

Problem 4.4. Is S_4 isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{C})$?

Proof. We've done this in Spring 2017 exam. We want to show there is no injective homomorphism from S_4 to $\mathrm{GL}_2(\mathbb{C})$, i.e., it is a representation. The 2 dimensional representation and the direct sum of 1-dimensional representations all send $(12)(34)$ to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. □

Problem 4.5. Let n be a positive integer and A an abelian group. Prove that

$$\mathrm{Ext}^1(\mathbb{Z}/n\mathbb{Z}, A) \cong A/nA.$$

Chapter 5

Fall 2017

Problem 5.1. Show that there is no simple group of order 30.

Proof. We know that $n_5 = 1$ or 6, if $n_5 = 1$, then we are done. If $n_5 = 6$, then there are $30 - 4 \cdot 6 = 6$ elements of order $\neq 6$, and we know there exists at least one Sylow 2-subgroup and one Sylow 3-subgroup, combined with the identity element, we see either $n_2 = 1$ or $n_3 = 1$. □

Problem 5.2. Let Λ be a free abelian group of finite rank n, and let $\Lambda' \subset \Lambda$ be a subgroup of the same rank. Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for Λ, and let $x_1', \ldots, x_n'$ be a $\mathbb{Z}$-basis for Λ'. For each i, write $x_i' = \sum_{j=1}^n a_{ij} x_j$, and let $A := (a_{ij}) \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$. Show that the index $[\Lambda : \Lambda']$ equals $|\det A|$.

Proof. We notice that $\Lambda = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, and Λ' is a subgroup of same rank thus

$$\Lambda' = d_1\mathbb{Z} \oplus \cdots \oplus d_n\mathbb{Z}$$

where d_i are integers, up to some basis change (we will argue below why change of basis doesn't affect the equality). We note that

$$[\Lambda : \Lambda'] = \left| \prod_{i=1}^n d_i \right|$$

It suffices to take the basis of Λ as $x_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where only the ith entry is nonzero and equal to 1, and the basis for Λ' as $x_j' = (0, \ldots, 0, d_j, 0, \ldots, 0)$, where only the jth entry is nonzero and equal to d_j. This is because for any change of basis matrix P, we have

$$\det(PAP^{-1}) = \det(A)$$

i.e., we can freely change the basis of A. With respect to the basis chosen above, we have

$$A = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & d_n \end{pmatrix}$$

This shows that

$$|\det A| = \left| \prod_{i=1}^n d_i \right| = [\Lambda : \Lambda']$$

as desired. □

Problem 5.3. In this problem all rings are commutative.

(a) Let R be a local ring with maximal ideal $\mathfrak{m}$, let N and M be finitely generated R-modules, and let $f\colon N \to M$ be an R-linear map. Show that f is surjective if and only if the induced map $N/\mathfrak{m}N \to M/\mathfrak{m}M$ is.

(b) Recall that a module M over a ring R is *projective* if the functor $\mathrm{Hom}_R(M, -)$ is exact. Show that if R is local and M is finitely generated projective, then M is free.

Proof. (a) If f is surjective, this means for any $y \in M$ there exists x such that $f(x) = y$, hence the induced map $\overline{f} : x + \mathfrak{m}N \mapsto f(x) + \mathfrak{m}M$ is also sujrective: for any $y + \mathfrak{m}M$ there exists $x + \mathfrak{m}M$ such that $\overline{f}(x + \mathfrak{m}M) = y + \mathfrak{m}M$. Conversely, consider $\mathrm{im}(f) \subset M$, since $\overline{f}$ is surjective, we have $M = \mathrm{im}(f) + \mathfrak{m}M$, by Nakayama's lemma,

$$\mathfrak{m}(M/\mathrm{im}(f)) = 0$$

implies that $M/\mathrm{im}(f) = 0$, i.e., $M = \mathrm{im}(f)$.

(b) I give up.

□

Problem 5.4. Compute the Galois group of $x^5 - 10x + 5$ over $\mathbb{Q}$.

Proof. One can graph this function and see there are only 3 real roots, we first note

$$\begin{cases} f(-2) < 0 \\ f(-1) > 0 \\ f(1) < 0 \\ f(2) > 0 \end{cases}$$

By IVT, there are at least 3 real roots. By Rolle's theorem, between any roots, there must exists a point $f'(c) = 0$, therefore we argue there can be at most 3 real roots because there are only two points p such that $f'(p) = 0$. This shows that there are 2 complex roots, and let r_1 be a complex root. By Eisenstein, this polynomial is irreducible, and we know the Galois group G is a subgroup of S_5. Because G contains a transposition (sending two complex roots to each other), and an element of order 5, we know that G must be equal to S_5.

□

Problem 5.5. Let K/k be an extension of finite fields with $\#k = q$, let $\Phi\colon x \mapsto x^q$ denote the qth power Frobenius map on K, and let $G := \mathrm{Gal}(K/k)$.

(a) Compute the minimal polynomial of Φ as a k-linear endomorphism of K.

(b) Use (a) to prove the *normal basis theorem* in the case of the extension K/k: there exists $x \in K$ such that the set $\{\sigma x \mid \sigma \in G\}$ is a k-basis for K.

Proof. (a) Let $|K| = q^n$, we claim that the minimal polynomial is $f(t) = t^n$. This is because Φ is a generator of G, and G has order n. (One can prove this fact by assuming there exists some $k < n$ such that $x^{p^k} = x$ for all $x \in K$, then q^n divides q^k, which is a contradiction).

(b) We will use some general fact about linear algebra: $T : V \to V$ is a linear map, the minimal polynomial is equal to the characteristic polynomial if and only if there exists a vector v such that $\{v, Tv, \ldots, T^{n-1}v\}$ is a basis for V. By (a), we know the minimal polynomial coincide with the characteristic polynomial, since G is cyclic with generator Φ, we see that there exists x such that

$$\left\{x, \Phi x, \ldots, \Phi^{n-1}x\right\}$$

is a basis for K over k.

□

Problem 5.6. Let G be a finite group with center $Z \subset G$. Show that if G admits a faithful irreducible representation $G \to \mathrm{GL}_n(k)$ for some positive integer n and some field k, then Z is cyclic.

Proof. We first assume that k is algebraically closed. We know that $\rho(z)$ is a G-invariant map: take any $g \in G$,

$$\rho(z)(\rho(g)(v)) = \rho(g)\rho(z)(v)$$

therefore $\rho(z) = \lambda I_n$ for some $\lambda \in k^\times$, this shows that ρ embdes z into a group of $k^\times$, i.e., a cyclic group.

Now for the case where k is not algebraically closed. Then any $\rho \otimes k^a$ is also faithful, and although $\rho \otimes k^a$ might not be irreducible, if $\rho \otimes k^a = \rho_1 + \rho_2$, where ρ_i are irreducible, then it follows that both ρ_1 and ρ_2 are faithful representations of G over k^a. This again shows that Z is cyclic. □

Chapter 6

Spring 2017

Problem 6.1. Let A be a commutative ring, and define the *nilradical* $\sqrt{0}$ to be the set of nilpotent elements in A. Show that $\sqrt{0}$ is equal to the intersection of all prime ideals in A. Show that if A is reduced, then A can be embedded into a product of fields.

