Algebra Qual Spring 2015

Problem 1

Statement. For a prime p, let G be a finite p-group, and let N be a normal subgroup of G of order p. Prove that N is contained in the center of G.

Solution. Since N is normal we may let G act on N by conjugation. Then since G is p-group acting on a set we have

$$|N| = \left|N^G\right| \bmod p$$

i.e. size of N is congruent to its number of fixed points mod p. Then $|N| = p$ so

$$\left|N^G\right| \equiv 0 \bmod p.$$

Now $e \in N$ is a fixed point of conjugation so $\left|N^G\right| \neq 0$. Then $\left|N^G\right| \geq p$. But then $\left|N^G\right|$ is at most all of N which has size p so every point of N is fixed point under conjugation. Then the fixed points of conjugation are just elements of the center (orbit size 1 means $gng^{-1} = n$ which implies $gn = ng$ for all $g \in G$) so N lies in the center. □

Problem 2

Statement. Let F be a finite field.

(a) Give, with proof, the decomposition of the additive group $(F, +)$ into a direct sum of cyclic groups.

(b) The exponent of a finite group is the least common multiple of the orders of its elements. Prove that a finite abelian group has an element of order equal to its exponent.

(c) Prove that the multiplicative group $(F^\times, \cdot)$ is cyclic.

Solution. **(a) Proof 1:** Let $(\mathbb{F}, +)$ be the additive group of a finite field of order p^n. Then it is finite a $\mathbb{Z}$-module and thus has a primary decomposition

$$\mathbb{F} = \bigoplus_{i=1}^{m} \frac{\mathbb{Z}}{\left\langle p_i^{a_i} \right\rangle}, \text{ where } p_i \neq 0 \text{ is prime.}$$

Now since $\mathbb{F}$ has characteristic p every element has additive order p exactly. Then each $\mathbb{Z}/\left\langle p_i^{a_i} \right\rangle$ being a subgroup also has elements only order p. Then this is true iff $p_i = p$ and $a_i = 1$ thus the primary decomposition simplifies to

$$\mathbb{F} = \bigoplus_{i=1}^{m} \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

Proof 2:
Let $\mathbb{F}$ be a finite. Then it has order p^n for some prime p and is a degree n extension of $\mathbb{F}_p$. Let $\{v_1, \ldots, v_n\}$ be a basis for $\mathbb{F}$ over $\mathbb{F}_p$. Then $\mathbb{F}$ is a sum of the modules

$$\mathbb{F} = \bigoplus_{i=1}^{n} \langle v_i \rangle \cong \bigoplus_{i=1}^{n} \frac{\mathbb{Z}}{p\mathbb{Z}}$$

since a dimension one module over the base field is just isomorphic to the base field.

(b)

Definition 2.1. The exponent a finite group is the smallest $m \in \mathbb{Z}$ such that $g^m = 1$ for all $g \in G$.

Then they want you to prove that a finite abelian group has an element that has the same order as its exponent.

Let G be a finite abelian group. Then it decomposes as a $\mathbb{Z}$-module

$$G \cong \bigoplus_{i=1}^{n} \frac{\mathbb{Z}}{\langle d_i \rangle}, \text{ where } d_i \mid d_{i+1}, \text{ and } d_i \neq 0.$$

Claim 2.2. The exponent of G is d_n, and thus the generator of $\frac{\mathbb{Z}}{\langle d_n \rangle}$ is an element of the desired order.

Proof. Let $(g_1, \ldots, g_n) \in G$ be arbitrary. Then each g_i has order dividing d_i and since $d_i \mid d_n$ we have that

$$(g_1, \ldots, g_n)^{d_n} = \left(g_1^{d_n}, \ldots, g_n^{d_n}\right) = (e, \ldots, e)$$

so certainly the exponent is at most d_n. Now consider a generator for $\mathbb{Z}/\langle d_n \rangle$ say g. Then $(e, \ldots, e, g)$ is an element of order d_n so the exponent is at least d_n, and were done. □

(c)

1st Proof:
Consider the invariant decomposition of $\mathbb{F}^\times$ namely

$$\mathbb{F}^\times \cong \bigoplus_{i=1}^{m} \frac{\mathbb{Z}}{\langle d_i \rangle}, \text{ where } d_i \mid d_{i+1}.$$

Note that we require $d_i \neq 0$ since the group is finite. We wish to show that $m = 1$. Indeed suppose $m \geq 2$. Then we may identify $\frac{\mathbb{Z}}{\langle d_1 \rangle} \oplus \frac{\mathbb{Z}}{\langle d_2 \rangle}$ with a subgroup of $\mathbb{F}^\times$. Then each of the $d_1 \cdot d_2$ elements is a solution to the equation

$$x^{d_2} - 1$$

in $\mathbb{F}^\times$, since $d_1 \mid d_2$. Then a polynomial of degree d has at most d roots in a field so this is a contradiction and $m = 1$.

