Algebra Qualifying Exam Solutions

(Accuracy Not Guaranteed)

Hui Sun

April 29, 2025

Contents

Chapter 1

Spring 2017

Problem 1.1. 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 1.1. 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 1.2. 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 1.2. 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 1.3. 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 1.4. 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 1.5. 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 1.6. 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 2

Fall 2016

Problem 2.1. 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 2.2. 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 2.3. 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 2.4. (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 2.5. 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 2.6. 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 3

Spring 2016

I can't do 6

Problem 3.1. 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 3.1. 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 3.2. 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 3.3. 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 3.4. 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

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

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 3.5. 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 3.6. 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.

Chapter 4

Fall 2011

2,4,5

Problem 4.1. (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 4.2. 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).

□

Problem 4.3. 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 4.1. 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 4.4. 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.

Problem 4.5. 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.

Chapter 5

Spring 2007

Problem 5.1. 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 5.2. 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 5.3. 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 5.1. 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 5.4. 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 5.5. 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 5.2. 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 $\mathrm{GL}_2(\mathbb{C})$. □