Proof. Let $\{P_i : i \in I\}$ be the collection of prime ideals in A. We first show that

$$\sqrt{0} = \bigcap_i P_i$$

Let $a \in \sqrt{0}$, then for some $n \geq 0$, $a^n = 0$, this implies that for all $i \in I$,

$$a^n \in P_i \Rightarrow a \in P_i \text{ or } a^{n-1} \in P_i$$

since P_i is prime. We claim that $a \in P_i$. If not, then $a^{n-1} \in P_i$ which implie $a^{n-2} \in P_i \dots$ which eventually implies $a \in P_i$, which is a contradiction. Hence $\sqrt{0} \subset \bigcap_i P_i$. Now for the reverse inclusion, we use the following lemma:

Lemma 6.1. Let S be a multiplicative set in A such that $0 \notin S$, then there exists a prime ideal $P \subset A$ such that

$$S \cap P = \varnothing$$

Let $a \in \bigcap_i P_i$, then the set

$$S = \{a, a^2, \dots\}$$

is a multiplicative set, suppose that a is not nilpotent, i.e., $a \notin S$, then there exists a prime ideal that does not interserct S, which is a contradiction since $a \in P_i$ for all i. Thus

$$\sqrt{0} = \bigcap_i P_i$$

Now we show that if A is reduced, then A can be embedded into a product of fields. If A is reduced, then $\sqrt{0} = 0$, i.e., if $a \neq 0$, then a cannot be in all the prime ideals. Suppose $a \neq 0$, then there exists some P_i such that $a \notin P_i$. Then we can consider the map

$$A \to \frac{A}{P_i} \to \text{Frac}\left(\frac{A}{P_i}\right)$$

where

$$a \mapsto a + P_i \mapsto \frac{a + P_i}{1}$$

Thus we claim that A embeds in

$$A \xrightarrow{\iota} \text{Frac}\left(\frac{A}{P_1}\right) \times \text{Frac}\left(\frac{A}{P_2}\right) \times \cdots = \prod_{i \in I} \text{Frac}\left(\frac{A}{P_i}\right)$$

where Frac denotes the field of fractions. If $a = 0$, then $\iota(a) = (0, \ldots, 0)$, if $a \neq 0$, then $a \notin P_j$ for some j, and

$$\iota(a) = \left(0, \ldots, 0, \frac{a + P_j}{1}, 0, \ldots, 0\right)$$

where only the j-th entry is nonzero. □

Problem 6.2. Write down the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible over $\mathbb{F}_p$ for every prime number p.

Proof. The minimal polynomial p_m is

$$p_m(t) = (t^2 - 5)^2 - 24 = t^4 - 10t^2 + 1$$

The roots are $\pm\sqrt{2} \pm \sqrt{3}$, thus this polynomial generates a field extension of $\mathbb{Q}$,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \frac{\mathbb{Q}[t]}{(p_m(t))}$$

We claim that it suffices to show that $\sqrt{2}$ or $\sqrt{3}$ or $\sqrt{6}$ are in $\mathbb{F}_p$ for any prime p. Take $\sqrt{2} \in \mathbb{F}_p$ for example, we know $p_m(t)$ is not irreducible over $\mathbb{Q}(\sqrt{2})$, because then it would mean the degree of field extension $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is 8, which is a contradiction.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \uparrow \\ \mathbb{Q}(\sqrt{2}) \\ \uparrow \\ \mathbb{Q} \end{array}$$

Thus $p_m(t)$ is reducible over $\mathbb{Q}(\sqrt{2})$. Now we show the following.

Lemma 6.2. For any prime p, $\sqrt{2}$ or $\sqrt{3}$ or $\sqrt{6}$ are in $\mathbb{F}_p$ for any prime p.

There exists a homomorphism (Legendre symbol) $\varphi : \mathbb{F}_p^\times \to \{\pm 1\}$, such that

$$\varphi(g) = \begin{cases} 1, & \text{if } g \text{ is a square} \\ -1, & \text{otherwise} \end{cases}$$

Suppose that $2, 3$ are not squares, i.e., $sqrt2, \sqrt{3} \notin \mathbb{F}_p^\times$, then

$$\varphi(2 \cdot 3) = 1$$

which implies $\sqrt{6} \in \mathbb{F}_p^\times$, concluding the proof. □

Problem 6.3. Let K/k be a finite separable field extension, and let L/k be any field extension. Show that $K \otimes_k L$ is a product of fields.

Proof. We know K/k implies there exists $\alpha \in K$ such that

$$K = k(\alpha)$$

moreover, for any $t \in K$, the minimal polynomial of t factors into distinct linear factors. Let p_α be the minimal polynomial of α,

$$\begin{aligned} K \otimes_k L &= \frac{k[t]}{(p_\alpha(t))} \otimes_k L \\ &= \frac{L[t]}{(p_\alpha(t))} \\ &= \frac{L[t]}{(p_\alpha^1(t)) \dots (p_\alpha^k(t))} \end{aligned}$$

where $p_\alpha^i(t)$ are distinct irreducible factors over in $L[t]$. By Chinese Remainder Theorem, we must have

$$K \otimes_k L = \frac{L[t]}{(p_\alpha^1(t))} \cdots \frac{L[t]}{(p_\alpha^k(t))}$$

i.e., a product of fields. □

Problem 6.4. Let M be an invertible $n \times n$ matrix with entries in an algebraically closed field k of characteristic not 2. Show that M has a square root, i.e. there exists $N \in \text{Mat}_{n\times n}(k)$ such that $N^2 = M$.

Proof. It suffices to show that every Jordan block

$$J_n(\lambda) = \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & \lambda & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & \lambda \end{bmatrix}$$

where $\lambda \neq 0$ is a square. We will proceed using inductino. When $n = 2$, the square root of

$$\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} \lambda^{\frac{1}{2}} & \frac{1}{2}\lambda^{-\frac{1}{2}} \\ 0 & \lambda^{\frac{1}{2}} \end{bmatrix}^2$$

Now assume that J_k is a square up to $k = n - 1$, we want to show J_n also has a square root. We claim J_n has the following square

$$J_n = \begin{bmatrix} B^2 & x \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} B & x \\ 0 & \lambda^{1/2} \end{bmatrix}^2$$

where B is a $(n-1) \times (n-1)$ matrix and $x = (x_1, \dots, x_{n-1}), 0 = (0, \dots, 0)$. It suffices to find such an x exists. Let $b_1, \dots, b_{n-1}$ denote the row vectors of B, we must satisfy

$$\begin{cases} b_1 \cdot x + x_1\lambda^{\frac{1}{2}} = 0 \\ \dots \\ b_{n-2} \cdot x + x_{n-2}\lambda^{\frac{1}{2}} = 0 \\ b_{n-1} \cdot x + x_{n-1}\lambda^{\frac{1}{2}} = 1 \end{cases}$$

Namely, we need to find x that satisfies

$$(B + \lambda^{\frac{1}{2}} I)x = \begin{bmatrix} 0 \\ \cdots \\ 0 \\ 1 \end{bmatrix}$$

Since $(B + \lambda^{1/2} I)$ is invertible, there exists a unique solution, hence such x exsits, J_n has a square root! □

Problem 6.5. Prove directly from the definition of (left) semisimple ring that every such ring is (left) Noetherian and Artinian. (You may freely use facts about semisimple, Noetherian, and Artinian modules.)

Proof. If R is Artinian, then R can be decomposed into a finite sum of simple rings, let $R_1, \ldots, R_n$ be simple rings, we can write

$$R = \bigoplus_{i=1}^{n} R_i$$

where R_i contains only the trivial ideal and R_i as ideals. Now it is quite clear that every ascending and descending chain of ideals stabilizes because there are only finitely many distinct ideals. □

Problem 6.6. Let G be a finite group and H an abelian subgroup. Show that every irreducible representation of G over $\mathbb{C}$ has dimension $\leq [G : H]$.

Proof. Any irreduicble representation $\rho : H \to \mathbb{C}^\times$ is one-dimensional, and we consider induced representation of ρ, $\mathrm{Ind}_H^G \rho$, we note that $\mathrm{Ind}_H^G \rho$ is not necessarily irreducible, hence for any irreducible representation $\tilde{\rho} : G \to \mathrm{GL}_n(\mathbb{C})$, we have

$$\dim \tilde{\rho} \leq \dim(\mathrm{Ind}_H^G \rho)$$

and

$$\mathrm{Ind}_H^G \rho = \bigoplus_{i=1}^{n} g_i H$$

where g_i are the representatives of the coset and the sum consists of exactly one copy for each coset. Hence we see

$$\dim \tilde{\rho} \leq \dim(\mathrm{Ind}_H^G \rho) = [G : H]$$

□

Chapter 7

Fall 2016

Problem 7.1. Determine $\mathrm{Aut}(S_3)$.

Proof. $\sigma \in \mathrm{Aut}(S_3)$ is determined by where (12) and (123) are sent to. There are 6 options in total and all of them are homomorphisms (conjugation). It is easy to check that this group is not commutative, i.e.,

$$\mathrm{Aut}(S_3) \cong S_3$$

□

Problem 7.2. A group G is a semidirect product of subgroups $N, H \subset G$ if N is normal and every element of G has a unique presentation nh, $n \in N$, $h \in H$. Find all semidirect products (up to isomorphism) of $N = \mathbb{Z}/11\mathbb{Z}$, $H = \mathbb{Z}/5\mathbb{Z}$.