2nd Proof:
Let m be the exponent of $\mathbb{F}^\times$. By part (b) there is an element $g \in \mathbb{F}^\times$ of this order. Then since a polynomial over a field has at most as many roots as its degree the powers of g exhaust the roots of $x^m - 1$ in $\mathbb{F}^\times$. Then by definition of the exponent every $h \in \mathbb{F}^\times$ is a root of the polynomial so every element must be a power of g, and the unit group is cyclic. □

Problem 3

Statement. Let F be a field, let V be a finite dimensional F-vector space, and let $A, B : V \to V$ be commuting F-linear maps. Suppose there is a basis $\mathcal{B}_1$ with respect to which A is diagonalizable and a basis $\mathcal{B}_2$ with respect to which B is diagonalizable. Prove that there is a basis $\mathcal{B}_3$ with respect to which A and B are both diagonalizable.

Solution. See *Algebra Fall 2025, Question 3*. □

Problem 4

Statement. Let N be a positive integer, and let G be a finite group of order N.

(a) Let $\operatorname{Sym} G$ be the set of all bijections from G to G, viewed as a group under composition. Note that $\operatorname{Sym} G \cong S_N$. Prove that the Cayley map $C : G \to \operatorname{Sym} G$ given by $g \mapsto (x \mapsto gx)$ is an injective homomorphism.

(b) Let $\Phi : \operatorname{Sym} G \to S_N$ be an isomorphism. For $a \in G$, define $\epsilon(a) \in \{\pm 1\}$ to be the sign of the permutation $\Phi(C(a))$. Suppose that a has order d. Prove that $\epsilon(a) = -1$ if and only if d is even and N/d is odd.

(c) Suppose $N > 2$ and $N \equiv 2 \pmod 4$. Prove that G is not simple. (Hint: Use part (b).)

Solution. **(a)** Let G act on itself by left multiplication. That is $g \cdot k = gk$. More formally let $m_g : G \to G$ be left multiplication by g. Then the homomorphism for the group action is precisely the Cayley map $C(g) = m_g$. It remains to show it is injective. Indeed suppose $m_g = m_{g'}$. Then in particular

$$m_g(e) = g \cdot e = g = g' = m_{g'}(e).$$

so the morphism is injective.

(b) Some preliminaries. First let $w \in S_n$. The sign of the permutation is -1 raised to the number of transpositions that are required to express it. For cycles

$$\operatorname{sgn}(a_1, a_2, \ldots, a_m) = (-1)^{m-1}.$$

Then every w has a DCD $w = c_1 \cdots c_k$ where the c_i are disjoint cycles of length ℓ_i. Then

$$\operatorname{sgn}(w) = \prod_{i=1}^{k} \operatorname{sgn}(c_i) = \prod_{i=1}^{k} (-1)^{\ell_i - 1} = (-1)^{\sum_{i=1}^{k} \ell_i - k} = (-1)^{n-k}.$$

In other words to compute the sign we just need to know the number of cycles in the DCD.

Now to compute sign of $C(a)$ we need to know its DCD. We get this by studying the action of $\langle a \rangle$ on G by left multiplication. Then for $g \in G$ we have

$$O_g = \left\{ a^i g : i \in [d] \right\} = g \langle a \rangle$$

i.e. orbits are just cosets. Then restricted to each coset a acts like a cycle namely the cycle

$$\left(g, ag, a^2 g, \ldots, a^{d-1} g \right).$$

Then picking distinct representatives for each coset we get the DCD

$$a = \prod_{i=1}^{N/d} \left(g_i, ag_i, \ldots, a^{d-1} g_i \right)$$

so the sign is

$$\operatorname{sgn}\left(\Phi\left(C\left(a\right)\right)\right) = \left(-1\right)^{N - N/d}.$$

Now this is -1 iff N and N/d differ in parity. Certainly if N/d is odd and N is even this is satisfied. If N/d is odd then d must be even since dividing an even by an odd yields an odd. We can't have the case N/d is even while N is odd because N/d is a divisor of N so if N is odd so is N/d.

