

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS
Solutions to September 2005 Algebra QR exams

MORNING

(1) Consider the ring $R = \mathbb{Z}[X]$.

(a) Is R a principal ideal domain? (Prove your answer.)

Solution. Suppose that $I = (2, X) = (a)$ for $a \in \mathbb{Z}[X]$. a divides 2 and X , hence a must be ± 1 . Clearly $1 \notin (2, X)$ because $\mathbb{Z}/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$. Contradiction, so I is not principal.

(b) Find a prime ideal \mathfrak{p} such that R/\mathfrak{p} has 4 elements.

Solution. Take $\mathfrak{p} = (2, X^2 + X + 1)$. Then $\mathbb{Z}/\mathfrak{p} \cong \mathbb{F}_2[X]/(X^2 + X + 1) \cong \mathbb{F}_4$ because $X^2 + X + 1$ is irreducible over \mathbb{F}_2 . Now \mathfrak{p} is a prime ideal because \mathbb{Z}/\mathfrak{p} is a field.

(c) Show that

$$M = \mathbb{Z}[X]/(X^2 - 5X - 2, 4X + 2).$$

is a finitely generated abelian group. Determine its structure.

Solution. $(X^2 - 5X - 2, 4X + 2) = (X^2 - X, 4X + 2)$.

$$\mathbb{Z}/(X^2 - X) \cong \mathbb{Z}[X]/(X) \times \mathbb{Z}[X]/(X - 1) \cong \mathbb{Z} \times \mathbb{Z}.$$

Using this isomorphism, $4X + 2$ corresponds to $(2, 6)$ in $\mathbb{Z} \times \mathbb{Z}$. The ideal in $\mathbb{Z} \times \mathbb{Z}$ generated by $(2, 6)$ contains $(2, 0)$ and $(0, 6)$. So we have

$$\mathbb{Z}/(X^2 - X, 4X + 2) \cong \mathbb{Z} \times \mathbb{Z}/(2\mathbb{Z} \times 6\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

(2) Suppose that V and W are \mathbb{C} -vector spaces of dimension n and m respectively.

(a) Suppose that e_1, e_2, \dots, e_n is a basis of V and $e_1^*, e_2^*, \dots, e_n^*$ is a dual basis in V^* .

We define a map $\Theta : \text{Hom}_{\mathbb{C}}(V^*, W) \rightarrow V \otimes W$ by

$$\Theta(\phi) = \sum_{i=1}^n e_i \otimes \phi(e_i^*).$$

Prove that Θ is a linear isomorphism.

Solution. Θ is linear:

$$\begin{aligned} \Theta(\lambda\phi + \mu\psi) &= \sum_{i=1}^n e_i \otimes (\lambda\phi + \mu\psi)(e_i^*) = \sum_{i=1}^n \lambda(e_i \otimes \phi(e_i^*)) + \mu(e_i \otimes \psi(e_i^*)) = \\ &= \lambda \sum_{i=1}^n e_i \otimes \phi(e_i^*) + \mu \sum_{i=1}^n e_i \otimes \psi(e_i^*) = \lambda\Theta(\phi) + \mu\Theta(\psi) \end{aligned}$$

for all $\lambda, \mu \in \mathbb{C}$ and $\phi, \psi \in \text{Hom}_{\mathbb{C}}(V^*, W)$.

Every element x in $V \otimes W$ can be written in the form $x = \sum_{i=1}^n e_i \otimes f_i$ for some $f_1, f_2, \dots, f_n \in W$. There is a unique linear map $\phi \in \text{Hom}_{\mathbb{C}}(V^*, W)$ such that $\phi(e_i^*) = f_i$ for $i = 1, 2, \dots, n$. Then $\Theta(\phi) = \sum_{i=1}^n e_i \otimes \phi(e_i^*) = \sum_{i=1}^n e_i \otimes f_i = x$. This shows that Θ is onto. The uniqueness of ϕ implies that Θ is injective. Therefore, Θ is a linear isomorphism.

- (b) Prove that the map Θ does not depend on the choice of the bases e_1, \dots, e_n (as long as we choose e_1^*, \dots, e_n^* dual to it).