Proof. Let $G = N \rtimes_\theta H$, where

$$\theta : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) \cong \mathbb{Z}/10\mathbb{Z}$$

such that

$$5\theta(1) \equiv 0 \mod 10$$

Thus $\theta(1)$ could be $0, 2, 4, 6, 8$. When $\theta(1) = 0$, this gives the abelian group

$$G \cong \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{11\mathbb{Z}}$$

We claim that all nontrivial θ give rise to the same semidirect product, namely, the following diagram commutes

$$\begin{array}{ccc} \mathbb{Z}/5\mathbb{Z} & \xrightarrow{\theta'} & \mathbb{Z}/10\mathbb{Z} \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ \mathbb{Z}/5\mathbb{Z} & \xrightarrow{\theta} & \mathbb{Z}/10\mathbb{Z} \end{array}$$

for $\theta : 1 \mapsto 2$ and any $\theta' : 1 \mapsto 4, 6, 8$, by taking m to be the multiplication map by $2, 3, 4$ respectively. Hence we see

$$\theta(h)(g) = g^{2^{2h}}$$

by observing

$$\mathbb{Z}/5\mathbb{Z} \xrightarrow{2} \mathbb{Z}/10\mathbb{Z} \xrightarrow{2^2} (\mathbb{Z}/11\mathbb{Z})^\times \xrightarrow[2^2\cdot(-)]{} \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z})$$

In other words,

$$G = \left\langle g, h : g^{11} = h^5 = 1, hgh^{-1} = g^4 \right\rangle$$

□

Problem 7.3. Let F be a finite field of order 2^n. Here $n > 0$. Determine all values of n such that the polynomial $x^2 - x + 1$ is irreducible in $F[x]$.

Proof. We know that $x^2 - x + 1$ is irreducible over $\mathbb{F}_2$, namely, it has no roots in $\mathbb{F}_2$. Since there is only one field of order 4, we must have

$$\mathbb{F}_4 \cong \frac{\mathbb{F}_2}{(x^2 - x + 1)}$$

Clearly $x^2 - x + 1$ is not irreducible over $\mathbb{F}_4$. For any $\mathbb{F}_{2^n}$, we know $(x^2 - x + 1)$ is irreducible if and only if $\mathbb{F}_4$ does not embed into $\mathbb{F}2^n$, i.e., $2 \nmid n$. This shows that when n is odd, the polynomial $x^2 - x + 1$ is irreducible over $\mathbb{F}_{2^n}$. □

Problem 7.4. (1) Determine the Galois group of $x^4 - 4x^2 - 2$ over $\mathbb{Q}$.

(2) Let G be a group of order 8 such that G is the Galois group of a polynomial of degree 4 over $\mathbb{Q}$. Show that G is isomorphic to the Galois group in part (1).

Proof. (1) The roots of this polynomial is $\pm\sqrt{2 \pm \sqrt{6}}$, and notice that

$$\sqrt{2}i = \sqrt{2 + \sqrt{6}}\sqrt{2 - \sqrt{6}}$$

This gives the splitting field (Galois extension) of this polynomila as

$$\mathbb{Q}\left(\sqrt{2 + \sqrt{6}}, \sqrt{2}i\right)$$

We see that

$$\mathbb{Q}\left(\sqrt{2 + \sqrt{6}}\right) \cap \mathbb{Q}(\sqrt{2}i) = \varnothing$$

because the first is contained in $\mathbb{R}$ and the second is not. We must have

$$\left[\mathbb{Q}\left(\sqrt{2 + \sqrt{6}}, \sqrt{2}i\right)/\mathbb{Q}\right] = 8$$

By part b, we see Gal $\cong D_8$.

(2) Any Galois group of a polynomial with 4 roots in the splitting field embeds into S_4, and we notice that $|G| = 2^3, |S_4| = 2^3 \cdot 3$, i.e., G is a Sylow 2-subgroup of S_4, and all Sylow 2-subgroups are conjugate/isomorphic of one another, hence

$$\text{Gal} \cong D_8$$

□

Problem 7.5. Let A be a linear transformation of a finite dimensional vector space over a field of characteristic $\neq 2$.

(1) Define the wedge product linear transformation $\wedge^2 A = A \wedge A$.

(2) Prove that

$$tr(\wedge^2 A) = \frac{1}{2}(tr(A)^2 - tr(A^2)).$$

Proof. (Recall we have analogous results for $A \otimes A$).

(1) The wedge product $A \wedge A$ is defined on the wedge product of vector spaces $V \wedge V$, so we first define the vector space: let $\{v_1, \dots, v_n\}$ be the basis of V, then $\{v_i \wedge v_j\}$ where $i < j$ forms a basis of $V \wedge V$, satisfying:

1. $v_i \wedge v_j = -v_j \wedge v_i$
2. $(a_i v_i + a_j v_j) \wedge (b_k v_k + b_l v_l) = (a_i b_k) v_i \wedge v_k + (a_i b_l) v_i \wedge v_l + (a_j b_k) v_j \wedge v_k + (a_j b_l) v_j \wedge v_l$

And $A \wedge A$ where $A : V \to V$ is defined as

$$A \wedge A(v_i \wedge v_j) = Av_i \wedge Av_j$$

(2) Consider the matrix representation of $A = (A_{ij})$, on the basis $\{v_i \wedge v_j : i < j\}$,

$$\begin{aligned} A \wedge A(v_i \wedge v_j) &= \sum_{k,l=1}^{n} A_{ki} A_{lj} (v_k \wedge v_l) \\ &= \sum_{k<l} A_{ki} A_{lj} (v_k \wedge v_l) + \sum_{l<k} A_{ki} A_{lj} (v_k \wedge v_l) \\ &= \sum_{k<l} A_{ki} A_{lj} (v_k \wedge v_l) - \sum_{l<k} A_{ki} A_{lj} (v_l \wedge v_k) \end{aligned}$$

Thus the diagonal term with respect to $v_i \wedge v_j$ is

$$A_{ii} A_{jj} - A_{ji} A_{ij}$$

Thus

$$\mathrm{Tr}(A \wedge A) = \sum_{i<j} A_{ii} A_{jj} - A_{ji} A_{ij}$$

Now

$$\mathrm{Tr}(A)^2 = \sum_{i=1}^{n} A_{ii}^2 + 2 \sum_{i<j} A_{ii} A_{jj}$$

and

$$\begin{aligned} \mathrm{Tr}(A^2) &= \sum_{k,l=1}^{n} A_{lk} A_{kl} \\ &= \sum_{i=1}^{n} A_{ii}^2 + 2 \sum_{k<l} A_{lk} A_{kl} \end{aligned}$$

Thus we see that

$$tr(\wedge^2 A) = \frac{1}{2}(tr(A)^2 - tr(A^2))$$

□

Problem 7.6. Find a table of characters for the alternating group A_5.

Proof.

	1 Id	20 (1 2 3)	15 (1 2)(3 4)	12 (1 2 3 4 5)	12 (1 2 3 5 4)
χ_1	1	1	1	1	1
χ_2	3	0	-1	ϕ	$1-\phi$
χ_3	3	0	-1	$1-\phi$	ϕ
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

where $\phi = \frac{1+\sqrt{5}}{2}$. □

Chapter 8

Spring 2016

Problem 8.1. Classify all groups of order 66, up to isomorphism.

Proof. There are a total of 4 groups. We have $n_{11} = 1$, take any Sylow-3 subgroup, we can construct a subgroup of order 33 by taking the semidirect product.

Lemma 8.1. Let H be a subgroup of G such that $[G : H] = p$ is the smallest prime dividing $|G|$, then H is normal.

