

Algebra Qual Fall 2025

Problem 1

Statement (10 points). Let G, H be finite cyclic groups. Prove that $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Solution.

Proof 1

Let $n = |G|, m = |H|$. Then $G \cong \mathbb{Z}/n\mathbb{Z}, H \cong \mathbb{Z}/m\mathbb{Z}$ and

$$G \times H \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Now if n and m are coprime the chinese remainder theorem gives an isomorphism of rings (and therefore an isomorphism of abelian groups as well)

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$$

so the converse direction holds.

For the forward direction consider the contrapositive. Suppose $\gcd(n, m) = d > 1$. Then suppose p is a prime divisor of d . Then Cauchy's theorem yields that C_p is a subgroup of both G, H . Then $C_p \times C_p$ is a subgroup of the direct product. Since subgroups of cyclic groups are cyclic this must also be cyclic, but it is not since every element has order $p < p^2$.

Proof 2

We'll use the following fact

Proposition 1.1. If G, H are finite groups then

$$|(g, h)| = \text{lcm}(|g|, |h|) = \frac{|g| \cdot |h|}{\gcd(|g|, |h|)}.$$

From this the $\Leftarrow$ direction is easy. Suppose $G = \langle g \rangle, H = \langle h \rangle$. Then

$$|(g, h)| = \frac{|g| \cdot |h|}{\gcd(|g|, |h|)} = \frac{|G| \cdot |H|}{\gcd(|G|, |H|)} = \frac{|G \times H|}{1}$$

so (g, h) have the order of the group and therefore generate. Conversely suppose $G \times H = \langle (g, h) \rangle$. Then g and h must generate G, H respectively since if there was some $g' \in G$ so that $g' \neq g^i$ for any $i \in \mathbb{Z}$ then $(g', e) \notin \langle (g, h) \rangle$ contradicting the assumption that (g, h) is a generator. Then we may run the above identity in reverse. We know

$$\frac{|G| \cdot |H|}{\gcd(|G|, |H|)} = \frac{|G \times H|}{1}$$

iff the GCD is 1. □

Problem 2

Statement (10 points). **(a)** Using Sylow theory show that every group of order 10 is not simple.

(b) Classify all groups of order 10 and justify your answer. For the non-abelian group(s), give a presentation by generators and relations.

Solution. **(a)** By the 3rd sylow theorem $n_5 \mid 2$ so $n_5 \in \{2, 1\}$, and also $n_5 \equiv 1 \pmod{5}$. Then we must have a unique 5-sylow subgroup C_5 . Then the conjugate of a p -sylow subgroup is another p -sylow subgroup and since there is only one this copy of C_5 must be normal no group of order 10 is simple.

(b) By the previous argument the 5-cylow subgroup is normal. Consider a 2-sylow subgroup C_2 . Since the orders of C_2 and C_5 are coprime they intersect trivially $C_2 \cap C_5 = \{e\}$. Then the product C_2C_5 is semidirect. Since $|C_2 \rtimes C_5| = 10$ this must be the entire group. Then classifying groups of order 10 is the same as classifying semi direct products of C_2 and C_5 . Now any such semi direct product is defined by a homomorphism

$$\phi : C_2 \rightarrow \text{Aut}(C_5) = (\mathbb{Z}/5\mathbb{Z})^* = C_4.$$

so it suffices to determine the homomorphisms. First if ϕ is not injective then it is trivial since the only two elements it can send to the same element of C_4 are the only two distinct elements of C_2 . If the morphism is trivial then semidirect product is direct

$$C_2 \rtimes C_5 = C_2 \times C_5.$$

Now if ϕ is injective then its image is an order two subgroup of $C_4 = (\mathbb{Z}/5\mathbb{Z})^*$. There is only one such subgroup namely $\langle 4 \rangle = \{1, 4\}$. This corresponds to the action on $\mathbb{Z}/5\mathbb{Z}$ by $1 \cdot a = a$ and $4 \cdot a = 4a$. $\square$

Problem 3

Statement (10 points). Let A be an $n \times n$ matrix over a field k .

(a) Define precisely what it means for A to be diagonalizable.

(b) Provide the definition of an eigenvalue for A , the definition of an eigenspace, and a criterion via eigenspaces for A to be diagonalizable.

