

Algebra Qual Spring 2018

Problem 1

Statement (10 points). **(a)** Use the Class Equation (equivalently, the conjugation action of a group on itself) to prove that any p -group (a group whose order is a positive power of a prime integer p) has a nontrivial center.

(b) Prove that any group of order p^2 (where p is prime) is abelian.

(c) Prove that any group of order $5^2 \cdot 7^2$ is abelian.

(d) Write down exactly one representative in each isomorphism class of groups of order $5^2 \cdot 7^2$.

Solution. **(a)** Suppose $|P| = p^n$, and let P on a finite set X . Recall that for $x \in X$

$$O_x = \{g \cdot x : g \in P\}.$$

If $O_x = \{x\}$ then $g \cdot x = x$ for all $g \in P$ i.e. the orbit has size 1 iff x is a fixed point of the action. Now let $F = \{y_1, y_2, \dots, y_m\}$ be the fixed points and $O = \{x_1, x_2, \dots, x_k\}$ be distinct representatives for the orbits with size > 1 . Then since the orbits partition the set

$$X = \bigsqcup_{i=1}^m \{y_m\} \sqcup \bigsqcup_{j=1}^k O_{x_j}$$

which implies

$$\begin{aligned} |X| &= \left| \bigsqcup_{i=1}^m \{y_m\} \right| + \left| \bigsqcup_{j=1}^k O_{x_j} \right| \\ &= |X^P| + \sum_{j=1}^k |O_{x_j}| \end{aligned}$$

where X^P denotes the fixed points of the action of P . Now by orbit stabilizer for each x_j we have

$$p^n = |P| = |P_{x_j}| \cdot |O_{x_j}|$$

so $|O_{x_j}| \mid p^n$. Then since $|O_{x_j}| > 1$ it must be a non-trivial power of p . That is $|O_{x_j}| = p^{n_j}$ for $n_j > 1$. Then we have

$$|X| = |X^P| + \sum_{j=1}^k p^{n_j}$$

and taking this equation mod p yields

$$|X| \equiv |X^P| \pmod{p}.$$

Now let P act on itself by conjugation. Then from the above we have

$$p^n \equiv |P| \equiv |P^P| \equiv 0 \pmod{p}.$$

Then p divides the number of fixed points. The fixed points of this action are precisely the things in the center. Then $e \in Z(P)$ so $|Z(P)| > 1$ and is divisible by p thus must be at least p and therefore is non-trivial.

(b) Suppose P has order p^2 . By (a) P has a non-trivial center $Z(P)$ which has order p or p^2 . If $|Z(P)| = p^2$ then $Z(P) = P$ and were done so suppose not. Consider that $P/Z(P)$ has order p thus is cyclic generated by some coset gP for $g \in P$. Then since the cosets partition the group every element is of the form $g^i n$ for $i \in [p]$ and $n \in Z(P)$. Then suppose $a, b \in P$. Write $a = g^i n_a$ and $b = g^j n_b$. Then since n_a, n_b are in the center and powers commute ($g^i \cdot g^j = g^{i+j} = g^j \cdot g^i$) we have

$$ab = g^i n_a g^j n_b = g^j n_b \cdot g^i n_a = ba.$$

(c) Suppose G has order $5^2 \cdot 7^2$. Then by the 3rd sylow theorem

$$n_5 \mid 7^2, \text{ and } n_5 \equiv 1 \pmod{5}$$

$$n_7 \mid 5^2, \text{ and } n_7 \equiv 1 \pmod{7}$$

Then $n_5 \in \{1, 7, 49\}$ and taking this mod 5 we see that $n_5 = 1$. Similarly $n_7 \in \{1, 5, 25\}$ and taking this mod 7 we see we must have $n_7 = 1$. Since the conjugate of a sylow subgroup is another sylow subgroup the only way this can happen is if the unique sylow 7-subgroup is normal, and the unique 5-sylow subgroup are normal. Let P be the normal 7-sylow and Q the normal 5-sylow.