Using the lemma, we know this subgroup N of order 33 must be normal and isomorphic to $\mathbb{Z}/33\mathbb{Z}$. Take any Sylow 2-subgroup of G, we know

$$G = \frac{\mathbb{Z}}{33\mathbb{Z}} \rtimes_\theta \frac{\mathbb{Z}}{2\mathbb{Z}}$$

where $\theta : P_2 \to \text{Aut}(N) = (\mathbb{Z}/33\mathbb{Z})^\times$ satisfies

$$2\theta(1) \equiv 1 \mod 33$$

We see there are four numbers in $(\mathbb{Z}/33\mathbb{Z})^\times$ that satisfy this:

$$\theta(1) \mapsto \{1, 10, 23, 32\}$$

When $\theta(1) = 1$,

$$G_1 \cong \frac{\mathbb{Z}}{33\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

When $\theta(1) = 10$, then

$$G_2 = \langle g, h : g^{33} = h^2 = 1, hgh^{-1} = g^{10} \rangle$$

When $\theta(1) = 23$, we have

$$G_3 = \langle g, h : g^{33} = h^2 = 1, hgh^{-1} = g^{23} \rangle$$

When $\theta(1) = 32$, we have

$$G_4 = \langle g, h : g^{33} = h^2 = 1, hgh^{-1} = g^{32} \rangle$$

□

Problem 8.2. Let $F \subset K$ be an algebraic extension of fields. Let $F \subset R \subset K$ where R is a F-subspace of K with the property such that $\forall a \in R$, $a^k \in R$ for all $k \geq 2$.

(1) Assume that $\text{char}(F) \neq 2$. Show that R is a subfield of K.

(2) Give an example such that R may not be a field if $\text{char}(F) = 2$.

Proof. I will only do (1), because I can't do (2). It suffices to show that R is closed under multiplication and taking inverses. Let $a, b \in R$, we know

$$(a+b)^2 \in R \Rightarrow a^2 + b^2 + 2ab \in R \Rightarrow ab \in R$$

Since $F \subset K$ is algebraic, for any $a \in R$, there exists a minimal polynomial $p_a(t)$ such that

$$p_a(a) = c_0 + c_1 a + \cdots + c_n a^n = 0$$

Multiplying both sides by a^{-n} and equating we get

$$c_0 a^{-n} + \cdots + c_n = c_0 + c_1 a + \cdots + c_n a^n$$

i.e.,

$$c_0 a^{-n} = c_0 + c_1 a + \cdots + c_n a^n - c_n - \cdots - c_1 a^{-(n-1)}$$

multiplying both sides by a^{n-1}, we see that $a^{-1} \in R$, as desired. □

Problem 8.3. Determine the Galois group of $x^6 - 10x^3 + 1$ over $\mathbb{Q}$.

Proof. Solving for the roots we see the splitting field for this polynomial is

$$\mathbb{Q}(\sqrt{5+2\sqrt{6}}, \sqrt{3}i)$$

which has degree 12, i.e., the order of the Galois group. Let

$$\begin{cases} \alpha_1 = \sqrt{5+2\sqrt{6}} \\ \beta_1 = \sqrt{5-2\sqrt{6}} \\ \alpha_2 = e^{\frac{2\pi i}{3}}\sqrt{5+2\sqrt{6}} \\ \beta_2 = e^{\frac{2\pi i}{3}}\sqrt{5-2\sqrt{6}} \\ \alpha_3 = e^{\frac{4\pi i}{3}}\sqrt{5+2\sqrt{6}} \\ \beta_3 = e^{\frac{4\pi i}{3}}\sqrt{5-2\sqrt{6}} \end{cases}$$

We see that there are two choices for $\alpha_1 \mapsto \alpha_i, \beta_j$ for any i, j. This gives a group of order 12 and by drawing a hexagon (or by guessing), one can conclude that this is D_{12}. □

Problem 8.4. Let V and W be two finite dimensional vector spaces over a field K. Show that for any $q > 0$,

$$\bigwedge^q (V \oplus W) \cong \sum_{i=0}^{q} (\bigwedge^i (V) \otimes_K \bigwedge^{q-i} (W)).$$

Proof. Any two finite dimensional vector spaces of the same dimension are isomorphic. Hence, it suffices to show that the dimensions are equal. We will convince ourselves it holds for $q = 2$. Let $\{v_1, \ldots, v_n\}$ be the basis of V, and $\{w_1, \ldots, w_k\}$ be the basis of W, then we begin with the LHS:

$$\bigwedge^2 (V \oplus W)$$

We note that $V \oplus W$ has basis

$$\{(v_i, w_j) : 1 \le i \le n, 1 \le j \le k\}$$

So we reenumerate the $n + k$ basis as

$$\{e_1, \ldots, e_{n+k}\}$$

Then $\bigwedge^q(V \oplus W)$ has basis

$$\{e_i \wedge e_j : i < j\}$$

There are exactly $1 + \cdots + (n + k - 1)$ basis vectors i.e.,

$$\dim\left(\bigwedge^2(V \oplus W)\right) = \frac{(n+k-1)(n+k)}{2}$$

As for the RHS:

$$\dim\left(\sum_{i=0}^{2}(\bigwedge^i(V) \otimes_K \bigwedge^{2-i}(W))\right) \frac{(k-1)k}{2} + nk + \frac{(n-1)n}{2}$$

And we observe that two two quantities are equal. Now we do the general case, just like above,

$$\dim\left(\bigwedge^q(V \oplus W)\right) = \binom{n+k}{q}$$

And the RHS:

$$\dim\left(\bigwedge^{q-1}(V \oplus W) \wedge (V \oplus W)\right) = \sum_{i=0}^{q}\binom{n}{i}\binom{k}{q-i}$$

and it is clear that these two quantities are equal.

□

Problem 8.5. Prove that a finite dimensional algebra over a field is a division algebra if and only if it does not have zero divisors.

Proof. Recall a finite dimensional algebra is a ring with a field action, and it is a division algebra if every nonzero element $a \in A$ has an $a^{-1} \in A$. We know A does not have a zero divisor if and only if for any $a \in A$, the multiplication map by a is injective. Since A is a finite dimensional vector space as well, an injective map is necessarily surjective, i.e., multiplication by a is surjective, this happens if and only if a is a unit, i.e., A is a division algebra. □

Problem 8.6. Let A be a semi-simple finite dimensional algebra over $\mathbb{C}$, and let V be a direct sum of two isomorphic simple A-modules. Find the automorphism group of the A-module V.

Proof. Schur's lemma says that if S is a simple A-module, then

$$\mathrm{End}(S, S) \cong \mathbb{C}$$

Thus

$$\mathrm{End}(V, V) = \mathrm{Mat}_2(\mathbb{C})$$

Thus the automorphisms are

$$\mathrm{Aut}(V, V) = \mathrm{GL}_2(\mathbb{C})$$

□

Chapter 9

Spring 2015

2,3,4,5,6

Problem 9.1. Let K be a field of characteristic $p > 0$. Prove that a polynomial $f(x) = x^p - x - a \in K[x]$ either irreducible, or is a product of linear factors. Find this factorization if f has a root $x_0 \in K$.

Proof. We first prove that if f has a root x_0, then f factors into linear factors over K. Suppose x_0 is a root of f, then we claim that

$$f(x_0 + k) = 0$$

for any $k \in K$. This is because

$$\begin{aligned} f(x_0 + k) &= x_0^p + k - x_0 - k - a \\ &= k^p - k \\ &= 0 \end{aligned}$$

Since $K = \mathbb{F}_p$ for some prime p. Thus f can be factored completely as

$$f(x) = (x - x_0)(x - (x_0 + k_1)) \dots (x - (x_0 + k_{p-1}))$$

Conversely, we show that if f doesn't have a root, then f is irreducible. Suppose that $f(x) = g(x)h(x)$, where g, h are irreducible over K and have degree strictly less than f. Now we consider the Galois closure L of f, suppose $\alpha \in L$ such that

$$f(\alpha) = 0 \Rightarrow g(\alpha) = 0 \text{ or } h(\alpha) = 0$$

WLOG, we suppose that $g(\alpha) = 0$. Then just like the above, we have $\alpha + k$ as a root of g as well, for any $k \in K$. This shows that

$$g(x) = (x - \alpha)(x - (\alpha + k_1)) \dots (x - (\alpha + k_{p-1}))$$

over L. This shows that g has degree p, which is a contradiction. □

Problem 9.2. Let A, B be two commuting operators on a finite dimensional space V over $\mathbb{C}$ such that $A^n = B^m$ is the identity operator on V for some positive integers n, m. Prove that V is a direct sum of 1-dimensional invariant subspaces with respect to A and B simultaneously.