(c) Prove that if A and B are two $n \times n$ matrices that are diagonalizable with the property that $AB = BA$ then they are simultaneously diagonalizable.

Solution. **(a)** A is diagonalizable if it has n independent eigenvectors in k^n . Equivalently if there is a basis of k^n composed of eigenvectors of A .

(b) An element $\lambda \in k$ is an eigenvalue for A if there is a vector $v \in k^n$ so that $Av = \lambda v$. Equivalently if the matrix $(A - \lambda I)$ has a non-trivial kernel.

If $\lambda \in k$ is an eigenvalue of A then the λ -eigenspace of A is $\ker(A - \lambda I)$ equivalently it is the set of λ eigenvectors of A .

A is diagonalizable if k^n can be written as a direct sum of its eigenspaces

$$k^n \cong \bigoplus_{i=1}^m \ker (A - \lambda_i I).$$

(c) First note that because A and B commute they preserve each others eigenspaces. That is if $Av = \lambda v$ then

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

so Bv is still a λ -eigenvector of A .

Now let $\{\lambda_1, \dots, \lambda_m\}$ be the eigenvalues of A and fix a basis

$$\mathcal{A}_i = \{u_1^i, \dots, u_{n_i}^i\}$$

for then λ_i eigenspace $\ker(A - \lambda_i)$. Let π_i be projection onto the i -th eigenspace for A . That is

$$\pi_i \left(\sum_{k=1}^m \sum_{j=1}^{n_k} a_{k,j} u_j^k \right) = \sum_{j=1}^{n_i} a_{i,j} u_j^i.$$

Then π_i acts like the identity on $\ker(A - \lambda_i)$, and since B preserves this eigenspace we have

$$\pi_i(Bv) = Bv = B\pi_i(v), \text{ for all } v \in \ker(A - \lambda_i)$$

And similarly since B preserves every other eigenspace

$$\pi_i(Bv) = 0 = B\pi_i(v) = B0, \text{ for all } v \in \ker(A - \lambda_j), j \neq i.$$

Then for a general vector $v \in k^n$ expanding it in the eigenbasis for A as $v = \sum_i \sum_j a_{i,j} u_j^i$ we get

$$B\pi_i(v) = B \left(\sum_j a_{i,j} u_j^i \right) = \sum_j a_{i,j} Bu_j^i = \pi_i(Bv)$$

so B commutes with each projection operator.

Note also that since the union of the $\mathcal{A}_i$ form a basis for k^n the sum of the projection operators

$$\pi_1 + \pi_2 + \dots + \pi_m = \text{id}_{k^n}.$$

Then if v is any non-zero vector some $\pi_i(v) \neq 0$.

Now suppose $\{\gamma_1, \dots, \gamma_\ell\}$ are the eigenvalues of B and

$$\mathcal{B}_i = \{v_1^i, \dots, v_{n_i}^i\}$$

is a basis for $\ker(B - \gamma_i)$. Now each eigenvector is non-zero thus $\pi_k(v_i^j) \neq 0$ for some π_k . Then we claim this non-zero image is a simultaneous eigenvector. Indeed since π_k is projection onto $\ker(A - \lambda_k)$ the image is λ_k -eigenvector for A , and since B commutes with the projection operators it is still a γ_j -eigenvector as well. Now let

$$\mathcal{C} = \left\{ \pi_k(v_l^j) : j, l, k \in \mathbb{N} \right\}.$$

We claim $\mathcal{C}$ contains a basis for k^n . Indeed every spanning set contains a basis so it suffices to show $\mathcal{C}$ spans k^n . Indeed if $v \in k^n$ then $v = \sum_{l=1}^{\ell} \sum_{j=1}^{n_l} a_{l,j} v_j^l$. Now

$$\begin{aligned} v &= \text{id}_{k^n}(v) = (\pi_1 + \cdots + \pi_m)(v) \\ &= \sum_{k=1}^m \pi_k \left(\sum_{l=1}^{\ell} \sum_{j=1}^{n_l} a_{l,j} v_j^l \right) \\ &= \sum_{k=1}^m \sum_{l=1}^{\ell} \sum_{j=1}^{n_l} a_{l,j} \pi_k(v_j^l) \in \text{span } \mathcal{C} \end{aligned}$$

as desired. □

Problem 4

Statement (10 points). Let $u \in \mathbb{C}$ be a root of the polynomial $m(x) = x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$, and consider the field extension $\mathbb{Q}(u) \subseteq \mathbb{C}$ of $\mathbb{Q}$.