Then since the orders are coprime $P \cap Q = \{e\}$ and we get $|PQ| = |P| \cdot |Q| = 7^2 \cdot 5^2$, thus

$$PQ = G.$$

It remains to show this product is abelian. First note that since P and Q are abelian (groups of order p^2) and all elements of PQ are of the form ab for $a \in P, b \in Q$ it suffices to show the element of P commute with the elements of Q . Indeed consider

$$aba^{-1}b^{-1}.$$

Since Q is normal $aba^{-1} \in Q$ and since $b^{-1} \in Q$ we have $aba^{-1}b^{-1} \in Q$. Similarly since P is normal $ba^{-1}b^{-1} \in P$ and $aba^{-1}b^{-1} \in P$ thus

$$aba^{-1}b^{-1} \in Q \cap P = \{e\}$$

so it must be equal to e and thus $ab = ba$ as desired.

(d) By the fundamental theorem of finitely generated abelian groups we have the following isomorphism classes

$$C_7 \times C_7 \times C_5 \times C_5$$

$$C_{7^2} \times C_5 \times C_5$$

$$C_{7^2} \times C_{5^2}$$

$$C_7 \times C_7 \times C_{5^2}.$$

□

Problem 2

Statement (10 points). Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

- (a) Find the splitting field K of f , and compute $[K : \mathbb{Q}]$.
- (b) Find the Galois group G of f , both as an explicit group of automorphisms, and as a familiar abstract group to which it is isomorphic.
- (c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K .

Solution. (a) We have

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

Let $u = \sqrt{2 + \sqrt{2}}$. We claim

$$K = \mathbb{Q}(u).$$

Indeed since u is a root of f certainly $\mathbb{Q}(u) \subseteq K$ so it suffices to show that $\mathbb{Q}(u)$ contains all the roots of $f(x)$, or rather that $v := \sqrt{2 - \sqrt{2}} \in \mathbb{Q}(u)$. Indeed consider the product

$$uv = \sqrt{(2 - \sqrt{2})(2 + \sqrt{2})} = \sqrt{4 - 2} = \sqrt{2}.$$

Then $v = u^{-1}\sqrt{2} \in \mathbb{Q}(u)$ so indeed $\mathbb{Q}(u)$ is the splitting field of K .

Now as a vector space of $\mathbb{Q}$ the map $x \mapsto u$ is an isomorphism

$$\frac{\mathbb{Q}[x]}{\langle f(x) \rangle} \cong \mathbb{Q}(u)$$

and since $\mathbb{Q}[x]/\langle f \rangle$ has dimension $\deg f = 4$ as a vector space over $\mathbb{Q}$ (the set $\{1, x, x^2, x^3\}$ is a basis) we see that

$$[\mathbb{Q}(u) : \mathbb{Q}] = \deg f = 4.$$

(b) Abstractly since G acts transitively on the roots of f it is a subgroup of S_4 . By the Galois correspondence

$$|G| = [K : \mathbb{Q}] = 4$$

so it is a transitive subgroup S_4 thus either C_4 or V_4 . We claim it is C_4 . It suffices to find an element of order 4 in G . Since the action is transitive there is an automorphism ϕ sending $u \mapsto v$. We will show this element has order 4. Indeed since

$$\sqrt{2} = u^2 - 2$$

we have that

$$\phi(\sqrt{2}) = \phi(u)^2 - 2 = v^2 - 2 = -\sqrt{2}.$$

Then

1. $\phi(u) = v = \sqrt{2}u^{-1}$
2. So $\phi(v) = \phi(\sqrt{2})\phi(u)^{-1} = -\sqrt{2}v^{-1} = -u$
3. And $\phi(-u) = -\phi(u) = -v$
4. Finally $\phi(-v) = -\phi(v) = -(-u) = u$.

So ϕ has order 4 and generates the entire Galois group.

(c) There is only one subgroup of G namely C_2 generated by ϕ^2 . The corresponding intermediate extension is the fixed field of ϕ^2 namely $\mathbb{Q}(\sqrt{2})$. $\square$

Problem 3

Statement (10 points). Let K be a Galois extension of $\mathbb{Q}$ with Galois group G , and let E_1, E_2 be intermediate fields of K which are the splitting fields of irreducible $f_i(x) \in \mathbb{Q}[x]$. Let $E = E_1E_2 \subset K$. Let $H_i = \text{Gal}(K/E_i)$ and $H = \text{Gal}(K/E)$.