Proof. Since $A^n = B^m = 1I$, then the minimal polynomial of A divides $x^n - 1$, and minimal polynomial of B divides $x^m - 1$. This shows both A, B are diagonalizable. Since A, B commute, we know we can diagonalize A, B simultaneously: Let E_λ be an eigenspace of A, then B can be diagnoalized in E_λ, because eigenvectors of B in E_λ are also eigenvectors of A. This shows A, B have a common eigenbasis, i.e., V can be decomposed into 1-dimensional eigenspaces for A, B simultaneously. □

Problem 9.3. Let G be a finite p-group. Determine all irreducible representations of G over a field K of characteristic p.

Proof. We claim that the only irreducible representation is the trivial one. Let $|G| = p^d$, then let $\rho : G \to \mathrm{GL}_n(K)$ be an irreducible representation, this is an action of G on $\mathbb{F}_p^n$, by the Orbit-Stabilizer theorem, the size of the orbit is either 1 (trivial) or divides p. Since there is a trivial orbit, let N denote the size of orbits of size 1, we know

$$N - 1 \equiv 0 \mod p$$

This shows there is at least one nontrivial orbit of size 1, let v be the element in this orbit. Then the vector space W generated by v is also fixed under the action of G. Since W is a one-dimensional subspace of $\mathbb{F}_p^n$ that is fixed by G, we must have ρ be one-dimensional, and

$$\rho(g)(w) = w$$

for any $w \in W$, thus ρ is the trivial representation. □

Problem 9.4. Prove that the polynomial x^4+1 is not irreducible over any field of positive characteristic.

Proof. We note the extension generated by $x^4 + 1$ is $\mathbb{Q}(\sqrt{2}, i)$, thus it suffices to show for $\mathbb{F}_p$ where p is any prmie p, we must have either $\sqrt{2} \in \mathbb{F}_p$ or $i \in \mathbb{F}_p$ or $\sqrt{2}i \in \mathbb{F}_p$. We see f is clearly reducible over $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(i)$, and it is also reducible over $\mathbb{Q}(\sqrt{2}i)$ because if it were irreducible, then the degree of extension $\mathbb{Q}(\sqrt{2}, i)$ would be 8, which is a contradiction. Now for any $\mathbb{F}_p^\times$, we have the Legendre homomorphism:

$$\chi(g) = \begin{cases} 1, g \text{ is a square} \\ -1, g \text{ is not a sqaure} \end{cases}$$

Hence assume 2 or -1 are not squares, then -2 must be a square:

$$\chi(2)\chi(-1) = \chi(-2) = 1$$

Thus $\sqrt{2}i$ must be in $\mathbb{F}_p$, hence f is reducible. □

Problem 9.5. Prove that a tensor product of irreducible representations over an algebraically closed field is irreducible.

Proof. Let ρ_1, ρ_2 be irreducible representations of G_1, G_2, then we define its tensor product $\rho_1 \otimes \rho_2 : G_1 \times G_2 \to \mathrm{GL}(V_1 \otimes V_2)$. Similarly, the characters are defined as

$$\chi_1 \otimes \chi_2(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$$

For an algebraically closed field, it suffices to show the tensor character has norm 1.

$$\begin{aligned} \langle \chi_1 \otimes \chi_2, \chi_1 \otimes \chi_2 \rangle &= \frac{1}{|G_1||G_2|} \sum_{(g_1,g_2)} \chi_1(g_1)\chi_2(g_2)\overline{\chi_1(g_1)\chi_2(g_2)} \\ &= \frac{1}{|G_1||G_2|} |G_1|\langle \chi_1, \chi_1 \rangle |G_2|\langle \chi_2, \chi_2 \rangle \\ &= 1 \end{aligned}$$

□

Problem 9.6. Let D be an algebra over a field K of characteristic $\neq 2$ generated by two elements i, j satisfying relations

$$i^2 = 1, j^2 = 1, ij = -ji.$$

Prove, that $D \simeq GL_2(K)$.

Proof. The isomorphism is given by

$$\varphi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \varphi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \varphi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

One can check this is indeed an isomorphism. □

Chapter 10

Fall 2014

2

Problem 10.1. (a) Let S_n be the symmetric group (permutation group) on n objects. Prove that if $\sigma \in S_n$ is an n-cycle and $\tau \in S_n$ is a transposition (i.e., a 2-cycle), then σ and τ generate S_n.

(b) Let $f_a(x)$ be the polynomial $x^5 - 5x^3 + a$. Determine an integer a with $-4 \leq a \leq 4$ for which f_a is irreducible over $\mathbb{Q}$, and the Galois group of [the splitting field of] f_a over $\mathbb{Q}$ is S_5. Then explain why the equation $f_a(x) = 0$ is not solvable in radicals.

Proof. (a) It suffices to assume that the n cycle is $(1 \dots n)$ (up to rearranging the terms), and the transposition is (12). One can show that conjugation gives all the transpositions, hence generate S_n.

(b) Take $a = 1$, then $f_a(x)$ is irreducible: it doesn't have a root by the Rational Root Theorem and cannot be factored into lower degree polynomial by term matching. Moreover, we see that $f_a'(x)$ has 3 roots, by Rolle's theorem, there are at most 4 real roots, this implies that there exists a complex root r_1, and since this has odd degree, it must also exist a real root r_2. This shows that there exists an element in the Galois group that has order 5 and a transposition (sending conjugate complex roots to each other). Thus by (a), since the Galois group is a subgroup of S_5, we must have it equal to S_5.

□

Problem 10.2. Let $R = \mathbb{Q}[X]$, I and J the principal ideals generated by $X^2 - 1$ and $X^3 - 1$ respectively. Let $M = R/I$ and $N = R/J$. Express in simplest terms [the isomorphism type of] the R-modules $M \otimes_R N$ and $\mathrm{Hom}_R(M, N)$. **Explain.**

Proof. This is tensor product over fields question, finally! We have

$$\begin{aligned} M \otimes_{\mathbb{Q}[x]} N &= \frac{\mathbb{Q}[x]}{(X^2-1)} \otimes_{\mathbb{Q}[x]} \frac{\mathbb{Q}[x]}{(X^3-1)} \\ &= \frac{\mathbb{Q}[x]}{(\gcd(X^2-1) + (X^3-1))} \\ &= \frac{\mathbb{Q}[x]}{(x-1)} \\ &= \mathbb{Q} \end{aligned}$$

□

Problem 10.3. Let $G = S_3$.

(a) Prove that G has an irreducible complex representation of dimension 2,—call it ρ—but none of higher dimension.

(b) Decompose $\rho \otimes \rho \otimes \rho$ (as a representation of G) into a direct sum of irreducible representations.

Proof. (a) S_3 has three conjugacy classes, i.e., 3 irreducible representations, the only way to write $|S_3| = 6$ as a sum of 3 squares is $1 + 1 + 4$, which implies that there exists a irred rep of dimension 2, and not any higher.

(b) We know that

$$\chi\left[(\rho \otimes \rho \otimes \rho)(g)\right] = \left(\chi(\rho(g))\right)^3$$

Thus with some trial and error, if we want to write

$$\rho \otimes \rho \otimes \rho = \sum \chi_{\text{triv}} \cdots \oplus \chi_{\text{sgn}} \cdots \oplus \rho \ldots \rho$$

Then we need to send

$$\rho \otimes \rho \otimes \rho(g) = \begin{cases} 8, g = e \\ 0, g = (12) \\ -1, g = (123) \end{cases}$$

Thus we see that

$$\rho \otimes \rho \otimes \rho = \chi_{\text{triv}} \oplus \chi_{\text{sgn}} \oplus \rho \oplus \rho \oplus \rho$$

□

Problem 10.4. (a) Let G be a group of order p^2q^2, where p and q are distinct odd primes, with $p > q$. Show that G has a normal subgroup of order p^2.

(b) Can a solvable group contain a non-solvable subgroup? **Explain.**

Proof. (a) n_p can only be 1 or q^2, if $n_p = q^2$, then

$$p \mid (q^2 - 1) = (q + 1)(q - 1)$$

i.e., p divides $q + 1$ or $q - 1$, which are both even, which is a contradiction. This implies $n_p = 1$.