Solution. There is a unique linear map $\Pi : V \otimes W \rightarrow \text{Hom}_{\mathbb{C}}(V^*, W)$ such that $\Pi(e \otimes f)(g) = g(e)f$ for all $e \in V, f \in W$ and $g \in V^*$. For any i and any $f \in W$ we have

$$(\Theta \circ \Pi)(e_i \otimes f) = \sum_{j=1}^n e_j \otimes \Pi(e_i \otimes f)(e_j^*) = \sum_{j=1}^n e_j \otimes (e_j^*(e_i))f = e_i \otimes f.$$

Since such elements $e_i \otimes f$ span $V \otimes W$, $\Theta \circ \Pi$ equals the identity. Now Π clearly did not depend on the choice of e_1, \dots, e_n , therefore, neither does Θ .

- (c) Suppose that $x \in V \otimes W$. Show that one can choose a bases e_1, \dots, e_n of V and f_1, \dots, f_m of W such that

$$x = e_1 \otimes f_1 + e_2 \otimes f_2 + \dots + e_r \otimes f_r$$

for some r . (You could use for example part (a).)

Solution. If $x \in V \otimes W$, then $\Theta^{-1}(x) \in \text{Hom}_{\mathbb{C}}(V^*, W)$ is a linear map of a certain rank r . With respect to some bases e_1^*, \dots, e_n^* and f_1, \dots, f_m of W , the matrix A of $\phi = \Theta^{-1}(x)$ is as follows: $A_{i,i} = 1$ for $i = 1, 2, \dots, r$ and $A_{i,j} = 0$ for all other (i, j) . We have

$$x = \Theta(\phi) = \sum_{i=1}^n e_i \otimes \phi(e_i^*) = \sum_{i=1}^r e_i \otimes f_i.$$

- (3) For which primes p and positive integers is every p -Sylow subgroup of the symmetric group Sym_n commutative?

Solution: If $n < p^2$, then there exists an r such that $rp \leq n < (r+1)p$. Then $n!$ (the order of S_n) is divisible by p^r , but not by p^{r+1} . The order of a p -Sylow subgroup is p^r . The group $(\mathbb{Z}/p\mathbb{Z})^r \subseteq \text{Sym}_p^p \subseteq \text{Sym}_n$ is abelian of order p^r . Hence it is a p -Sylow group and all p -Sylow groups must be abelian because all of them are conjugate.

Suppose that $n \geq p^2$. Define

$$\sigma_i = (i \ p+i \ 2p+i \ \dots \ p^2-p+i)$$

for $i = 1, 2, \dots, p$ and

$$\tau = (1 \ 2 \ 3 \ \dots \ p)(p+1 \ p+2 \ \dots \ 2p) \dots (p^2-p+1 \ p^2-p+2 \ \dots \ p^2).$$

The group generated by $\sigma_1, \dots, \sigma_p, \tau$ is isomorphic to

$$G = \mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/p\mathbb{Z})^p$$

Now G is contained in some p -Sylow subgroup of Sym_n . Since G is nonabelian, so is the p -Sylow group.

- (4) Suppose that A is an invertible complex 3×3 matrix such that A and A^2 are conjugate. What are the possible Jordan normal forms of A .

Solution:

The eigenvalues of A are nonzero. If $\lambda_1, \lambda_2, \lambda_3$ are the eigenvalues of A , then so are $\lambda_1^2, \lambda_2^2, \lambda_3^2$. Hence squaring permutes the eigenvalues. This permutation may be a 3-cycle, a 2 cycle and a 1-cycle, or three 1-cycles.

3-cycle: $\lambda_1^2 = \lambda_2, \lambda_2^2 = \lambda_3, \lambda_3^2 = \lambda_1$.

Then $\lambda_1^8 = \lambda_1$, so $\lambda_1^7 = 1$. There are two possibilities

$$\begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^2 & 0 \\ 0 & 0 & \zeta_7^4 \end{pmatrix}, \begin{pmatrix} \zeta_7^3 & 0 & 0 \\ 0 & \zeta_7^6 & 0 \\ 0 & 0 & \zeta_7^5 \end{pmatrix}$$

where ζ_7 is a primitive 7-th root of unity.

2-cycle and a 1-cycle: $\lambda_1^2 = \lambda_2, \lambda_2^2 = \lambda_1$ and $\lambda_3^2 = \lambda_3$. So λ_1 is a third root of unity and $\lambda_3 = 1$. We get

$$\begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where ζ_3 is a primitive third root of unity.

