Algebra Qual Fall 2016

Problem 1

Statement (10 points)**.** Let G be a finite group and let $s, t \in G$ be two distinct elements of order 2. Show that the subgroup of G generated by s and t is a dihedral group. Recall that the dihedral groups of order $2m$ are of the form

$$D_{2m} = \langle \sigma, \tau \mid \sigma^m = 1 = \tau^2,\ \tau\sigma = \sigma^{-1}\tau \rangle,$$

for some $m \geq 2$.

Solution. Let $\sigma = st$. Note that the subgroup generated by s, t is the same as that generated by s, σ since clearly $\langle s, \sigma \rangle \subseteq \langle s, t \rangle$ and $t = s\sigma \in \langle s, \sigma \rangle$. Then it suffices to check that the group generated by s, σ has the correct presentation and order $2m$. That we have

$$D_{2m} = \left\langle \sigma, s \mid \sigma^m = s^2 = 1, s\sigma = \sigma^{-1}s \right\rangle, \text{ for some } m \in \mathbb{N}.$$

Indeed since G is finite σ has some order $m \geq 2$ (its order is at least two since $\sigma = e$ implies $s = t$.) and it suffices to check the second relation. Then

$$s\sigma s = ssts = ts = \sigma^{-1}$$

since s and t are self inverse so

$$(st)^{-1} = t^{-1}s^{-1} = ts.$$

Now note that $\langle s, \sigma \rangle = \langle s \rangle \cdot \langle \sigma \rangle$ so to show the group has order $2m = |\langle s \rangle| \cdot |\langle \sigma \rangle|$ it suffices to check that these groups intersect trivially. Indeed if $s = (st)^k$ then $(st)^k$ and $(st)^{m/2}$ are two distinct elements of order 2 in $\langle \sigma \rangle$, but $\langle \sigma \rangle$ is a finite cyclic group so it has only one subgroup (hence only one element) of order 2. □

Problem 2

Statement (10 points)**.** Let A and B be two $n \times n$ matrices with the property that $A \cdot B = B \cdot A$. Suppose that A and B are diagonalizable. Prove that A and B are simultaneously diagonalizable.

Solution. Let $\Lambda = \{\lambda_1, \ldots, \lambda_m\}$ be the distinct eigenvalues of A, and E_{λ_i} the eigenspaces of A. Since A is diagonalizable

$$k^n = \bigoplus_{i=1}^{m} E_{\lambda_i}.$$

Claim 2.1. The E_{λ_i} are invariant subspaces for B. I.e. $BE_{\lambda_i} \subseteq E_{\lambda_i}$.

Proof. Suppose $v \in E_{\lambda_i}$. Then

$$A(Bv) = B(Av) = \lambda Bv$$

so $Bv \in E_{\lambda_i}$ as desired. □

Claim 2.2. The restriction of B to each eigenspace is diagonalizable.

Proof. Let $M_B(x)$ be the minimal polynomial of B. Then $M_B(B) = 0$ and

$$M_B(B) \restriction E_{\lambda_i} = M_B(B \restriction E_{\lambda_i}) = 0$$

since the restriction the zero map is 0. Then if $B' = B \restriction E_{\lambda_i}$ the above shows that $M_B(B') = 0$ thus the minpoly of B' divides M_B. But then M_B splits into distinct linear factors so $M_{B'}$ must as well, thus B' is diagonalizable. □

Claim 2.3. For each λ_i there is a basis of simultaneous eigenvectors for E_{λ_i}.

Proof. Since the restriction of B to this eigenspace is diagonalizable there is basis $\mathcal{C}_{\lambda_i} = \{u_1^i, \ldots, u_{n_i}^i\}$ such that each u_k^i is an eigenvector for B. Then since each u_k^i is in E_{λ_i} they are also eigenvectors for A. □

Then the union of the $\mathcal{C}_{\lambda_i}$ form a basis of simultaneous eigenvectors for the space. □

Problem 3

Statement (10 points)**.** How many groups are there up to isomorphism of order pq, where $p < q$ are prime integers?

