

Algebra Qual Spring 2016

Problem 1

Statement (10 points). Let

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix} \in M_3(\mathbb{C}).$$

(a) Find the Jordan canonical form J of A .

(b) Find an invertible matrix P such that $P^{-1}AP = J$. (You do not need to compute P^{-1} .)

Solution. (a) After some careful computation we find

$$\chi_A(x) = -x^3 + 5x^2 - 8x + 4 = -(x-1)(x-2)^2.$$

Then

- we can conclude we have a block of size 1 or 1
- either two blocks of size one for 2 or one block of size 2, and it just depends on how many chains we have, so we just need to check the rank of $A - 2$.

We have

$$A - 2 = \begin{bmatrix} -5 & 3 & -2 \\ -7 & 4 & -3 \\ 1 & -1 & 0 \end{bmatrix}$$

Then we can see this has rank two because the last two columns are not multiples of one another (last column has a 0 in last coordinate so can't be scaled to get a 1 there like the 2nd has) and the first column is the last minus the second.

Then the kernel has size 1 so we have only one chain and the JCF is

$$\begin{bmatrix} 1 & & \\ & 2 & 1 \\ & & 2 \end{bmatrix}.$$

(b) We'll need a rank 2 eigenvector for 2 so we'll have to compute $(A - 2)^2$. This will be

$$(A - 2)^2 = \begin{bmatrix} 2 & -1 & 1 \\ 4 & -2 & 2 \\ 2 & -1 & 1 \end{bmatrix}$$

Then an obvious rank 2 is $(0, 1, 1)$ since the last column is the negation of the second and this vector clearly isn't in the kernel of $(A - 2)$. Then

$$(A - 2) \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}$$

so this is our eigenvector. It remains to compute an eigenvector for 1. We have

$$A - 1 = \begin{bmatrix} -4 & 3 & -2 \\ -7 & 5 & -3 \\ 1 & -1 & 1 \end{bmatrix}$$

Then an easy eigenvector is $(1, 2, 1)$ so

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & -1 & 1 \end{bmatrix}.$$

□

Problem 2

Statement (10 points). Let $K = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.

- (a) Find $[K : \mathbb{Q}]$.
- (b) Show that $K/\mathbb{Q}$ is Galois, and find the Galois group G of $K/\mathbb{Q}$.
- (c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K .

Solution. (a) There are a few approaches we could take here.

1. Compute the minimal polynomial of $\sqrt{2} + \sqrt{5}$. We can do this by letting $x = \sqrt{2} + \sqrt{5}$ and performing algebraic operations until we get something with purely rational coordinates.

$$\begin{aligned} x &= \sqrt{2} + \sqrt{5} \\ x^2 &= 2 + 2\sqrt{10} + 5 \\ x^2 - 7 &= 2\sqrt{10} \\ (x^2 - 7)^2 &= 40 \\ (x^2 - 7)^2 - 40 &= 0 \\ x^4 - 14x^2 - 9 &= 0 \end{aligned}$$

is then a relation annihilating the element we adjoined so it is certainly divisible by the min poly. If you can show its irreducible then we can see that the field has degree 4.

2. This is the solution I like. You can notice that $K = \mathbb{Q}[\sqrt{2} + \sqrt{5}] \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and try to show they are actually equal. A few ways to do this

1. Show that one of $\sqrt{2}, \sqrt{5}$ is in K . You can do this by finding a linear combination of the two with unequal coefficients. You can expand $(\sqrt{2} + \sqrt{5})^3$ using the binomial theorem to do this.
2. You can notice that $(\sqrt{2} + \sqrt{5})(\sqrt{2} - \sqrt{5}) = 2 - 5 = -3$ is rational thus $\sqrt{2} + \sqrt{5} = -\frac{3}{\sqrt{2} + \sqrt{5}} \in K$ hence $\sqrt{2} + \sqrt{5} + \sqrt{2} - \sqrt{5} = 2\sqrt{2} \in K$ and so also $\sqrt{5}$ is in K . This is nice.
3. You can just classify the subfields of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ and show that $\sqrt{2} + \sqrt{5}$ doesn't live in any proper one. This kinda solves the whole problem at once.