(c) Note that

$$\left(N \equiv 2 \bmod 4\right) \iff \left(N = 4k + 2\right)$$

so that $N/2 = 2k + 1$ is odd. Now since N is even G has an element of order 2 by Cauchy's theorem. Call this element $a \in G$. Then since N is even and $N/\left|a\right| = \frac{N}{2}$ is odd by part (b) $\epsilon\left(\Phi\left(a\right)\right) = -1$. Now since $\epsilon \circ \Phi : G \to \{-1, 1\}$ is a group hom, and it is non-zero (and not injective since $N > 2$) it must have a proper non-zero kernel $\ker\left(\epsilon \circ \Phi\right)$. This is a normal subgroup so G is not simple. □

Problem 5

Statement. Let $f(x) = x^4 - 5 \in \mathbb{Q}[x]$.

(a) Compute the Galois group of f over $\mathbb{Q}$.

(b) Compute the Galois group of f over $\mathbb{Q}(\sqrt{5})$.

Solution. **(a)** We have

$$\begin{aligned} f\left(x\right) = x^4 - 5 &= \left(x^2 - \sqrt{5}\right)\left(x^2 + \sqrt{5}\right) \\ &= \left(x - 5^{1/4}\right)\left(x + 5^{1/5}\right)\left(x + i5^{1/4}\right)\left(x - i5^{1/4}\right). \end{aligned}$$

We claim the splitting field of $f\left(x\right)$ (which is irred over $\mathbb{Q}$ by Eisensteins with $p = 5$) is $K = \mathbb{Q}\left(i, 5^{1/4}\right)$. Indeed $f\left(x\right)$ splits in K since it contains all the roots, and any field that contains the roots would contain $5^{1/4}$ and $i = i5^{1/4} \cdot 5^{-1/4}$ and thus contain K.

Now $G = \operatorname{Gal}\left(K/\mathbb{Q}\right)$ is a transitive subgroup of S_4 since it acts transitively on the roots of $f\left(x\right)$. Then from the Galois correspondence

$$\left|G\right| = \left[K : \mathbb{Q}\right] = \left[K : \mathbb{Q}\left(2^{1/4}\right)\right] \cdot \left[\mathbb{Q}\left(2^{1/4}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

Where $\left[\mathbb{Q}\left(i, 2^{1/4}\right) : \mathbb{Q}\left(2^{1/4}\right)\right] = 2$ since i is a root of $x^2 + 1$ which is irred in $\mathbb{Q}\left(2^{1/4}\right)$ as $x^2 + 1$ is degree 2 and has not roots there.

Then there is only one subgroup of S_4 of order 8 up to isomorphism namely the dihedral group D_4. So $G = D_4$. In this case its easy to see that it is generate by $s = \bar{\cdot}$ complex conjugation and $r\left(5^{1/4}\right) = i5^{1/4}$ which has order 4.

(b) Since K is still the splitting field over any intermediate field this group is precisely

$$H = \operatorname{Gal}\left(K/\mathbb{Q}\left(\sqrt{5}\right)\right)$$

which is the subgroup of automorphisms fixing $\sqrt{5}$. Since $G = \langle r, s \mid r^4 = s^2 = e, \text{ and } srs^{-1} = r^{-1} \rangle$ we have an explicit form for the elements (everything is of the form $r^i s^j$) and its easy enough to check. Note $s \cdot \sqrt{5} = \sqrt{5}$ since complex conjugation fixes the reals. Then it suffices to check what powers of r fix $\sqrt{5}$. Indeed

$$\begin{aligned} r\left(\sqrt{5}\right) &= i^2\sqrt{5} = -\sqrt{5} \\ r^2\left(\sqrt{5}\right) &= \sqrt{5} \\ r^3\left(\sqrt{5}\right) &= -\sqrt{5} \end{aligned}$$

so r^2 fixes it only. Then $\{e, s, r^2, r^2 s\}$ is order 4 subgroup fixing $\mathbb{Q}\left(\sqrt{5}\right)$. Since this is a proper intermediate extension this must be all of them.

Remark. You could also compute the degree $[k : \mathbb{Q}\left(\sqrt{5}\right)]$ to see the group must have order 4. To make what I'm saying above more explicit however the subgroup with fixed field $\mathbb{Q}\left(\sqrt{5}\right)$ can't be the entire group (which has order 8) so it has order at most 4, and since we've found 4 automorphisms this must be all of them.

□

Problem 6

Statement. Let F be a field, and let n a positive integer. Consider

$$A = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \in M_n(F).$$

Show that A has a Jordan normal form over F, and find it. (Suggestion: treat the cases $n \cdot 1 \neq 0$ in F and $n \cdot 1 = 0$ in F separately.)

Solution. I believe this is the matrix of all ones. If so we already know it has a $n-1$ dimensional kernel.

We can immediately identify two (not necessarily distinct) eigenvalues namely 0 and n. The vector $v_1 = (1, 1, \ldots, 1)$ satisfies $Av_1 = nv_1$.