Solution. Suppose G has order pq. Then from the 3rd sylow theorem

$$n_q \equiv 1 \bmod q, \text{ and } n_q \mid p$$

so n_q is one or p. But since $p < q$ in particular p is not congruent to 1 mod q so $n_q = 1$ and there is normal copy of C_q in G. Then there is also a sylow p subgroup C_p. Since they have coprime order $C_p \cap C_q = \{e\}$. Then since C_q is normal we have that the product $C_p \rtimes C_q$ is semidirect, and has size pq thus

$$G = C_q \rtimes C_p.$$

Now each semidirect product is determined by a group homomorphism

$$\phi : C_p \to \mathrm{Aut}(C_q) = (\mathbb{Z}/q\mathbb{Z})^\times$$

there where each $m \in (\mathbb{Z}/q\mathbb{Z})^\times$ the corresponding automorphism is

$$m \cdot g_q = g_q^m$$

where g_q is the generator for C_q. Then to classify semidirect products it suffices to determine the possible homomorphisms.

Now $\ker \trianglelefteq C_p$ and since C_p is simple this kernel is either trivial or the entire group. In the case of the entire group the semidirect product is direct

$$C_q \rtimes C_p = C_q \times C_p.$$

Now if it is injective then we must have $p \mid \left|\mathbb{F}_q^\times\right| = q-1$. Then since $\mathbb{F}_q^\times$ is cyclic there is a unique subgroup of order p and every element is a generator.

Then if $P \subseteq \mathbb{F}_q^\times$ is this order p subgroup then there is a morphism ϕ_a sending $g_p \to \left(a \cdot g_q = g_q^a\right)$.

We claim all of these morphisms yield identical semidirect products.

To show they are equal it suffices to show there is an automorphism of C_p such that $\phi_a \circ \psi = \phi_b$. Indeed note that since P is cyclic of prime order it is generated by ϕ_a. Then the automorphims of C_p send our generator g_p to any other power g_p^b. Then Call this map ψ_b. Then

$$\phi_a \circ \psi_{b^{-1}}^{-1}\left(g_p\right) = \phi_a \circ \psi_b\left(g_p\right) = \phi_a\left(g_p^b\right) = \phi_a\left(g_p\right)^b$$

i.e. $\phi_a \circ \psi_{b^{-1}}^{-1} = \phi_a^b$ and picking b such that $\phi_a^b = \phi_c$ for any other c we see all morphisms give equivalent semidirect products.

In summary there are two distinct groups of order pq. □

Problem 4

Statement (10 points)**.** Set $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

(a) Find the splitting field K of $f(x)$ over $\mathbb{Q}$.

(b) Find the Galois group G of K over $\mathbb{Q}$.

(c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

Solution. **(a)** Note that $f\left(x\right)$ is irred over $\mathbb{Q}$ by Eisenstein's with $p = 5$. Then also

$$f\left(x\right) = \left(x - \sqrt[3]{5}\right)\left(x - w\sqrt[3]{5}\right)\left(x - w^2\sqrt[3]{5}\right), \text{ where } w = e^{2\pi i/3}.$$