Lets expand on (1) first. We have

$$\begin{aligned} (\sqrt{2} + \sqrt{5})^3 &= (\sqrt{2})^3 + 3\sqrt{2} \cdot (\sqrt{5})^2 + 3(\sqrt{2})^2 \cdot \sqrt{5} + (\sqrt{5})^3 \\ &= 2\sqrt{2} + 15\sqrt{2} + 6\sqrt{5} + 5\sqrt{5} \\ &= 17\sqrt{2} + 11\sqrt{5}. \end{aligned}$$

Then

$$17\sqrt{2} + 11\sqrt{5} - 11(\sqrt{2} + \sqrt{5}) = 6\sqrt{2}$$

hence $\sqrt{2} \in K$ and thus also $\sqrt{5} \in K$.

Let's suppose we've used either one or (2) to show $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and continue on. Then note that $x^2 - 5$ is irreducible in $\mathbb{Q}(\sqrt{2})$ (it has none of its roots there) so $[K : \mathbb{Q}(\sqrt{2})] = 2$. Similarly $x^2 - 2$ is irred over $\mathbb{Q}$ so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Then

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

so part (a) is done.

(b) This extension is Galois since it is the smallest field where

$$(x^2 - 2)(x^2 - 5)$$

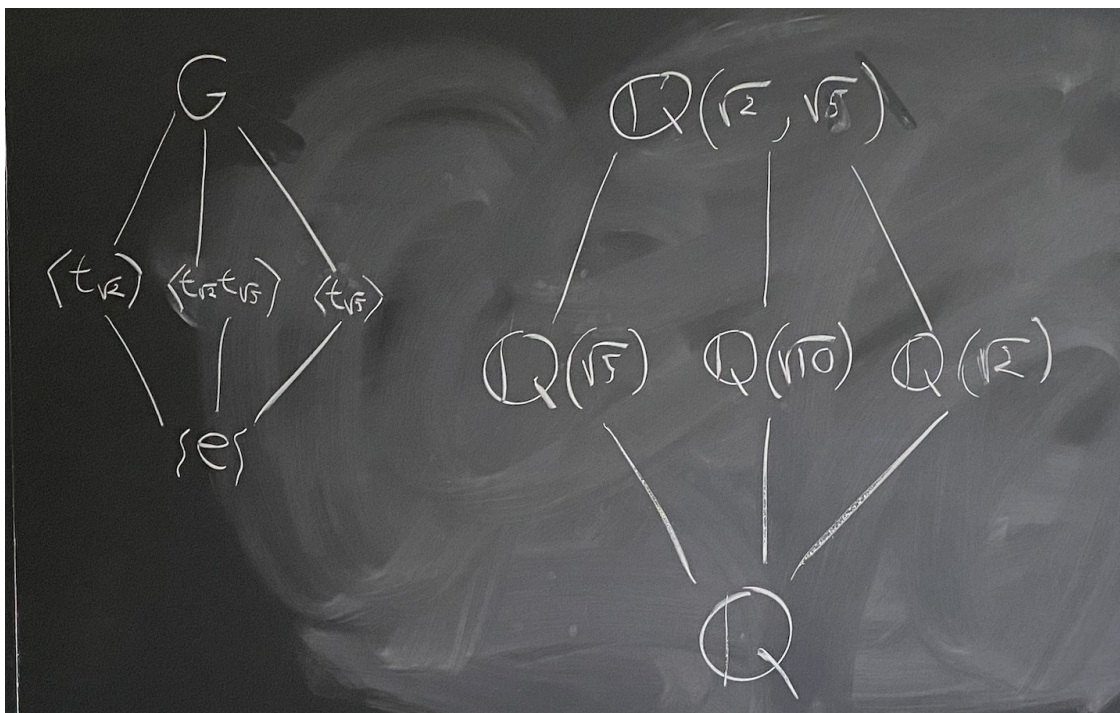
splits.

From the Galois correspondence $|G| = [K : \mathbb{Q}] = 4$ so it is a transitive subgroup of S_4 of size 4. Then it is either $V_4 = C_2 \times C_2$ or C_4 . We will show it is V_4 . Indeed consider again the irreducible polynomials

$$\begin{aligned} x^2 - 5 &= (x - \sqrt{5})(x + \sqrt{5}) \\ x^2 - 2 &= (x - \sqrt{2})(x + \sqrt{2}). \end{aligned}$$

Let $\phi \in G$. Since ϕ has to send roots to roots all it can do is swap or fix each of $\sqrt{5}, \sqrt{2}$ thus it must have order 2. Then G is certainly not cyclic since all its elements have order 2 so it must be V_4 . In particular it is generated by $t_{\sqrt{5}}$ which swaps $\sqrt{5}$ and fixes $\sqrt{2}$ and $t_{\sqrt{2}}$ which fixes $\sqrt{5}$ and swaps $\sqrt{2}$.