- (a) Show that $H = H_1 \cap H_2$.
- (b) Show that H_1H_2 is a subgroup of G .
- (c) Show that $\text{Gal}(K/(E_1 \cap E_2)) = H_1H_2$.

Solution. This is about composite fields. They might not ask us about this since we didn't really discuss them.

(a) Recall that E is generated by products of the form uv where $u \in E_1, v \in E_2$. Then an automorphism fixes the field E iff it fixes all such products. Then if $\phi \in H_1 \cap H_2$ it certainly fixes all such products since it fixes E_1, E_2 . Now for the converse note that $E_1, E_2 \subseteq E$ by definition (consider all the products $u \cdot 1$ and $1 \cdot v$) so if $\phi \in H$ since it fixes E it must fix E_1, E_2 as well.

(b) From the Galois correspondence $E_i/\mathbb{Q}$ is Galois iff H_i is normal in G . Then since E_i is a splitting field for an irreducible it is Galois over $\mathbb{Q}$ so each H_i is normal. Then a product of groups is a group precisely when one of the groups is normal. Since both H_i are normal then H_1H_2 is certainly a group.

(c) Let $\phi \in H_1, \psi \in H_2$ so that $\phi\psi \in H_1H_2$. Then if $u \in E_1 \cap E_2$ certainly it is fixed by both automorphisms so it is fixed by the product

$$\phi\psi(u) = \phi(u) = u.$$

For the other inclusion recall that if E/K is Galois then the only elements in E fixed by the entire Galois group $\text{Gal}(E/K)$ are the elements of the base field $\text{Fix Gal}(E/K) = K$. To see this recall that the Galois group acts transitively on the roots of minimal polynomials so if $u \in E$ has a min poly of degree > 1 then we may find an automorphism taking u to the other root of that minimal polynomial.

Now suppose $u \in \text{Fix}(H_1H_2)$. Since $H_i \subseteq H_1H_2$ and E/E_i is Galois we see that u is fixed by H_i and thus must lie in the corresponding base field E_i . Then $u \in E_1 \cap E_2$ as desired. $\square$

Problem 4

Statement (10 points). Let

$$A = \begin{pmatrix} 0 & 1 & -2 \\ 1 & 1 & -3 \\ 1 & 2 & -4 \end{pmatrix} \in M_3(\mathbb{C}).$$

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

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

Solution. (a) After a careful calculation we get

$$\chi_A(x) = -(x^3 + 3x^2 + 3x + 1) = -(x+1)^3$$

the last equality is just coming from recognizing this as the binomial expansion of $(x+1)^3$. Then to determine the JCF we just need to know how many chains we have. Then

$$A + 1 = \begin{bmatrix} 1 & 1 & -2 \\ 1 & 2 & -3 \\ 1 & 2 & -3 \end{bmatrix}$$

so this has column rank 2 since the 3rd column is the negation of the sum of the first two. Then we only have one chain so the JCF is just

$$\begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix}$$

(b) We need to compute the square.

$$(A + 1)^2 = \begin{bmatrix} 0 & -1 & 4 \\ 0 & -3 & 1 \\ 0 & -3 & 1 \end{bmatrix}$$

The cube should be zero so for our rank 3 generalized eigenvector we can take $(0, 0, 1)$. Then our rank 2 will be $(4, 1, 1)$, and our rank 1 (our genuine eigenvector) will be $(3, 3, 3)$ so our P is

$$\begin{bmatrix} 0 & 4 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 3 \end{bmatrix}$$

□

Problem 5

Statement (10 points). Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $N = \begin{pmatrix} x & u \\ -y & -v \end{pmatrix}$ over a commutative ring R ,

where b and x are units of R . Prove that if $MN = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}$, then $MN = 0$.

