

Algebra Qual Spring 2017

Problem 1

Statement (10 points). Let G be a finite group and let $\pi : G \rightarrow \text{Sym}(G)$ be the Cayley representation. (Recall that this means that for an element x in G , $\pi(x)$ acts by left translation on G .) Prove that $\pi(x)$ is an odd permutation if and only if the order $|\pi(x)|$ of $\pi(x)$ is even and $|G| / |\pi(x)|$ is odd.

Solution. Fix $x \in G$ and restriction the left translation action to the cyclic subgroup $H := \langle x \rangle$. That is

$$x^n \cdot g = x^n g.$$

Then the cycles in the DCD for x are precisely the orbits of this action. Then these orbits are by definition the distinct cosets of H . That is

$$O_g = \{x \cdot g, x^2 \cdot g, \dots, x^n \cdot g\} = Hg$$

and the corresponding cycle in the DCD for x is simply $(x \cdot g, x^2 \cdot g, \dots, x^n \cdot g)$ (where the cycle is only defined up to cyclic rotation.) Then the sign of x is the product of signs of the cycles and the sign of cycle is $(-1)^{\ell-1}$ where ℓ is the length of the length of the cycle. Then if the distinct cosets of H are $g_1 H, \dots, g_k H$ (i.e. $k = [G : H] = |G| / |x|$) we have

$$\text{sgn}(x) = \prod_{i=1}^k (-1)^{|g_i H|-1} = \prod_{i=1}^k (-1)^{|x|-1} = (-1)^{k|x|-k} = (-1)^{|G|-|G|/|x|}.$$

Then $\text{sgn}(x) = -1$ iff $|G|$ and $|G| / |x|$ differ in parity. Then if $|G|$ is odd they cannot differ in parity since $|G| / |x|$ being a divisor of $|G|$ must be odd as well. Then $|G|$ must be even forcing $|G| / |x|$ to odd which implies $|x|$ must be even since an even divided by an odd is odd. $\square$

Problem 2

Statement (15 points). (a) How many isomorphism classes of abelian groups of order 56 are there? Give a representative for one of each class.

(b) Prove that if G is a group of order 56, then either the Sylow-2 subgroup or the Sylow-7 subgroup is normal.

(c) Give two non-isomorphic groups of order 56 where the Sylow-7 is normal, and the Sylow-2 subgroup is not normal. Justify that your two groups are not isomorphic.

Solution. (a) Note $56 = 2^3 \cdot 7$. Then by the fundamental theorem of finitely generated abelian groups the isomorphism classes are

$$C_2 \times C_2 \times C_2 \times C_7$$

$$C_4 \times C_2 \times C_7$$

$$C_8 \times C_7$$

(b) By the 3rd sylow theorem

$$n_2 \in \{1, 7\}, \text{ and } n_7 \in \{1, 8\}.$$

If neither is normal then $n_7 = 8$ and $n_2 = 7$. Then since the 7-sylow subgroups are cyclic of prime order they are either equal or intersect trivially. Then the distinct identity elements in the 7-sylows yield $6 \cdot 8 = 48$ elements of G . Now the 7-sylows and 2-sylows intersect trivially since they have coprime order so if have at least 8 non-identity elements in the 2 sylow subgroups then counting the identity we have at least $48 + 8 + 1 = 57 > |G|$ elements a contradiction. Then we have at least 8 such elements since we know there are two distinct 2-sylow subgroups P, Q where P has 7 elements discounting the identity and Q has some element not in P since they are distinct.

(c) Consider the semidirect products

$$C_7 \rtimes C_8, \text{ and } C_7 \rtimes D_4$$

with the non-trivial group homomorphisms

$$\phi : C_8 \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times$$

$$g \mapsto 6$$

(and)

$$\phi : D_4 \rightarrow (\mathbb{Z}/7\mathbb{Z})^\times$$

$$r \mapsto 1$$

$$s \mapsto 6$$

Now the sylow 2 subgroups of $C_7 \rtimes C_8$ are C_8 (sylow subgroups are all isomorphic by conjugation and this is a order 8 subgroup so sylow) and the sylow 2 subgroups of $C_7 \rtimes D_4$ are precisely copies of D_4 . Then these semidirect products are not isomorphic since for example $C_7 \rtimes D_4$ contains no subgroup isomorphic to C_8 . $\square$

Problem 3

Statement (10 points). Let R be a commutative ring with 1. Suppose that M is a free R -module with a finite basis X .

(a) Let I be a proper ideal of R . Prove that M/IM is a free R/I -module with basis X' , where X' is the image of X under the canonical map $M \rightarrow M/IM$.

(b) Prove that any two bases of M have the same number of elements. You may assume that the result is true when R is a field.