Any of the vectors $u_i = e_1 - e_i$, for $i \in \{2, \ldots, n\}$ is an eigenvector for 0. Regardless of the base field the u_i are all independent, thus the 0 eigenspace has dimension at least $n-1$.

Now consider the cases for the base field.

Case 1: ($\operatorname{char} F \nmid n$**)** Then 0 and n are distinct eigenvalues so we have an eigenbasis for A and its diagonalizable.

Case 2: ($\operatorname{char} F \mid n$**)** Then $0 = n$ and the eigenvalues are no longer distinct. Indeed since the 0 eigenspace still has dimension $n-1$ there is at most one more eigenvalue say λ. Then since trace is sum of eigenvalues

$$\lambda + (n-1) \cdot 0 = n = 0$$

so $\lambda = 0$ and the matrix has only the 0 eigenvalue. Then it has $n-1$ distinct chains since it has $n-1$ independent eigenvectors, thus it must have one chain of length two and its JCF is

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

□

Problem 7

Statement. Let R be a commutative ring. Let S be a subset of R which is nonempty, does not contain 0, and for all $x, y \in S$ we have $xy \in S$. Let $\mathcal{I}$ be the set of all ideals I of R such that $I \cap S = \varnothing$. Show that for every ideal $I \in \mathcal{I}$, there is an ideal $J \in \mathcal{I}$ such that $I \subset J$ and J is not properly contained in any other ideal in $\mathcal{I}$. Prove that every such ideal J is prime.

Solution. Define

$$\Sigma_J = \{I \in \mathcal{I} : J \subseteq I\}$$

as a poset ordered by inclusion. It is non-empty since $J \in \Sigma_J$. Let $C = \{I_i\}_{i \in K}$ be a chain in K and $M = \bigcup_{i \in K} I_i$.

Claim: $M \in \Sigma_J$. Indeed $J \subseteq M$ since it is contained in each I_i. Then also

$$M \cap S = \bigcup_i I_i \cap S = \bigcup_i \varnothing = \varnothing$$

and M is an ideal since it is a union of a chain. Then $M \in \Sigma_J$ as desired and by zorn's lemma Σ_J has maximal elements.

It remain to show these maximals are prime. Let $M \in \Sigma_J$ be maximal, and suppose towards contradiction that M is not prime. Then there are $a, b \in R \setminus M$ such that $ab \in M$. Then consider the ideals

$$M_a = M + (a)\,, \text{ and } M_b = M + (b)\,.$$

Then both M_a and M_b contain M and J and as M is maximal in Σ_J they must lie outside of $\mathcal{I}$. In otherwords $M_a \cap S$ and $M_b \cap S$ are non-empty. Pick elemnts

$$m_a + ax \in M_a \cap S$$
$$m_b + by \in M_b \cap S$$

Then

$$(m_a + ax)(m_b + by) = m_a m_b + m_a by + axm_b + abxy \in M \cap S$$

contradicting that $M \in \mathcal{I}$ thus M is prime. □

Problem 8

Statement. Let R be a principal ideal domain, and let M be a finitely generated R-module.

(a) Prove that there are R-submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of M such that for all $0 \leq i \leq n-1$, M_{i+1}/M_i is cyclic (i.e., generated by a single element).

(b) Is the integer n of part (a) uniquely determined by M? (Prove your answer.)

Solution. **(a)** Since M is finitely generated over a PID we have an invariant decomposition

$$M \cong \bigoplus_{j=1}^{n} \frac{R}{\langle d_j \rangle}, \text{ where } d_j \mid d_{j+1}.$$

Now let

$$M_i = \bigoplus_{j=1}^{i} \frac{R}{\langle d_j \rangle}.$$

Then for example $M_n = M$, and $M_n/M_{n-1} = \frac{R}{\langle d_n \rangle}$, which is cyclic as an R-module generated by $1 + \langle d_n \rangle$. Similarly $M_{i+1}/M_i = \frac{R}{\langle d_{i+1} \rangle}$ and $M_0 = \{0\}$.

(b) I would think no. The primary and invariant decompositions won't always have the same size.

No. For example $\mathbb{Z}/6\mathbb{Z}$ is already cyclic as a $\mathbb{Z}$-module (its generated by $1 + 6\mathbb{Z}$) but we could also take the decomposition

$$0 \subseteq \frac{\mathbb{Z}}{3\mathbb{Z}} \subseteq \frac{\mathbb{Z}}{6\mathbb{Z}}$$

since the intermediate quotient is $\mathbb{Z}/2\mathbb{Z}$ which is cyclic. □