(c)



□

Problem 3

Statement (10 points). (a) State the three Sylow theorems.

(b) Prove that any group of order 1225 is abelian.

(c) Write down exactly one representative in each isomorphism class of (abelian) groups of order 1225.

Solution. (a)

Sylow I (existence): Let G be a group of order mp^k where $p \nmid m$. Then there exists a group $P \leq G$ of order p^k . These are the sylow p -subgroups of G .

Sylow II (p groups are conjugate): If $P, Q \leq G$ are sylow p -subgroups then there is a $g \in G$ such that

$$P = gQg^{-1}.$$

Sylow III: Let n_p denote the number of sylow p -groups of G . Then $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$.

(b) Note the prime factorization. $1225 = 5^2 \cdot 7^2$. I did this recently. See *Algebra Spring 2018*. The jist of the argument is you get normal 5 and 7 sylow subgroups thus the group is a semidirect product of them. Being groups of order p^2 they are abelian, and since both are normal the groups commute with each other so the entire group is abelian.

(c) By the fundamental theorem of finitely generated abelian groups we have the following

isomorphism classes

$$\begin{aligned} &C_7 \times C_7 \times C_5 \times C_5 \\ &C_{7^2} \times C_5 \times C_5 \\ &C_{7^2} \times C_{5^2} \\ &C_7 \times C_7 \times C_{5^2}. \end{aligned}$$

□

Problem 4

Statement (10 points). Let R be a ring with the following commutative diagram of R -modules (each row represents a short exact sequence of R -modules).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

Prove that if α and γ are isomorphisms then β is an isomorphism.

Solution. We can do a diagram chase.

Injective: Suppose $\beta(b) = 0$. Then

$$\gamma \circ g(b) = g' \circ \beta(b) = g'(0) = 0.$$

Since γ is injective then $g(b) = 0$ so that $b \in \ker g = \operatorname{im} f$. Then write $f(a) = b$. We then have

$$0 = \beta(b) = \beta \circ f(a) = f' \circ \alpha(a).$$

Since f' is injective $\alpha(a) = 0$. But then since α is injective $a = 0$ so that $f(a) = f(0) = b = 0$.

Surjective: This one is a bit more wordy. Don't get lost in the setup.

- Let $b' \in B'$ so that $g'(b') \in C'$.
- Since γ is surjective we can take $c \in C$ such that $\gamma(c) = g'(b')$.
- Since g is surjective we can take $b \in B$ so that $g(b) = c$. Then

$$\gamma \circ g(b) = g' \circ \beta(b)$$

so that $g'(\beta(b)) = b'$ i.e. $g'(\beta(b) - b') = 0$. Then

$$\beta(b) - b' \in \ker g' = \operatorname{im} f'.$$

Then there is $a' \in A'$ so that $f'(a') = \beta(b) - b'$. Since α is surjective there is $a \in A$ so that $\alpha(a) = a'$. Then

$$f' \circ \alpha(a) = \beta \circ f(a) = \beta(b) - b'.$$

Then $\beta(f(a) - b) = b'$ and β is surjective.

□

Problem 5

Statement (10 points). Let G be a finite group acting on a set X . For $x \in X$, let G_x be the stabilizer of x , and $G \cdot x$ be the orbit of x .

(a) Prove that there is a bijection between the left cosets G/G_x and $G \cdot x$.

(b) Prove that the center of every finite p -group G is non-trivial by considering the action of G on $X = G$ by conjugation.

Solution. (a) We define the map $f : G/G_x \rightarrow G \cdot x$ by

$$f(kG_x) = k \cdot x.$$

Well defined: Suppose $kG_x = hG_x$. Then $h = kg$ for $g \in G_x$. Then

$$f(hG_x) = h \cdot x = kg \cdot x = k \cdot (g \cdot x) = k \cdot x = f(kG_x).$$

Injective: suppose

$$f(hG_x) = h \cdot x = k \cdot x = f(kG_x).$$

Then $hk^{-1} \cdot x = x$ so $hk^{-1} \in G_x$ thus the cosets are equal.