(b) Let H be a subgroup of G, where G is solvable. Then there exists a sequence

$$\{e\} = G_0 \subset G_1 \subset \ldots G_n = G$$

such that each G_i is normal in G_{i+1} and G_{i+1}/G_i is abelian/cyclic. If we take

$$H_i = G_i \cap H$$

then one can show that

$$\{e\} = H_0 \subset \cdots \subset H_n = H$$

is a sequence satisfying the above condition, i.e., H is solvabla.

□

Problem 10.5. (a) Prove that every group of order p^2 (p a prime) is abelian. Then classify such groups up to isomorphism.

(b) Give an example of a non-abelian group of order p^3 for $p = 3$. **Suggestion**: Represent the group as a group of matrices.

Proof. (a) We know any nontrivial p-group has a nontrivial center, thus either $Z(G) = p$ or $Z(G) = p^2$. We are done in the latter case. If $Z(G) = p$, then

$$G/Z(G) \text{is cyclic}$$

which implies G is again abelian, hence we must have $Z(G) = p^2$, as desired.

(b) The Heisenburg group over $\mathbb{F}_3$.

□

Chapter 11

Spring 2014

1,2,3

Problem 11.1. Find the number of colouring of faces of a cube in 3 colours. Two colourings are equal if they are the same after a rotation of the cube. [Hint Use the Burnside formula

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|,$$

where a group G acts on a set X, X/G is the set of orbits, and, for every $g \in G$, X^g is the fixed subset of g in X.]

Problem 11.2. Proof that all groups of order < 60 are solvable.

Problem 11.3. Let L/K be a Galois extension of degree p with char$K = p$. Show that $L = K(\theta)$, where θ is a root of $x^p - x - a, a \in K$, and, conversely, any such extension is Galois of degree 1 or p.

Problem 11.4. Proof that a finite dimensional associative algebra over a field is a division algebra if and only if it has no zero divisors.

Proof. A division algebra is one such every nonzero element is a unit. Let $a \in \mathcal{A}$ be any element in the algebra. We have the following equivalences:

$$\begin{aligned} a \text{ is not a zero divisor} &\iff \text{multiplication by } a \text{ is injective} \\ &\iff \text{multiplication by } a \text{ is surjective since} V \text{ is finite-dim} \\ &\iff a \text{ is a unit} \\ &\iff \mathcal{A} \text{ is a division algebra} \end{aligned}$$

□

Problem 11.5. Find the table of characters for S_4.

Proof.

Class	[1]	[(12)(34)]	[(123)]	[(1234)]	
Size	1	6	3	8	6
$\chi^{(1)}$	1	1	1	1	1
$\chi^{(2)}$	1	-1	1	1	-1
$\chi^{(3)}$	2	0	2	-1	0
$\chi^{(4)}$	3	1	-1	0	-1
$\chi^{(5)}$	3	-1	-1	0	1

□

Chapter 12

Fall 2011

Problem 12.1. (a) Let G be a group of order 5046. Show that G cannot be a simple group. You may not appeal to the classification of finite simple groups.

(b) Let p and q be prime numbers. Show that any group of order p^2q is solvable.

Proof. (a) $5046 = 29^2 \cdot 2 \cdot 3$, we must have $n_{29} = 1$. This shows G is not simple.

(b) There are two cases: $p < q$ and $p > q$. When $p < q$, we if $n_q = p^2$ then $n_p = 1$, thus when $n_p = q$, we have $n_q = 1$. In other words, you either have a normal group of order p^2 or q, and both cases are solvable. When $p > q$, then $n_q = 1$, also solvable.

□

Problem 12.2. Consider the special orthogonal group $G = SO(3, \mathbb{R})$, namely,

$$G = \{A \in GL(3, \mathbb{R}) : A^T A = \mathrm{I}_3, \det(A) = 1\}$$

(a) Show that for any element A in G, there exists a real number α with $-1 \leq \alpha \leq 3$ such that

$$A^3 - \alpha A^2 + \alpha A - \mathrm{I}_3 = 0.$$

(b) For which real numbers α with $-1 \leq \alpha \leq 3$ does there exist an element A in G whose minimal polynomial is $x^3 - \alpha x^2 + \alpha x - 1$? Explain your answer.

Proof. This question is quite computational, and I will not list all the computations here.

(a) Writing A in a general form, we see that

$$\alpha = \mathrm{tr}(A)$$

Thus it sufficees to compute the eigenvalues of A (in the algebraic closure). One can show that it takes the above form using the size of these eigenvalues.

(b) It is when there are distinct three eigenvalues, i.e., $\alpha \neq -1, 3$.

□

Problem 12.3. Let G be a cyclic group of order 100. Let $K = \mathbb{Q}$, the field of rational numbers, or $K = F_p$, the finite field with p elements, p being a prime number. For each such K, construct a Galois extension L/K whose Galois group $\mathrm{Gal}(L/K)$ is isomorphic to G. Explain your construction in detail.

Proof. First we do $K = \mathbb{F}_p$. Let E be the splitting field of $(x^{p^{100}} - x)$, then by definition E is Galois, we see $\mathbb{F}_p \subset E$ (so it is an extension) because if $a \in \mathbb{F}_p$,

$$a^p = a \Rightarrow (a^{p^{100}} - a) = 0$$

Thus $\mathbb{F}_p \subset E$. Now E is a degree 100 extension of $\mathbb{F}_p$, i.e., $|\text{Gal}(E/\mathbb{F}_p)| = 100$. Now by the following lemma, we are done.

Lemma 12.1. Let $\mathbb{F}_p \subset E = \mathbb{F}_{p^n}$ be a Galois extension, then the Galois group is cyclic, i.e., is $\mathbb{Z}/n\mathbb{Z}$.

This is because the Frobenius map

$$F : a \mapsto a^p$$

has order n, therefore is a generator of $\text{Gal}(E/\mathbb{F}_p)$.

Now let $K = \mathbb{Q}$. We claim that $\mathbb{Q}(\zeta_{101})$ is a Galois extension with

$$\text{Gal}(\mathbb{Q}(\zeta_{101})/\mathbb{Q}) = \frac{\mathbb{Z}}{100\mathbb{Z}} = G$$

It is easy to see that $\mathbb{Q}(\zeta_{101})/\mathbb{Q}$ is Galois, and

$$\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$$

Since 101 is prime, we know the Galois group $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times = \frac{\mathbb{Z}}{100\mathbb{Z}}$, as desired. (We will do the more general case where cyclic G such that $|G| \neq p - 1$ and when G is abelian in the notes). □

Problem 12.4. Let $\rho : S_3 \to \mathbb{C}^2$ be a two-dimensional irreducible representation of the symmetric group S_3. Decompose $\rho^{\otimes 2}$ and $\rho^{\otimes 3}$ into a direct sum of irreducible representations of S_3.

Proof. Let ρ_e, ρ_s, ρ denote the trivial, sign, 2-dimensional representations of S_3, then Using the fact that

$$\text{Tr}(\rho \otimes \rho) = (\text{Tr}(\rho))^2, \text{Tr}(\rho \otimes \rho \otimes \rho) = (\text{Tr}(\rho))^3$$

we see

$$\rho \otimes \rho = \rho_e \oplus \rho_s \oplus \rho$$

and similarly,

$$\rho \otimes \rho \otimes \rho = \rho_e \oplus \rho_s \oplus \rho \oplus \rho \oplus \rho$$

□

Problem 12.5. Let A be a finite-dimensional semisimple algebra over $\mathbb{C}$, and V an A-module of finite type (i.e., finitely-generated as an A-module). Prove that V has only finitely many A-submodules if and only if V is a direct sum of pairwise non-isomorphic irreducible (i.e., simple) A-modules.

Proof. If V is a finite direct sum of non-isomorphic A-modules, then there are only finitely many A-submodules (for each simple module, the only submodule is $\{e\}$ and itself).