Solution. Lets compute this.

$$MN = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & u \\ -y & -v \end{pmatrix} = \begin{pmatrix} ax - by & au - bv \\ cx - dy & cu - dv \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix}$$

so

$$ax = by$$

$$au = bv$$

$$cx = dy$$

and we want to show that $cu = dv$. Solving the relations for y and v we have

$$y = xab^{-1}, \text{ and } v = uab^{-1}.$$

Then our matrix N has a more obvious dependency in its columns

$$N = \begin{pmatrix} x & u \\ -xab^{-1} & -uab^{-1} \end{pmatrix}$$

Then they are both multiples of the vector $(1, -ab^{-1})$. Then it suffices to check that the row vector $[c \ d]$ annihilates this vector. Indeed we're given that it annihilates x times this vector and x is a unit so we may conclude it annihilates this vector

$$\begin{aligned} (c, d) \cdot (1, -ab^{-1}) x &= (c - dab^{-1}) x = 0 \\ \iff (c - dab^{-1}) &= 0 \end{aligned}$$

Then indeed

$$\begin{aligned} (c, d) \cdot (u, -v) &= (c, d) \cdot (u, -uab^{-1}) \\ &= (c, d) \cdot (1, ab^{-1}) u \\ &= 0 \cdot u = 0 \end{aligned}$$

so $MN = 0$ as desired. □

Problem 6

Statement (10 points). Let $M = \{(w, x, y, z) \in \mathbb{Z}^4 \mid w + x + y + z \in 2\mathbb{Z}\}$, and $N = \{(w, x, y, z) \in \mathbb{Z}^4 \mid 4 \mid (w - x), 4 \mid (x - y), 4 \mid (y - z)\}$.

(a) Show that N is a $\mathbb{Z}$ -submodule of M .

(b) Find vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ and integers d_1, d_2, d_3, d_4 such that $\{u_1, u_2, u_3, u_4\}$ is a free basis for M , and $\{d_1 u_1, d_2 u_2, d_3 u_3, d_4 u_4\}$ is a free basis for N .

(c) Find vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ and integers d_1, d_2, d_3, d_4 such that $\{u_1, u_2, u_3, u_4\}$ is a free basis for M , and $\{d_1u_1, d_2u_2, d_3u_3, d_4u_4\}$ is a free basis for N .

(d) Use the previous part to describe M/N as a direct sum of cyclic $\mathbb{Z}$ -modules.

Problem 7

Statement (10 points). Let R be a PID and M be an R -module. Let p be a prime element of R . The module M is called $\langle p \rangle$ -primary if for every $m \in M$ there exists $k > 0$ such that $p^k m = 0$.

(a) Suppose M is $\langle p \rangle$ -primary. Show that if $m \in M$ and $t \in R, t \notin \langle p \rangle$, then there exists $a \in R$ such that $atm = m$.

(b) A submodule S of M is said to be pure if $S \cap rM = rS$ for all $r \in R$. Show that if M is $\langle p \rangle$ -primary, then S is pure if and only if $S \cap p^k M = p^k S$ for all $k \geq 0$.

Solution. (a) Recall that PIDs are UFD thus have a well defined notion of GCD. Now if $t \notin \langle p \rangle$ then t is coprime to p thus also coprime to any power of p . Suppose $p^k m = 0$. Since t and p^k are coprime there are $x, y \in R$ such that

$$(ty + p^k x = 1) \iff (yt = 1 - p^k x).$$

Then

$$ytm = (1 - p^k x)m = m - xp^k m = m - 0 = m$$

so we may take $a := y$ to satisfies the condition.

(b) I feel like I need to unpack this still. When does this actually happen?

- $S \cap rM = rS$. Is one inclusion here just always true? Yes $rS \subseteq S \cap rM$ no matter what since S is a submodule $rS \subseteq S \subseteq M$, and $rS \subseteq rM$ as sets.
- So the goal is to show the converse happens exactly when $S \cap p^k M = p^k S$. I.e. it suffices to check it for special submodules when M is p -primary.
- Oh and one direction of this iff is also easy. If S is pure then applying the statement to $r := p^k$ yields $S \cap p^k M = p^k S$.
- Then the only thing we need to check is that if M is p -primary and $S \cap p^k M = p^k S$ for all $k \geq 0$ then S is pure.
- First consider the case r coprime to p . Then we can apply part (a). Suppose $u \in S \cap rM$. Then there is $m \in M$ such that $u = rm$

Suppose again that M is p -primary. First note that $rS \subseteq S \cap rM$ regardless of whether or not S is pure as S is a submodule. Then the claim reduces to

$$(S \cap rM \subseteq rS, \text{ for all } r \in R) \iff (S \cap p^k M \subseteq p^k S, \text{ for all } k \geq 0)$$

Then note that the $\implies$ direction is obvious so it suffices to check $\impliedby$.