3 1-cycles: In this case all the eigenvalues are 1. If A is a $n \times n$ Jordan block with eigenvalue 1, then $A - I$ has rank $n - 1$. But then $A^2 - I = (A - I)(A + I)$ also has rank $n - 1$ because $A + I$ is invertible. This means that A^2 is also conjugate to a Jordan block with eigenvalue 1. So any matrix A with eigenvalues all 1 is conjugate to its square. This gives us the following possible Jordan normal forms:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

- (5) Let q be a prime power and m an integer. For the field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ we have the trace map T and the norm map N defined by $T(x) := \sum_{i=0}^{m-1} x^{q^i}$ and $N(x) := \prod_{i=0}^{m-1} x^{q^i}$, respectively. These maps have domain \mathbb{F}_{q^m} and codomain \mathbb{F}_q .

(a) Prove that T is onto.

Solution: First proof. There exists a degree m irreducible polynomial $g(x) \in \mathbb{F}_q[x]$ so that \mathbb{F}_{q^m} is the splitting field.

Let x_1, \dots, x_m be roots of $g(x)$. Choose indices so that $x_j = x_1^{q^{j-1}}$, for $j = 1, 2, \dots, m$ (this can be done since the root set is an orbit under the Galois group, which is generated by the Frobenius map). Then the $m \times m$ van der Monde matrix (x_i^j) is nonsingular. It follows that for any nonzero m -tuple (a_1, \dots, a_m) in \mathbb{F}_q , there exist a k so that $\sum_i a_i x_i^k \neq 0$. The trace of x_1^k is the special case $(a_1, \dots, a_m) = (1, 1, \dots, 1)$. (Note that x_1^k, \dots, x_m^k is a length m orbit of the Galois group so is the complete set of roots for a degree m irreducible polynomial.)

Second proof.

The trace is transitive over iterated field extensions, so it suffices to do the case where m is prime.

If m is unequal to the characteristic, then trace restricted to the prime field is just multiplication by m so is onto (this observation solves part (c)).

Suppose $m = p$, the characteristic. We take any scalar c outside the prime field. Its minimal polynomial is an irreducible of degree p . We are done if the coefficient at x^{p-1} is nonzero. Sometimes it is 0, depending on c , but it suffices by

the theory of finite fields to exhibit a degree p irreducible where this coefficient is nonzero.

Since $x^q - x - 1$ has no roots in the ground field, every irreducible divisor has degree p . Change variables $y = x^{-1}$ and deduce that for $1 - y^{q-1} - y^q$, every irreducible divisor has degree p . Therefore, some irreducible divisor of it has nonzero second-highest coefficient.

- (b) Prove that N is onto.

Solution. The multiplicative group of the larger field is cyclic of order $a := q^m - 1$. The norm map raises every element to the power $b := 1 + q + q^2 + \dots + q^{m-1}$. Since $b|a$, the kernel of the norm map restricted to $\mathbb{F}_{q^m}^\times$ has order b . The image therefore has order $a/b = q - 1$, whence onto.

- (c) Give necessary and sufficient conditions on q and m which makes the restriction of T to \mathbb{F}_q onto.

Solution. $(m, q) = 1$.

- (d) Give necessary and sufficient conditions on q and m which makes the restriction of N to \mathbb{F}_q onto.

Solution. $(m, q - 1) = 1$.

AFTERNOON

- (1) Suppose that $A, B, C \in M_n(\mathbb{C})$ are matrices such that A commutes with B and C , but B and C do not commute. Prove that the minimum polynomial of A has degree at most $n - 1$.

Solution. We deny the conclusion and have that the minimum polynomial of A has degree n . Then there exists a cyclic vector. An easy argument shows that a linear transformation which commutes with A is a polynomial in A . If so, B and C are each polynomials in A and so commute with each other, contradiction.

- (2) (a) Prove that if a group H acts on a set and K is a normal subgroup of H , then H leaves invariant the set of fixed points of K .
 (b) Suppose that the finite group G acts transitively on the set Ω . Let P be a p -Sylow subgroup of G for a prime number p . Prove that $N(P)$, the normalizer of P , acts transitively on the set of fixed points of P on Ω (when this set of fixed points is nonempty).