Solution. (a) Suppose $X = \{x_1, x_2, \dots, x_k\}$ is our basis any $q : M \rightarrow M/IM$ is the quotient map. Since the quotient map is surjective and X is a generating set for M its image $X' = q(X) = \{x_1 + IM, \dots, x_k + IM\}$ generates the image $q(M) = M/IM$. It remains to check that X' is independent as a R/I basis. Indeed suppose

$$(a_1x_1 + IM) + \dots + (a_kx_k + IM) = 0_{M/IM}$$

i.e. $\sum_i a_i x_i \in IM$. We want to show that $a_i = 0_{R/I}$ i.e. that each $a_i \in I$. Indeed since $\sum_i a_i x_i \in IM$ we may write $\sum_i a_i x_i = \sum_j b_j m_j$ for some $b_j \in I, m_j \in M$. Then since X is a generating set there are $c_i^j \in R$ such that $m_j = \sum_i c_i^j x_i$. Then we have

$$\sum_i a_i x_i = \sum_j b_j m_j = \sum_j \sum_i b_j c_i^j x_i.$$

and by the independence of the x_i we must have $a_i = \sum_j b_j c_i^j \in I$ since $b_j \in I$ and I is an ideal.

(b) Since R is a commutative ring with 1 it is not the zero ring thus it has a maximal ideal $I \subseteq R$. Let X, Y be two basis for M . Then their images under the quotient map $q : M \rightarrow M/IM$ form a basis for M/IM as a R/I module i.e. an R/I vector space since R/I is a field. Then any two basis for the vector space M/IM has the same size so $|X| = |Y|$ as desired. $\square$

Problem 4

Statement (10 points). (a) Let R be an integral domain with quotient field F . Suppose that $p(x)$, $a(x)$, and $b(x)$, are monic polynomials in $F[x]$ with $p(x) = a(x)b(x)$, and with $p(x)$ in $R[x]$, $a(x)$ not in $R[x]$, and both $a(x)$ and $b(x)$ not constant. Prove that R is not a UFD. You may assume Gauss' lemma.

(b) Prove that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD. Hint: let $p(x) = x^2 - 2$.

Problem 5

Statement (10 points). Let R be an integral domain, and let M be a nonzero torsion R -module.

(a) Prove that if M is finitely generated then the annihilator in R of M is nonzero.

(b) Give an example of a non-finitely generated torsion R -module whose annihilator is (0) . Justify your answer.

Solution. (a) Suppose

$$M = \text{span}_R \{m_1, m_2, \dots, m_k\}.$$

Since each m_i is a torsion element there is $a_i \in R$ such that $a_i m_i = 0$ and $a_i \neq 0$. Then since R is a domain $a = a_1 a_2 \dots a_k \neq 0$ and $am_i = \left(\frac{a}{a_i}\right) \cdot a_i m_i = 0$. Then $a \in \text{Ann}(M)$ since it annihilates each generator.

(b) Consider the $\mathbb{Z}$ -module

$$M = \bigoplus_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}.$$

This is a torsion module since any element is a finite sum $\sum_i a_i$ for $a_i \in \mathbb{Z}/n_i\mathbb{Z}$ for some $n_i \in \mathbb{N}$. Then since each a_i is killed by n_i this element is killed by the product $\prod_i n_i$ which is non-zero since $n_i > 0$ and $\mathbb{Z}$ is a domain.

Indeed pick $n \in \mathbb{N}$ and consider the submodule $\mathbb{Z}/(n+1)\mathbb{Z}$ where $n \equiv -1 \pmod{n+1}$ scaling by n is an automorphism sending each element to its additive inverse. $\square$

Problem 6

Statement (10 points). Let A be an $n \times n$ matrix with all entries equal to 0 except for the $n-1$ entries just above the diagonal being equal to 2.

- (a) What is the Jordan Canonical Form of A , viewed as a matrix in $M_n(\mathbb{C})$?
- (b) Find a non-zero matrix $P \in M_n(\mathbb{C})$ such that $P^{-1}AP$ is in Jordan Canonical Form.