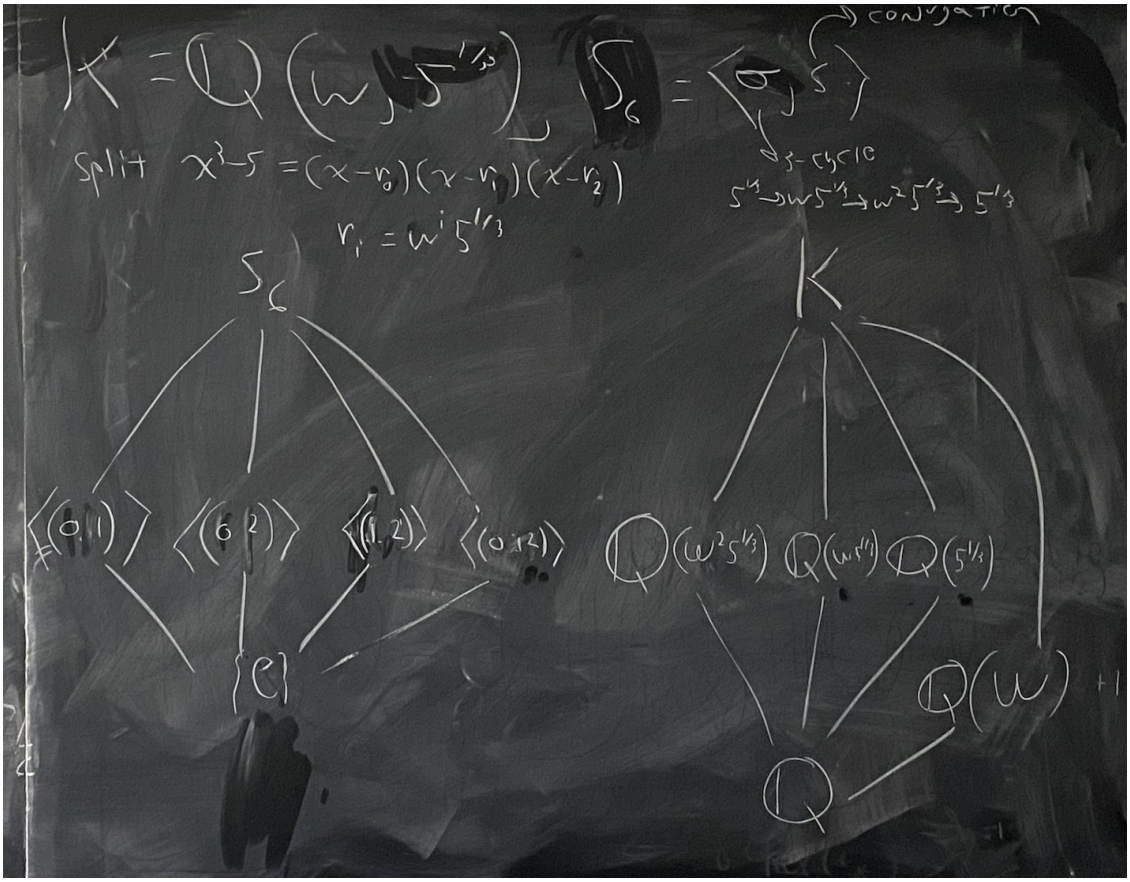
We claim the $K = \mathbb{Q}\left(\sqrt[3]{5}, w\right)$. Indeed $f\left(x\right)$ certainly splits in $\mathbb{Q}\left(\sqrt[3]{5}, w\right)$ since it contains all the roots of $f\left(x\right)$. Then also if K is the splitting field it contains the roots $\sqrt[3]{5}$ and $w\sqrt[3]{5}$ thus $w = \sqrt[3]{5}^{-1} \cdot w\sqrt[3]{5} \in K$ as well.

(b) This is subgroup of S_3 since the Galois group acts transitively on the roots of $f\left(x\right)$. Now $K \subseteq \mathbb{C}$ so complex conjugation is an automorphism of order 2 hence a transposition. Then since the Galois groups acts transitively there is an automorphism $\sigma \in G$ sending sending $\sqrt[3]{5} \to w\sqrt[3]{5}$. Then σ has order 3 since

$$\sqrt[3]{5} \to w\sqrt[3]{5} \to w^2\sqrt[3]{5} \to w^3\sqrt[3]{5} = \sqrt[3]{5}.$$

Then the only elements of order 3 in S_3 are 3-cycles and a 3-cycle and a transposition generate all of S_3 so $G = S_3$.

(c)



□

Problem 5

Statement (10 points)**.** How many monic irreducible polynomials over $\mathbb{F}_p$ of prime degree ℓ are there? Justify your answer.

Solution. Let $F = \mathbb{F}_p$, and let $p(x) \in F[x]$ be monic irreducible of degree ℓ. Then

$$\frac{F[x]}{\langle p(x) \rangle}$$

is a degree $\ell = \deg p$ extension of $\mathbb{F}_p$ and is thus a finite field of over p^ℓ. Then there is a unique such field $F_\ell := \mathbb{F}_{p^\ell}$ namely the splitting field of $x^{p^\ell} - x$. Then this field contains a root of $p(x)$ and since it is normal and separable it contains all the roots of p and they are distinct in F_ℓ.