- (a) Show that $m(x)$ is irreducible in $\mathbb{Q}[x]$.
- (b) Define a ring homomorphism $f : \mathbb{Q}[x] \rightarrow \mathbb{C}$ with image $\mathbb{Q}(u)$. Conclude that there is an isomorphism between $\mathbb{Q}(u)$ and a quotient of $\mathbb{Q}[x]$, and specify that quotient ring explicitly.
- (c) What is the degree $[\mathbb{Q}(u) : \mathbb{Q}]$? Give a $\mathbb{Q}$ -basis of $\mathbb{Q}(u)$.
- (d) Express the elements u^4 and u^{-1} in $\mathbb{Q}(u)$ in terms of the basis you gave in part (c).

Solution. (a) $m(x)$ is irreducible by Eisenstein's criterion with $p = 3$.

(b) We define $f(p(x)) = p(u)$ evaluation at u . This is clearly a morphism. Then something is in the kernel if

$$f(p(x)) = p(u) = 0$$

so the kernel is precisely the annihilating polynomials of u . Then clearly $\langle m(x) \rangle \subseteq \ker \phi$. Conversely if $p(x) \in \ker \phi$ since $m(x)$ is irreducible over $\mathbb{Q}$ and monic it is the unique minimal annihilating polynomial for u hence $m(x) \mid p(x)$ so $p \in \langle m \rangle$. Then by the first isomorphism theorem

$$\mathbb{Q}[x] / \langle m(x) \rangle \cong \mathbb{Q}(u).$$

(c) A $\mathbb{Q}$ -basis for $\mathbb{Q}[x] / \langle m \rangle$ is $1, x, x^2$ and its image under our isomorphism is $1, u, u^2$ thus $1, u, u^2$ is a $\mathbb{Q}$ -basis for $\mathbb{Q}(u)$ and

$$[\mathbb{Q}(u) : \mathbb{Q}] = 3 = \deg m(x).$$

(d) We have that

$$m(u) = u^3 - 6u^2 + 9u + 3 = 0$$

so that $u^3 = 6u^2 - 9u - 3$. Then $u^4 = 6u^3 - 9u^2 - 3u$, and again using our relation for u^3 this is

$$u^4 = 6(6u^2 - 9u - 3) - 9u^2 - 3u = 27u^2 - 57u - 18.$$

Then also

$$u^2 - 6u + 9 + 3u^{-1} = 0 \implies u^{-1} = \frac{-u^2 + 6u - 9}{3}.$$

□

Problem 5

Statement (10 points). Let $F = \mathbb{Q}(\sqrt[3]{5})$.

- (a) Find the smallest field K such that $F \subseteq K$ such that K is a Galois extension over $\mathbb{Q}$.
- (b) Prove that K is Galois over F .
- (c) Compute that Galois group $\text{Gal}(K/\mathbb{Q})$ and $\text{Gal}(K/F)$.

Solution. (a) Suppose $F \subseteq K$ and K is Galois. Then since $\sqrt[3]{5} \in K$ it contains a root of $x^3 - 5$ and since it is normal it must contain all the roots thus contain the splitting field of $x^3 - 5$. Then splitting fields are Galois so the smallest Galois extension containing $\sqrt[3]{5}$ is the splitting field for $x^3 - 5$. Then $x^3 - 5$ factors as

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

so if K splits $x^3 - 5$ it contains $\sqrt[3]{5}$ and $w = \sqrt[3]{5}^{-1} \cdot w\sqrt[3]{5}$ thus contains $\mathbb{Q}(\sqrt[3]{5}, w)$. Conversely $\mathbb{Q}(\sqrt[3]{5}, w)$ contains all the roots of $x^3 - 5$ so contains K thus $K = \mathbb{Q}(\sqrt[3]{5}, w)$.