Conversely, suppose that there are isomorphic copies of A module in the sum of V, by Schur's lemma, we know

$$\text{End}(S, S) = \mathbb{C}$$

Thus if $V = S \oplus S$, then for fixed ϕ,

$$\{(x, \phi(x)) \in (S, S)\}$$

is a submodule. Since there are infiniteyly many ϕ, there are infinitely many submodules. □

Chapter 13

Spring 2010

Problem 13.1. Let G be a non-abelian group of order p^3, here p is prime. Determine the number of distinct conjugacy classes in G.

Proof. We know that G has nontrivial and abelian, this forces the center $Z(G)$ to have order p. Then we take any $g \in G \setminus Z(G)$, then consider the centralizers (stabilizers of g), denoted as $Z_g(G)$, then

$$Z(G) \subset Z_g(G) \subset G$$

Since $Z_g(G)$ is a proper subgroup of G strictly containing $Z(G)$, we must have $|Z_g(G)| = p^2$. By the Orbit-Stabilizer theorem, the conjugacy class of $g \in G \setminus Z(G)$ has size p, thus the number of conjugacy classes other than the center is

$$(p^3 - p)/p = p^2 - 1$$

and each element in $Z(G)$ is its own conjugacy class, i.e., the total number is

$$p^2 + p - 1$$

□

Problem 13.2. Let R be a ring such that $r^3 = r$ for all $r \in R$. Show that R is commutative. (Hint: First show that r^2 is central for all $r \in R$.)

Proof. This question is not so informative and quite computational, so I will skip here. □

Problem 13.3. Compute Galois groups of the following polynomials.

(a) $x^3 + t^2x - t^3$ over k, where $k = \mathbb{C}(t)$ is the field of rational functions in one variable over complex numbers $\mathbb{C}$.

(b) $x^4 - 14x^2 + 9$ over $\mathbb{Q}$.

(a) The polynomial is homogeneous and solving for the roots we take $x = at$ for some $a \in \mathbb{C}$, then we see $x = at$ is a root if and only if

$$a^3 + a - 1 = 0$$

since $\mathbb{C}$ is algebraically closed, we know that there are 3 roots in $\mathbb{C}$, i.e., $x^3 + t^2x - t^3$ completely factors over $\mathbb{C}(t)$. This implies that the Galois group is the trivial group.

(b) Solving for the roots, they are

$$\left\{\pm\sqrt{7+2\sqrt{10}}, \pm\sqrt{7-2\sqrt{10}}\right\} := \{\pm\alpha, \pm\beta\}$$

We note that $\alpha\beta = 3$, hence there are only four elements of the Galois group:

$$\begin{cases} \alpha \mapsto \alpha, \beta \mapsto \beta \\ \alpha \mapsto -\alpha, \beta \mapsto -\beta \\ \alpha \mapsto \beta, \beta \mapsto \alpha \\ \alpha \mapsto -\beta, \beta \mapsto -\alpha \end{cases}$$

In other words, the each element is completely determined by where α is sent to. Thus we see the group is

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Problem 13.4. Let V be a n-dimensional vector space over a field k. Let $T \in \text{End}_k(V)$.

(a) Show that $tr(T \otimes T \otimes T) = (tr(T))^3$. Here $tr(T)$ is the trace of T.

(b) Find a similar formula for the determinant $\det(T \otimes T \otimes T)$.

Proof. (a) We will show that $\text{tr}(T \otimes T) = (\text{tr}T)^2$, and the $T \otimes T \otimes$ is done similarly. We will use matrix representation to do an explicit computation. Let $\{v_1, \ldots, v_n\}$ be a basis of$V$, then $V \otimes V$ has basis

$$\{v_i \otimes v_j : 1 \leq i, j \leq n\}$$

and

$$T \otimes T(v_i \otimes v_j) = Tv_i \otimes Tv_j$$

Let $T = (a_{ij})$, then we know

$$(\text{tr}(T))^2 = \left(\sum_{i=1}^{n} a_{ii}\right)^2$$

And we have

$$T \otimes T(v_i \otimes v_j) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{ki}a_{lj}v_k \otimes v_l$$

Therefore computing the trace we see

$$\text{tr}(T \otimes T) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ii}a_{jj} = \text{tr}(T)^2$$

as desired!

(b) It suffices to figure out this formula by looking at diagonalizable matrices, where $\det(T) = \prod_{i=1}^{n} \lambda_i$, then it is easy to see that

$$\det(T \otimes T) = (\det(T))^{2n}$$

where n is the dimension. and three times is the same process

$$\det(T \otimes T \otimes T) = (\det(T))^{3n^2}$$

□

Problem 13.5. Classify all non-commutative semi-simple rings with 512 elements. (You can use the fact that finite division rings are fields.)

Proof. By Artin-Wedderburn, we know that this finite semisimple ring can be decomposed into a finite direct sum of matrix rings:

$$R \cong M_{n_1}(F_1) \oplus \cdots \oplus M_{n_k}(F_k)$$

where F_i are finite fields. Further more we can assume $n_1 \geq n_2 \geq \cdots \geq n_k$.The total number of elements is

$$F_1^{n_1^2} \dots F_k^{n_k^2} = 512 = 2^9$$

Thus we see all the components are powers of 2. Since R is noncommutative, we may assume that $n_1 \geq 2$. If $n_1 = 3$, then $F_1 = 2$, we have

$$R \cong M_3(\mathbb{F}_2)$$

If $n_1 = 2$, we can have $n_2 = 2$, then

$$R \cong M_2(\mathbb{F}_2) \oplus M_2(\mathbb{F}_2) \oplus \mathbb{F}_2$$

or $n_3 = \cdots = n_k = 1$, then we have (different ways of adding to 5):

$$R \cong M_2(\mathbb{F}_2) \oplus \begin{cases} \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus F_2 \\ \mathbb{F}_4 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \oplus F_2 \\ \mathbb{F}_8 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2 \\ \mathbb{F}_{16} \oplus \mathbb{F}_2 \\ \mathbb{F}_8 \oplus \mathbb{F}_4 \\ \mathbb{F}_{16} \oplus F_2 \\ \mathbb{F}_{32} \end{cases}$$

□

Problem 13.6. Let G be a group with 24 elements. **Use representation theory** to show that $G \neq [G, G]$. (Here $[G, G]$ is the commutator subgroup of G.)

Proof. Let $\rho : G \to \mathbb{C}^\times$ be a one-dimensional representation, then $[G, G] \subset \ker(\rho)$, if $G = [G, G]$, then ρ must be trivial. However, we cannot write

$$|G| = 24 = 1 + d_1^2 + \cdots + d_k^2$$

where $d_i \geq 2$, hence this is a contradiction. □

Chapter 14

Fall 2007

Problem 14.1. Let G be a cyclic group of order 12. Construct a Galois extension K over $\mathbb{Q}$ so that the Galois group is isomorphic to G.

Proof. Since $12 = 13 - 1$, we know how to construct Galois group

$$(\mathbb{Z}/13\mathbb{Z})^\times = \mathbb{Z}/12\mathbb{Z}$$

The Galois extension is $\mathbb{Q}(\zeta_{13})$, where ζ_{13} is the 13th root of unity. □

Problem 14.2. Prove that no group of order 148 is simple.

Proof. We see that

$$148 = 2^2 \cdot 37$$

Thus $n_{37} = 1$. □

Problem 14.3. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a real matrix such that $a, b, c, d > 0$.

(1) Prove that A has two distinct real eigenvalues, $\lambda > \mu$.

(2) Prove that λ has an eigenvector in the first quadrant and μ has an eigenvector in the second quadrant.

Proof. (1) The eigenvalues are as follows

$$\frac{(a+d) \pm \sqrt{(a-d)^2 + bc}}{2}$$

Thus there are two distinct eigenvalues that are both real.

(2) It suffices to plug in λ, μ:

$$\begin{cases} ax_1 + by_1 - \lambda x_1 = 0 \\ cx_1 + by_1 - \lambda x_2 = 0 \end{cases}$$

We see that

$$y_1 = \frac{\lambda - a}{b} x_1$$

We see that $\lambda > a$, hence x_1, y_1 have the same sign, i.e., it has an eigenvector in the first quadrant. Similarly, plugging in μ we see that μ has an eigenvalue in the second quadrant.

□

Problem 14.4. A differentiation of a ring R is a mapping $D : R \to R$ such that, for all $x, y \in R$,

(1) $D(x + y) = D(x) + D(y)$; and

(2) $D(xy) = D(x)y + xD(y)$.