Then since $p(x) \in F[x]$ was arbitrary every degree ℓ polynomial splits into distinct factors in F_ℓ.

Now we will show that every element in $F_\ell \setminus F$ is the root of a monic irreducible of degree ℓ. Indeed let $\alpha \in F_\ell \setminus F$ and consider its minimal polynomial p_α. Since $\alpha \notin F$ we know $\deg p_\alpha > 1$. Then $F(\alpha)$ is a subfield of F_ℓ and $[F(\alpha) : F] = \deg p_\alpha$. Then $\deg p_\alpha \mid [F_\ell : F] = \ell$. Then ℓ is prime and $\deg p_\alpha > 1$ so we must have $\deg p_\alpha = \ell$ as desired.

Then to count polynomials it suffices to count the distinct minimal polynomials of elements. Then monic has ℓ-roots and there are $q^\ell - q$ elements if $F_\ell \setminus F$ so there are precisely

$$(\#\text{monic irred poly's of degree } \ell \text{ in } F) = \frac{q^\ell - q}{\ell}.$$

□

Problem 6

Statement (10 points)**.** Let R be a ring and $f : M \to N$ and $g : N \to M$ be R-module homomorphisms such that $g \circ f = \mathrm{id}_M$. Show that $N \cong \operatorname{Im} f \oplus \operatorname{Ker} g$.

Solution. Let $u \in N$ and consider $v = f \circ g\,(u)$. Then

$$g\,(u - f\,(g\,(u))) = g\,(u) - g\,(f\,(g\,(u))) = g\,(u) - g\,(u) = 0$$

so $u - v \in \ker g$. Suppose the difference is k. Then

$$u = v + k \in \operatorname{im} f + \ker g$$

since $v \in \operatorname{im} f$. Then it remains to show that the intersection is trivial. Indeed suppose $u \in \operatorname{im} f \cap \ker g$. Then $u = f\,(v)$ for some $v \in M$ and

$$0 = g\,(u) = g\,(f\,(v)) = v$$

so $v = 0$. Then since f is a module morphism $f\,(0) = u = 0$ as well. □

Problem 7

Statement (10 points)**. (a)** (1 point) Define solvable for a group G.

(b) (9 points) Show that every group G of order 36 is solvable. Hint: You can use that S_4 is solvable.

Solution. **(a)** A group G is solvable if there exists a sequence of subgroups

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G$$

such that each is normal in the next and the quotients G_i/G_{i-1} are abelian.

(b) Note $|G| = 2^2 \cdot 3^2$. By the 3rd sylow theorem we have

$$n_3 \equiv 1 \bmod 3, \text{ and } n_3 \mid 4$$

so $n_3 \in \{1, 4\}$. Suppose $n_3 = 1$. Then there is a normal 3-sylow subgroup P or order 9. Then G/P has order 4 and both are groups of square prime order. Then every such group is abelian therefore solvable. Then since P and its quotient G/P are solvable so is G.

Now suppose $n_3 = 4$. Then letting G act by conjugation on the set of 3-sylow subgroups we get an isomorphism $\phi : G \to S_4$. Since $|G| = 36 > 24 = |S_4|$ we know that ϕ cannot be injective hence $\ker \phi$ is a proper non-trivial normal subgroup of G.

Now $G/\ker\phi \cong \operatorname{im}\phi$ which is solvable being a subgroup of the solvable group S_4. Then it suffices to show that $\ker\phi$ is solvable.

First note that the stabilizers of a 3-sylow subgroup is precisely its normalizer $N_G(P)$ so orbit stabilizer yields

$$|N_G(P)| = \frac{|G|}{n_p} = 9.$$

Now

$$\ker\phi = \bigcap_{3\text{-sylow } P} N_G(P) \subseteq N_G(P), \text{ for every 3-sylow } P$$

Since $\ker\phi \neq \{e\}$, and we cannot have $\ker\phi$ a 3-sylow subgroup (since we're handling the case where there is not normal 3-sylow) we must have $|\ker\phi| = 3$. Then $\ker\phi = C_3$ and is thus abelian and solvable as desired. □