Solution. (a) In the case $n = 3$ this is the matrix

$$A = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

and more generally

$$A = \begin{bmatrix} 0 & 2 & & & \\ & 0 & 2 & & \\ & & \ddots & \ddots & \\ & & & 0 & 2 \\ & & & & 0 \end{bmatrix}.$$

Then A is nilpotent of order n and its char poly is simply x^n . Then A also has rank $n-1$ so there is only one chain and thus the JCF of A is simply a single Jordan block of size n for the eigenvalue zero. Really

$$J_A = \frac{1}{2}A.$$

(b) Since there is only one chain it suffices find one rank $n-1$ generalized eigenvector for 0. That is a single vector such that $A^n v = 0$ but $A^{n-1}v \neq 0$. Note that $A^n = 0$ so any vector is in its kernel, but that all smaller powers A^{n-k} always have an entry in their last column so $e_n := (0, 0, \dots, 0, 1)$ is not in the kernel of A^{n-1} . Then

$$Ae_n = 2e_{n-1}, A^2e_n = 2^2e_{n-2}, \dots, A^ke_n = 2^ke_{n-k}$$

and $A^{n-1}e_n = 2^{n-1}e_1$ which is in the kernel of A thus an eigenvalue for 0. Really the we have

$$P = \begin{bmatrix} 2^{n-1} & & & & \\ & 2^{n-2} & & & \\ & & 2^{n-3} & & \\ & & & \ddots & \\ & & & & 2^0 \end{bmatrix}.$$

$\square$

Problem 7

Statement (10 points). Let F be a field and let $f(x) \in F[x]$.

(a) Define what is a splitting field of $f(x)$ over F .

(b) Let F now be a finite field with q elements. Let E/F be a finite extension of degree $n > 0$. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting field of $g(x)$ over F . Fully justify your answer.

(c) Show that the extension E/F in (b) is a Galois extension.

Solution. (a) A polynomial $f(x) \in F[x]$ splits in an extension L/F if all of its roots are in L . Then L is called a splitting field for f if f splits in L but not in any proper subfield of L . Splitting fields are unique up to isomorphism.

(b) We claim E/F is a splitting field for

$$f(x) := x^{q^n} - x \in F[x].$$

Indeed since E is n dimensional vector space of F and F has size q counting possible linear combinations of a basis yields

$$|E| = q^n.$$

Then note that the unit group $E \setminus \{0\}$ has size $q^n - 1$ thus every $a \in E \setminus \{0\}$ has order dividing $q^n - 1$ and thus is a root of

$$x^{q^n-1} - 1 = f(x) / x.$$

Then since 0 is also a root of $f(x)$ we see that all elements of E are roots of $f(x)$. Then any polynomial over a field has at most $\deg f$ roots in that field so as $|E| = q^n$ we see that all the roots of f live in E . Then E' was any proper subfield it simply wouldn't have enough elements to contain all the roots of $f(x)$. Then we've shown f splits in E and in no proper subfield of E hence E is a splitting field for $f(x)$.

(c) Splitting fields are always Galois.

First we check normality. Let $g(x) \in F[x]$ be the minimal polynomial of $\alpha \in E$. If $\deg g = 1$ then all the roots of g are in E and we're done, else suppose there is another root $\beta \in F[x]$.

Then we may view E as an extension of $F[x] / \langle g \rangle$ in two different ways. One via the embedding $\phi_1 : F[x] / \langle g \rangle \rightarrow F(\alpha) \subseteq E$ which sends $x \mapsto \alpha$ and another via the embedding $\phi_2 : F[x] / \langle g \rangle \rightarrow F(\beta) \subseteq E$ sending $x \mapsto \beta$.

Then by uniqueness of splitting fields there is field automorphism $\psi : E \rightarrow E$ such that the following diagram commutes (replace K in the below diagram by F , and L by E .)

$$\begin{array}{ccccc} K & \xhookrightarrow{\iota} & K[x] / \langle p \rangle & \xhookrightarrow{\phi_1} & L \\ & & \searrow \phi_2 & & \downarrow \psi \\ & & & & L \end{array}$$

i.e. $\psi(\alpha) = \psi \circ \phi_1(x) = \phi_2(x) = \beta$. Since the ϕ_i fix the base field F so does ψ . Then $\beta \in E$ and since β was an arbitrary root of $g(x)$ all the roots of g lie in E and E is normal.

Now since E is normal separability follows from the separability of $f(x)$. Indeed since all the roots of g lie in E and all the elements of E are roots of f we must have $g \mid f$. Then since f is separable (it has no repeated roots since $f' = q^n x^{q^n-1} - 1 = -1$ in F since F has characteristic dividing q) $g(x)$ is separable and E is a separable extension.

Remark. Its not clear to me what they want you to assume in this problem. If you assume that splitting fields act transitively on the roots of irreducibles then its also trivial, but the argument for that is just what I've given above.

□

Problem 8

Statement (15 points). **(a)** Let K denote the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is isomorphic to the group of invertible matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a \in \mathbb{F}_5^*$ and $b \in \mathbb{F}_5$.

(b) Determine all intermediate fields between the splitting field K of $x^5 - 2$ and $\mathbb{Q}$ which are Galois over $\mathbb{Q}$.