If K is a field and R is a K-algebra, then its differentiation are supposed to be over K, that is,

(3) $D(x) = 0$ for any $x \in K$.

Let D be a differentiation of the K-algebra $M_n(K)$ of $n \times n$-matrices. Prove that there exists a matrix $A \in M_n(K)$ such that $D(X) = AX - XA$ for all $X \in M_n(K)$.

Proof. It suffices to consider basis elements of M_{ij},

$$A = \sum_{i,j} D(M_{ij})E_{ji}$$

and one can check $D(X) = AX - XA$ holds. □

Problem 14.5. Prove the existence of a 1-dimensional invariant subspace for any 5-dimensional representation of the group A_4 (the alternating group of degree 4).

Proof. The 4 conjugacy classes in A_4 are

$$e, (12)(34), (123), (132)$$

We now find the one-dimensional representation by observing

$$\frac{A_4}{(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})} \cong \mathbb{Z}/3\mathbb{Z}$$

And we know the character table for $\mathbb{Z}/3\mathbb{Z}$, thus combining and using orthogonality relations, we get

Class size	1	4	3	4
Representative	()	(123)	(12)(34)	(132)
χ_1	1	1	1	1
χ_2	1	ζ_3	1	ζ_3^2
χ_3	1	ζ_3^2	1	ζ_3
χ_4	3	0	-1	0

□

Chapter 15

Spring 2007

Problem 15.1. Prove that the integer orthogonal group $O_n(\mathbb{Z})$ is a finite group. (By definition, an $n \times n$ square matrix X over $\mathbb{Z}$ is orthogonal if $XX^t = I_n$.)

Proof. Let $A \in O_n(\mathbb{Z})$, since $\det(A) = \pm 1$ and all entries are integers, we can only have one nonzero entry ± 1 in every row, this matrix is necessarily invertible and has $\det = \pm 1$. There a total of

$$2^n \cdot n!$$

of choices of place ± 1 such that each row has one nonzero entry. This shows that O_n is a finite group. □

Problem 15.2. Prove that no group of order 224 is simple.

Proof. We have $224 = 2^5 \cdot 7$, thus $n_7 = 1, 8$ and $n_2 = 1, 7$. If $n_2 = n_7 = 1$, then we are done. Suppose $n_2 = 7$, then G acts on the Sylow 2 subgroups, i.e., there exists a map

$$\varphi : G \to S_7$$

If $\ker(\varphi) \neq \{e\}$, then $\ker(\varphi)$ is a nontrivial normal subgroup ($\ker(\varphi) \neq G$ becuase this action is transitive and nontrivial), and we are done. Thus it suffces to rule out $\ker(\varphi) = \{e\}$, in this case φ is an embedding, i.e., $|G|$ must divide $|S_7$ but this is false thus a contradiction. □

Problem 15.3. Write down the irreducible polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible modulo p for every prime p.

Proof. Note this question is exactly the same S2017-Q2. The minimal polynomial p_m is

$$p_m(t) = (t^2 - 5)^2 - 24 = t^4 - 10t^2 + 1$$

The roots are $\pm\sqrt{2} \pm \sqrt{3}$, thus this polynomial generates a field extension of $\mathbb{Q}$,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \frac{\mathbb{Q}[t]}{(p_m(t))}$$

We claim that it suffices to show that $\sqrt{2}$ or $\sqrt{3}$ or $\sqrt{6}$ are in $\mathbb{F}_p$ for any prime p. Take $\sqrt{2} \in \mathbb{F}_p$ for example, we know $p_m(t)$ is not irreducible over $\mathbb{Q}(\sqrt{2})$, because then it would mean the degree of field extension

$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$ is 8, which is a contradiction.

$$\begin{array}{c}\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \uparrow\\ \mathbb{Q}(\sqrt{2})\\ \uparrow\\ \mathbb{Q}\end{array}$$

Thus $p_m(t)$ is reducible over $\mathbb{Q}(\sqrt{2})$. Now we show the following.

Lemma 15.1. For any prime p, $\sqrt{2}$ or $\sqrt{3}$ or $\sqrt{6}$ are in $\mathbb{F}_p$ for any prime p.

There exists a homomorphism (Legendre symbol) $\varphi : \mathbb{F}_p^\times \to \{\pm 1\}$, such that

$$\varphi(g) = \begin{cases} 1, \text{ if } g \text{ is a square} \\ -1, \text{ otherwise} \end{cases}$$

Suppose that $2, 3$ are not squares, i.e., $sqrt2, \sqrt{3} \notin \mathbb{F}_p^\times$, then

$$\varphi(2 \cdot 3) = 1$$

which implies $\sqrt{6} \in \mathbb{F}_p^\times$, concluding the proof. □

Problem 15.4. Find the invertible elements, the zero divisors and the nilpotent elements in the following rings:

(a) $\mathbb{Z}/p^n\mathbb{Z}$, where n is a natural number, p is a prime.

(b) the upper triangular matrices over a field.

Proof. I will denote the invertible elements as I, zero divisors as ZD and nilpotent elements are N.

(a) For $\mathbb{Z}/p^n\mathbb{Z}$,

$$I(\mathbb{Z}/p^n\mathbb{Z}) = (\mathbb{Z}/p^n\mathbb{Z})^\times$$

we know the invertible elements are exactly the ones coprime to p^n: for any a, there exists integers b, k such that

$$ab + nk = 1$$

if and only if $\gcd(p^n, a) = 1$.

$$ZD(\mathbb{Z}/p^n\mathbb{Z})(= \mathbb{Z}/p^n\mathbb{Z}) \setminus I$$

The ring is commutative and finite, if g is not a unit, then it implies multiplication by g is also not injective, i.e., g is a zero divisor.

$$N(\mathbb{Z}/p^n\mathbb{Z}) = \{g \in \mathbb{Z}/p^n\mathbb{Z} : g \equiv 0 \mod p\}$$

This is because if $g^k = 0 \mod p^n$ for some k, then $g^k = 0 \mod p \Rightarrow p \mid g^k$. Since p is prime, we must have $p \mod g$, i.e., $N \subset \{g : g \equiv 0 \mod p\}$, and it is clear the reverse inclusion holds.

(b) The invertible elements

$$I = \{A \in M_n(k) : a_{ii} \neq 0 \text{ for all } 1 \leq i \leq n\}$$

The zero divisors:

$$ZD = M_n(k) \setminus I$$

by a dimension argument. And finally

$$N = \{A \in M_n(k) : a_{ii} = 0 \text{ for all } 1 \leq i \leq n\}$$

One can easily show both inclusions by explicit matrix computations.

□

Problem 15.5. Prove that the group $\mathrm{GL}(2, \mathbb{C})$ does not contain a subgroup isomorphic to S_4.

Proof. We know that S_4 embeds into $\mathrm{GL}_2(\mathbb{C})$ if and only if there exists a homomorphism $\varphi : G \to \mathrm{GL}_2(\mathbb{C})$ such that φ is injective. By definition, φ is a representation, and we know there are one irreducible representations of dimension 2 and two irreducible representations of dimension 1. We know the character table of S_4, recall the following lemma:

Lemma 15.2. Let $\rho \to \mathrm{GL}_n(\mathbb{C})$ be a representation, if for some g,

$$\chi(\rho(g)) = n$$

then $\rho(g) = I_n$. In other words, if there is an entry in the character table that is the same as its left most entry (dimension), then it is (the trace of)the identity matrix.

By the character table of S_4

S_4	(1)	(12)	(123)	(1234)	$(12)(34)$
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1
$\chi_{\perp}$	3	1	0	-1	-1
$\text{sgn} \otimes \chi^{\perp}$	3	-1	0	1	-1
$\chi^{(5)}$	2	0	-1	0	2

We see that the two-dimensional representation $\chi^{(5)}$ is not injective, since $\chi^{(5)}(12)(34) = 2$. It suffices to show that if the direct sum of two one-dimensional representations is also not injective:

$$\chi_{\text{triv}} \oplus \chi_{\text{sgn}}(12)(34) = 1 + 1$$

i.e., it is not injective. This shows that S_4 cannot be embedded into $\mathrm{GL}_2(\mathbb{C})$. □