Surjective: Every $y \in G \cdot x$ is of the form $k \cdot x$ for some k . Then $f(kG_x) = k \cdot x = y$.

(b) I also just did this in *Algebra Spring 2018*. Act by conjugation, the fixed points are precisely things in the center. When acting by a p -group fixed points are congruent to size of set which in this case is the group which has order a power of p , thus size of center is a multiple of p . It has the identity so its non-zero thus must have size at least p . $\square$

Problem 6

Statement (10 points). Let K be a Galois extension of a field F with $[K : F] = 2015$. Prove that K is an extension by radicals of the field F .

Problem 7

Statement (10 points). Let $D = \mathbb{Q}[x]$ where $\mathbb{Q}$ are the rational numbers and let M be a $\mathbb{Q}[x]$ -module such that

$$M \cong \frac{\mathbb{Q}[x]}{(x-1)^3} \oplus \frac{\mathbb{Q}[x]}{(x^2+1)^3} \oplus \frac{\mathbb{Q}[x]}{(x-1)(x^2+1)^5} \oplus \frac{\mathbb{Q}[x]}{(x+2)(x^2+1)^2}.$$

Determine the elementary divisors and invariant factors of M .

Solution. Using chinese remainder theorem we can split this up as

$$\frac{\mathbb{Q}[x]}{(x-1)^3} + \frac{\mathbb{Q}[x]}{(x^2+1)^3} + \frac{\mathbb{Q}[x]}{(x-1)} + \frac{\mathbb{Q}[x]}{(x^2+1)^5} + \frac{\mathbb{Q}[x]}{(x+2)} + \frac{\mathbb{Q}[x]}{(x^2+1)^2}.$$

Then the above is primary decomposition and the moduli are the primary factors.

The invariant decomposition is

$$\frac{\mathbb{Q}[x]}{(x^2+1)^5(x-1)^3(x+2)} + \frac{\mathbb{Q}[x]}{(x^2+1)^3(x-1)} + \frac{\mathbb{Q}[x]}{(x^2+1)^2}$$

and these are the invariant factors. $\square$

Problem 8

Statement (10 points). Let R be a simple rng (a nonzero ring which is not assumed to have a 1, whose only two-sided ideals are $\{0\}$ and R) satisfying the following two conditions:

- (i) R has no zero-divisors; and
- (ii) if $0 \neq x \in R$ then $2x \neq 0$ (where $2x := x + x$).

Prove the following:

- (a) For each $x \in R$ there is one and only one element $y \in R$ such that $x = 2y$.
- (b) Suppose $x, y \in R$ such that $x \neq 0$ and $2(xy) = x$. Then $yz = zy$ for all $z \in R$.

[You can get partial credit for part (b) if you do it assuming R has a 1.]

Solution. (a) First we show uniqueness. Suppose $x = 2y = 2y'$. Then

$$2y - 2y' = 2(y - y') = 0.$$

Then we must have $y - y' = 0$ since otherwise twice it could not be zero by (ii). Of course then $y = y'$.

Now for existence. Consider the ideal

$$2R = \{2r : r \in R\}.$$

This is an ideal

$$2r - 2r' = 2(r - r')$$

and it is two sided since “2” commutes

$$r(2r') = r(r' + r') = rr' + rr' = 2(rr').$$

Then since R has no proper two sided ideals we must have $2R = R$ thus for $x \in R$ we have $x \in 2R$ thus $x = 2y$ for some $y \in R$.

(b) Let $e = 2y$. Then

$$(2(xy) = x) \iff (x \cdot e = x).$$

Then also

$$x(ex - x) = x^2 - x^2 = 0$$

so $ex - x = 0$ since R has no zero divisors. Now to show $yz - zy = 0$ it suffices to show that $2yz - 2zy = 0$ since $2x = 0$ iff $x = 0$. Then we want to show that $ez - ze = 0$. Indeed

$$x(ez - ze)x = (xz - xze)x = xzx - xzx = 0.$$

Then $ez - ze$ is a zero divisor so must be 0 hence $ze = ez$ as desired. □