First consider the case $r \notin \langle p \rangle$, and let $u = rm \in S \cap rM$. Then there is $a \in R$ such that $r(au) = u = rm \in rS$ since $au \in S$ as S is a module.

Now suppose $r \in \langle p \rangle$. Then $r = tp^k$ for $t \notin \langle p \rangle$, and $k \geq 1$, and thus $rM \subseteq p^k M$ so that

$$S \cap rM \subseteq S \cap p^k M \subseteq p^k S.$$

Remark. If we take the primary decomposition of M what this is really saying is

$$M \cong \bigoplus_{i=1}^m \frac{R}{\langle p^{m_i} \rangle}$$

i.e. the only prime in the decomposition is p .

□

Problem 8

Statement (10 points). Let $R = C[0, 1]$ be the ring of continuous real-valued functions on the interval $[0, 1]$. Let I be an ideal of R .

- (a) Show that if $f \in I$, $a \in [0, 1]$ are such that $f(a) \neq 0$, then there exists $g \in I$ such that $g(x) \geq 0$ for all $x \in [0, 1]$, and $g(x) > 0$ for all x in some open neighborhood of a .
- (b) If $I \neq R$, show that the set $Z_I = \{x \in [0, 1] \mid f(x) = 0, \text{ all } f \in I\}$ is nonempty.
- (c) Show that if I is maximal, then there exists $x_0 \in [0, 1]$ such that $I = \{f \in R \mid f(x_0) = 0\}$.

Solution. (a) First note that since f is continuous it is non-zero in some neighborhood of a .

$$(f \text{ CTS}) \implies (\exists \delta > 0 : |f(a) - f(x)| < \epsilon, \text{ for all } x \in (a - \delta, a + \delta)).$$

I.e. $f(x) \in (f(a) - \epsilon, f(a) + \epsilon)$. Then so long as $\epsilon < f(a)$ we obtain the necessary neighborhood. Since $f(x)$ is non-zero in this neighborhood so is its square $f(x)^2$. Then its square is also in the ideal since f is and squares are non-negative everywhere so we're done.

(b) This is actually kind of cool.

Suppose $Z_I = \emptyset$. Then by part (a) for each $a \in [0, 1]$ there is an open neighborhood $U_a \subseteq [0, 1]$ of a and a continuous function $f_a(x) \in I$ such that $f_a \geq 0$ and $f_a \upharpoonright U_a > 0$. Then the U_a form an open cover of $[0, 1]$ so there is a finite subcover $\{U_{a_i}\}_{i=1}^n$. Now let $f(x) = \sum_{i=1}^n f_{a_i}(x)$. Then f is strictly positive on $[0, 1]$. To see this suppose $a \in [0, 1]$. Then since the U_{a_i} form a cover $a \in U_{a_i}$ for some i . Then since each f_{a_i} is non-negative

$$f(a) \geq f_{a_i}(a) > 0, \text{ since } f_{a_i} \text{ is positive on } U_{a_i}.$$

Then $f(x) \in I$ is a unit since it is non-zero on all of $[0, 1]$ thus $I = R$.

(c) Suppose I is maximal. Then since it is proper by (b) there is $x_0 \in [0, 1]$ such that $f(x_0) = 0$ for all $f \in I$. Now consider the set

$$J = \{f \in R : f(x_0) = 0\}.$$

This is an ideal since if $f, g \in J$ then $(f - g)(x_0) = f(x_0) - g(x_0) = 0$, and if $f \in J, g \in R$ we have $(fg)(x_0) = f(x_0)g(x_0) = 0 \cdot g(x_0) = 0$. Now J is also a proper ideal since for example the constant function 1 is not in J . Then clearly $I \subseteq J$, and since both are proper and I is maximal $I = J$ as desired. □