Solution. We use right action. (a) If a is a point fixed by K and $g \in H$, then $(ag)H = a(gH) = a(Hg) = (aH)g = ag$, whence ag is fixed by H . (b) Let a, b be points fixed by P . Take $g \in G$ so that $ag = b$. Then $g^{-1}Pg$ fixes b . By Sylow's theorem applied to the subgroup $Stab_G(b)$, there exists $h \in Stab_G(b)$ so that $P = h^{-1}(g^{-1}Pg)h = (gh)^{-1}Pgh$, whence $gh \in N(P)$. Now check that $a(gh) = (ag)h = bh = b$.

- (3) Let p be a prime and let \mathbb{F}_q be a finite field of $q = p^m$ elements.
 (a) Prove that if $x \in GL_2(\mathbb{F}_q)$ is a nonidentity element of order a power of p , then its order is p and its minimal polynomial is $(t - 1)^2$. Such an element fixes a unique 1-dimensional space.

Solution. If $x^{p^m} = 1$, then x satisfies the polynomial $t^{p^m} - 1 = (t - 1)^{p^m}$. Since the minimal polynomial of x has degree at most 2, x satisfies $t^p - 1 = 0$, so x has order p . Its minimal polynomial is therefore $(t - 1)^2$.

Since 1 is an eigenvalue, x fixes a 1-space. If x fixes two independent 1-spaces, x is diagonalizable. Since its minimal polynomial has a repeated factor, this is a contradiction.

- (b) Prove that Ω , the set of 1-dimensional subspaces in \mathbb{F}_q^2 , has cardinality $1 + q$.

Solution. This is clear by partitioning $\mathbb{F}_q^2 \setminus \{0\}$ by the relation of linear dependence.

- (c) Prove that an element of $GL_2(\mathbb{F}_q)$ fixes exactly one point of Ω if and only if it has order divisible by p .

Solution. If $x \in GL_2(\mathbb{F}_q)$ has order p , it fixes a unique 1-space, and so does any abelian subgroup (e.g., cyclic) of $GL_2(\mathbb{F}_q)$ which contains x . (Reason: if y commutes with x , then y stabilizes the set of points fixed by x : see problem (2) in the Afternoon Algebra QR Exam.)

Conversely, suppose that x fixes a unique 1-space. Then x has an eigenvalue, so its (degree 2) characteristic polynomial factorizes $(t - a)(t - b)$. Since there is just one fixed 1-space, $a = b$ since eigenspaces are fixed by x . If the minimal polynomial of x has degree 1, then x is a scalar, which fixes all 1-spaces. Therefore x has minimum polynomial $(t - a)^2$. Therefore $y := a^{-1}x$ has minimal polynomial

$(t-1)^2$. Therefore y has order p since it satisfies $(t-1)^p = t^p - 1$. The scalar a has order k dividing $q-1$. Therefore x has order kp .

- (4) Let E_1, E_2 be subfields of the algebraic closure \bar{F} of the field F . Assume that E_i/F is a finite degree Galois extension for $i = 1, 2$ and that $\text{Gal}(E_1/F) \cong \text{Dih}_{10}$ and $\text{Gal}(E_2/F) \cong \text{Dih}_{14}$. (Here Dih_{2n} is the dihedral group of order $2n$.) The compositum E_1E_2 is the subfield of \bar{F} generated by E_1 and E_2 .

There is a homomorphism of groups

$$\phi = (r_1, r_2) : \text{Gal}(E_1E_2/F) \rightarrow \text{Gal}(E_1/F) \times \text{Gal}(E_2/F),$$

where r_i is the restriction to the subfield E_i/F , for $i = 1, 2$.

- (a) Prove that ϕ is a monomorphism.

Solution. An element in $\text{Ker}(\phi)$ fixes both E_1 and E_2 elementwise, hence also the field they generate.

- (b) Prove that $|\text{Im}(\phi)| = 2 \cdot 5 \cdot 7$ or $2^2 \cdot 5 \cdot 7$.

Solution. From Galois theory, any automorphism of a normal field extension extends to any normal overextension. Therefore each of r_1 and r_2 is onto. Therefore $\text{Im}(\phi)$ has order divisible by each of $\text{Gal}(E_i/F)$ hence also by their least common multiple.

- (c) In case $|\text{Im}(\phi)| = 2 \cdot 5 \cdot 7$, prove that $\text{Im}(\phi)$ is dihedral of order 70.