(b) We claim K is the splitting field for

$$\begin{aligned} m(x) &= (x - w\sqrt[3]{5}) (x - w^2\sqrt[3]{5}) = (x^2 - x(w + w^2)\sqrt[3]{5} + \sqrt[3]{5}^2) \\ &= x^2 + x\sqrt[3]{5} + \sqrt[3]{5}^2 \end{aligned}$$

over F . Indeed $m(x)$ has degree 2 so it is irreducible over F since none of its roots are in F . Then if F_m is the splitting field over F it must contain $w\sqrt[3]{5}$ and thus w so contains $F(w) = K$. Conversely $m(x)$ splits in $F(w)$ so $F_m = K$. Then splitting fields are Galois so K is Galois over F .

Remark. This is always true. Any Galois extension is still Galois over any intermediate subfield. This essentially comes from the definition that Galois extensions are algebraic. Every element has a minimal polynomial over the base field. Then the minpoly over the base must be divisible by the minpoly over the intermediate extension so normality and separability pass to the minpoly over the intermediate extension. See *graduate algebra notes.pdf* worksheet 20 part C for details.

(c) Recall that if L/K is Galois then

$$|\text{Gal}(L/K)| = [L : K].$$

Then $[K : F] = 2$ and there is only one group of order two namely C_2 . More explicitly this corresponds to the complex conjugation automorphism. Now

$$[K : \mathbb{Q}] = [K : F][F : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Then the Galois group of a degree 3 polynomial is a transitive subgroup of S_3 and there is only one subgroup of S_3 of size 6 namely the entire group. $\square$

Problem 6

Statement (10 points). Let R be a ring with unity.

(a) Define what it means for an R -module to be torsion free.

(b) Prove that if F is a free module, then any short exact sequence of R -modules $0 \rightarrow N \rightarrow M \rightarrow F \rightarrow 0$ splits.

(c) Let R be a PID. Show that any finitely generated R -module M can be expressed as a direct sum of a torsion module and a free module. [You may assume that a finitely generated torsion free module over a PID is free.]

Solution. (a) Let M be an R -module. Then $m \in M \setminus \{0\}$ is said to be a torsion element if there is $a \neq 0 \in R$ so that $am = 0$. Then M is torsion free if it has no torsion element.

(b) We have an exact sequence

$$0 \rightarrow N \xrightarrow{f} M \xrightarrow{g} F \rightarrow 0$$

where F is free. Let $\{u_i\}_{i \in I}$ be a basis for F . Then since g is surjective there are $v_i \in M$ so that $g(v_i) = u_i$. Since F is free we may define map out of it by picking an image for its basis. Then we may define $h : F \rightarrow M$ by $h(u_i) = v_i$. Then by construction $g \circ h(u_i) = u_i$ and $g \circ h = \text{id}_F$. Now we claim

$$M = \text{im } f \oplus \text{im } h.$$

Indeed let $m \in M$, and $m' = g(m) = \sum_i a_i u_i \in F$. Then

$$g\left(m - \sum_i a_i v_i\right) = g(m) - \sum_i a_i u_i = 0$$

so the difference $m - \sum_i a_i v_i \in \ker g = \text{im } f$. Let $m'' = m - h(m')$. Then

$$m = h(m') + m'' \in \text{im } f + \text{im } h.$$

It remains to show $\text{im } f \cap \text{im } h = \{0\}$. Indeed suppose m is in the intersection. Then $m = h(m')$ so that

$$0 = g(m) = g(h(m')) = m'.$$

Then since h is a morphism $h(m') = m = 0$ as well.

(c) Let M be an R -module and let $T(M)$ denote its torsion submodule. Then we have an exact sequence

$$0 \rightarrow T(M) \xrightarrow{\iota} M \xrightarrow{q} M/T(M) \rightarrow 0$$

where ι is inclusion and q is the quotient map. Then $\frac{M}{T(M)}$ is torsion free since it is finitely generated over a PID. Then by part (b) we know M splits as

$$M = T(M) \oplus M/T(M).$$

Remark. Torsion free implies when your finitely generated over a PID by the structure theorem. Suppose R is a PID and M an f.g R -module. Then

$$M \cong R/P_1 \oplus \cdots \oplus R/P_m$$

where the $P_i = \langle p_i^{a_i} \rangle$ are primary ideals. Then if any $P_i \neq 0$ we have torsion elements. For example if $P_1 \neq 0$ then $(1 + P_1, 0, \dots, 0)$ is torsion element since it is annihilated by the non-zero element $p_1^{a_1} \in R$.