Solution. **(a)** Note that

$$K = \mathbb{Q} \left(2^{1/5}, w \right), \text{ where } w = e^{2\pi i/5}, \text{ is a primitive 5th root of 1.}$$

This can be by a simple minimality argument once you note that

$$x^5 - 2 = (x - 2^{1/5}) (x - w^2 2^{1/5}) (x - w^3 2^{1/5}) (x - w^4 2^{1/5}) (x - w^1 2^{1/5}).$$

We claim that

$$[K : \mathbb{Q}] = [K : \mathbb{Q} (2^{1/5})] [\mathbb{Q} (2^{1/5}) : \mathbb{Q}] = 4 \cdot 5 = 20$$

Indeed

$$\mathbb{Q} (2^{1/5}) \cong \frac{\mathbb{Q}[x]}{\langle x^5 - 5 \rangle}$$

so it has degree 5 since the quotient is 5 dimensional fields as $x^5 - 5$ is irreducible. K also contains the intermediate extension $\mathbb{Q}(w)/\mathbb{Q}$ which has degree 4 since its a root of $1 + x + x^2 + x^3 + x^4$ which is irreducible in $\mathbb{Q}$ since it is a cyclotomic polynomial, thus $4 \mid [K : \mathbb{Q}]$. This yields $[K : \mathbb{Q}] \geq 20$. To show it is at most 20 it suffices to check that $[K : \mathbb{Q} (2^{1/5})] \leq 4$. Indeed this extension has the same degree as the minpoly of w over $\mathbb{Q} (2^{1/5})$. Since this minpoly will divide the annihilating polynomial over $\mathbb{Q}$ namely $1 + x + x^2 + x^3 + x^4$ it has degree at most 4 and we're done.

Now we classify the automorphisms in G . We claim for any $(a, b) \in \mathbb{F}_5^\times \times \mathbb{F}_5$ there is an automorphism $\phi_{a,b} \in G$

$$\phi_{a,b} (2^{1/5}) = 2^{1/5} w^b, \text{ and } \phi_{a,b} (w) = w^a.$$

Indeed since $\mathbb{F}_5^\times \times \mathbb{F}_5$ has the same size as the Galois group it suffices to check that every $\phi \in G$ is of this form. Now since

$$f(x) = x^5 - 2, \text{ and } g(x) = 1 + x + x^2 + x^3 + x^4$$

are irreducible any $\phi \in G$ must permute their roots. Then the roots of $g(x)$ are precisely the primitive roots of 5th roots which are all powers of w thus $\phi(w) = w^a$ where $a \neq 0$. Similarly $\phi(2^{1/5})$ must be a root of $f(x)$ and these are precisely things of the form $2^{1/5} w^b$ for $b \in \mathbb{F}_5$ ($b = 0$ is allowed.)

Then furthermore we claim

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto \phi_{a,b}$$

is a group isomorphism. Certainly it is a bijection so it suffices to check it commutes with multiplication. Indeed

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ac & ad+b \\ 0 & 1 \end{bmatrix}$$

while

$$\begin{aligned} \phi_{a,b}(\phi_{c,d})(2^{1/5}) &= \phi_{a,b}(w^d 2^{1/5}) = w^{ad+b} 2^{1/5} \\ \phi_{a,b}(\phi_{c,d})(w) &= \phi_{a,b}(w^c) = w^{ac} \end{aligned}$$

so indeed it is a group isomorphism.

(b) By the Galois correspondence it suffices to determine the normal subgroups of G . Define

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \text{ and } B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then A generates a normal 5-sylow subgroup (a quick 3rd sylow argument shows the 5-sylow is unique,) and B generates 2-sylow subgroup. Thus

$$G \cong \langle A \rangle \rtimes \langle B \rangle = C_5 \rtimes C_4.$$

A computation shows the conjugation action is squaring $BAB^{-1} = A^2$.

Since conjugation is non-trivial B is not a normal subgroup of G , and neither is any subgroup of B since

$$A \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} A^{-1} = \begin{bmatrix} a & 1-a \\ 0 & 1 \end{bmatrix} \notin \langle B \rangle.$$

Then the only possibilities are $\langle A \rangle$ and the subgroups containing it. Then it suffices to count the normal subgroups of $G / \langle A \rangle \cong C_4$. Then there is only one proper normal subgroup namely $C_2 \subseteq C_4$. Then by the lattice isomorphism theorem there is a normal subgroup of order 10 corresponding to the preimage of this C_2 under the quotient map. Then there are two normal subgroups namely C_5 and this normal subgroup of order 10.

By the Galois correspondence the fixed fields of these subgroups are the only intermediate extensions that are Galois over $\mathbb{Q}$. $\square$