Solution. Let $G = \text{Gal}(E_1E_2/F)$ and let $G_i = \text{Gal}(E_1E_2/E_i)$. Then each G_i is a normal subgroup of G . Since each r_i is onto, we have $G_1 \cong \mathbb{Z}_7$ and $G_2 \cong \mathbb{Z}_5$. Since $G_1 \cap G_2 = 1$, $G_1G_2 = G_1 \times G_2 \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$. A Sylow 2-group of G has order just 2. Let t be a generator. The restrictions of conjugation by t to each E_i is nontrivial (inversion, in both cases), so conjugation by t inverts the cyclic group G_1G_2 . Therefore, $G = G_1G_2\langle t \rangle$ is dihedral.

- (5) Consider the $\mathbb{C}[X]$ -modules $M_1 := \mathbb{C}[X]/(X^6 - X^2)$ and $M_2 := \mathbb{C}[X]/(X^9 - X^3)$. Let $M = M_1 \otimes_{\mathbb{C}[X]} M_2$ be the tensor product of M_1 and M_2 as $\mathbb{C}[X]$ -modules. Write M as a finite direct sum of cyclic modules of the form $\mathbb{C}[X]/((X-a)^m)$, $a \in \mathbb{C}$, $m \in \mathbb{N}$.

Solution. In general we prove that

$$\mathbb{C}[X]/(p(X)) \otimes_{\mathbb{C}[X]} \mathbb{C}[X]/(q(X)) = \mathbb{C}[X]/(p(X), q(X))$$

for any polynomials $p(X)$ and $q(X)$. Consider the homomorphism

$$\phi : \mathbb{C}[X] \rightarrow \mathbb{C}[X]/(p(X)) \otimes_{\mathbb{C}[X]} \mathbb{C}[X]/(q(X)).$$

defined by

$$\phi(1) = \bar{1} \otimes \bar{1}.$$

It is easy to see that ϕ is onto because $\mathbb{C}[X]/(p(X)) \otimes_{\mathbb{C}[X]} \mathbb{C}[X]/(q(X))$ is spanned by elements of the form

$$\overline{a(X)} \otimes \overline{b(X)} = a(X)b(X) \cdot \bar{1} \otimes \bar{1} = a(X)b(X)\phi(1) = \phi(a(X)b(X))$$

Clearly $p(X)$ and $q(X)$ lie in its kernel, so ϕ induces a homomorphism

$$\bar{\phi} : \mathbb{C}[X]/(p(X), q(X)) \rightarrow \mathbb{C}[X]/(p(X)) \otimes_{\mathbb{C}[X]} \mathbb{C}[X]/(q(X)).$$

such that $\bar{\phi}(\bar{1}) = \bar{1} \otimes \bar{1}$.

Conversely, consider the homomorphisms $\psi_1 : \mathbb{C}[X]/(p(X)) \rightarrow \mathbb{C}[X]/(p(X), q(X))$
 $\psi_2 : \mathbb{C}[X]/(q(X)) \rightarrow \mathbb{C}[X]/(p(X), q(X))$. There is a unique homomorphism

$$\psi : \mathbb{C}[X]/(p(X)) \otimes_{\mathbb{C}[X]} \mathbb{C}[X]/(q(X)) \rightarrow \mathbb{C}[X]/(p(X), q(X))$$

such that $\psi(f \otimes g) = \psi_1(f)\psi_2(g)$. In particular,

$$\psi(\bar{1} \otimes \bar{1}) = \psi_1(\bar{1})\psi_2(\bar{1}) = \bar{1} \cdot \bar{1} = \bar{1}.$$

Therefore

$$\psi(\overline{\phi}(\bar{1})) = \psi(\bar{1} \otimes \bar{1}) = \bar{1}$$

so the composition $\psi \circ \overline{\phi}$ is equal to the identity and $\overline{\phi}$ is injective. Therefore $\overline{\phi}$ is a bijection and an isomorphism of $\mathbb{C}[X]$ -modules.

In particular we have

$$M = M_1 \otimes_{\mathbb{C}[X]} M_2 = \mathbb{C}[X]/(X^6 - X^2, X^9 - X^3)$$

A GCD computation (say using Euclid's algorithm for polynomials) shows that the greatest common divisor of $X^9 - X^3$ and $X^6 - X^2$ is $X^4 - X^2 = X^2(X - 1)(X + 1)$. By the Chinese Remainder Theorem, we have

$$\mathbb{C}[X]/(X^2(X - 1)(X + 1)) \cong \mathbb{C}[X]/(X^2) \times \mathbb{C}[X]/(X - 1) \times \mathbb{C}[X]/(X + 1).$$