□

Problem 7

Statement (10 points). Consider the matrix in $M_3(\mathbb{C})$

$$A = \begin{pmatrix} 0 & -1 & 2 \\ 3 & 8 & -14 \\ 3 & 6 & -10 \end{pmatrix}.$$

(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) We have

$$\det(A - \lambda) = \det \begin{bmatrix} -\lambda & -1 & 2 \\ 3 & 8 - \lambda & -14 \\ 3 & 6 & -10 - \lambda \end{bmatrix}$$

I find its best to just not do any row operations. Just compute the terms for each minor and add them. We expand along the top row.

1st minor $-\lambda$ multiplier

$$\begin{aligned} -\lambda \det \begin{pmatrix} 8 - \lambda & -14 \\ 6 & -10 - \lambda \end{pmatrix} &= -\lambda [(8 - \lambda)(-10 - \lambda) + 84] \\ &= -\lambda [\lambda^2 + 2\lambda + 4] \\ &= -(\lambda^3 + 2\lambda^2 + 4\lambda) \end{aligned}$$

2nd minor 1 multiplier

$$\det \begin{bmatrix} 3 & -14 \\ 3 & -10 - \lambda \end{bmatrix} = -(30 + 3\lambda) + 42 = -3\lambda + 12 = 3(4 - \lambda)$$

3rd minor 2 multiplier

$$\begin{aligned} 2 \det \begin{bmatrix} 3 & 8 - \lambda \\ 3 & 6 \end{bmatrix} &= 2(18 - 3(8 - \lambda)) = 2(18 - 24 + 3\lambda) \\ &= 2(-6 + 3\lambda) = 6\lambda - 12 \end{aligned}$$

Then adding all of these the char poly should be

$$\begin{aligned} \chi_A(\lambda) &= -\lambda^3 - 2\lambda^2 - 4\lambda - 3\lambda + 12 + 6\lambda - 12 \\ &= -\lambda^3 - 2\lambda^2 - \lambda = -\lambda(\lambda^2 + 2\lambda + 1) \\ &= -\lambda(\lambda + 1)^2 \end{aligned}$$

so we have two eigenvalues $0, -1$ and there is just a 1×1 block for the 0 eigenvalue. Then to determine the form we just need to check how many chains for have the -1 eigenvalue. We have

$$A + 1 = \begin{bmatrix} 1 & -1 & 2 \\ 3 & 9 & -14 \\ 3 & 6 & -9 \end{bmatrix}$$

This row reduces to

$$\begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -5 \\ 0 & 0 & 0 \end{bmatrix}$$

so this has rank 2 and there is only one chain. Then we may conclude our JCF is

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

(b) We need to find an eigenvector for 0 and a rank 2 eigenvector for -1 . We have

$$A \sim \begin{bmatrix} 0 & -1 & 2 \\ 0 & 0 & 0 \\ 3 & 0 & 2 \end{bmatrix}$$

so

$$\begin{pmatrix} -\frac{2}{3} \\ 2 \\ 1 \end{pmatrix}$$

spans the kernel and we can take 3 times this to get $(-2, 6, 3)$ to be our eigenvector.

Now

$$(A + 1)^2 = \begin{bmatrix} 4 & 4 & -2 \\ -12 & -6 & 6 \\ -6 & -3 & 3 \end{bmatrix}$$

It's easy to see this isn't full rank because the last row is half the second. Something in the kernel is $(-\frac{1}{2}, 2, 1)$ so $(-1, 4, 2)$ is as well. Neither of these is in the kernel of $A + 1$ so we have our rank 2 eigenvector.

An easier rank two eigenvector however is $(1, -1, 1)$. Then its image is easy to compute

$$(A + 1) \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -20 \\ -12 \end{pmatrix}$$

so we have

$$P = \begin{bmatrix} -2 & 4 & 1 \\ 6 & -20 & -1 \\ 3 & -12 & 1 \end{bmatrix}.$$

□