

UNIVERSITY OF MICHIGAN
DEPARTMENT OF MATHEMATICS
Solutions to January 2008 Algebra QR Exams
MORNING

Problem 1. Consider the action of G on the set of left congruence classes $(G/H)_\ell$, given by $g \cdot (uH) = guH$. This gives a homomorphism

$$G \rightarrow S((G/H)_\ell) \simeq S_n,$$

whose kernel is $H' := \bigcap_{x \in G} xHx^{-1}$. Therefore $[G: H']$ divides $|S_n| = n!$, by Lagrange's Theorem.

Suppose now that H is not normal, hence H' is a proper subgroup of H . Since $[G: H'] = [G: H] \cdot [H: H']$, we deduce from the first part that $[H: H']$ divides $(n-1)!$. If p is a prime that divides $[H: H']$, then p divides $|G|$ and $p \leq n$. Since n is prime and p divides $(n-1)!$, we deduce that in fact $p < n$, a contradiction with the assumption that n is the minimal prime factor of $|G|$.

Problem 2. Let K denote the splitting field of f in an algebraic closure of \mathbb{Q} . Since $G = G(K/\mathbb{Q})$ is abelian, it follows that every subgroup of G is normal in G . By Galois theory, this implies that every subextension $k \subseteq K$ is normal over \mathbb{Q} .

If u is a root of f in K , since $\mathbb{Q}(u)$ is normal over \mathbb{Q} , we deduce that all the other roots of f lie in $\mathbb{Q}(u)$, hence $K = \mathbb{Q}(u)$. Since f is irreducible of degree n , we conclude that $n = \deg(\mathbb{Q}(u)/\mathbb{Q}) = \deg(K/\mathbb{Q}) = m$.

The group G does not have to be cyclic. Consider, for example, the extension $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ of \mathbb{Q} . This is normal, as the composite of two normal extensions. Using the Primitive Element Theorem, we can write $L = \mathbb{Q}(u)$ for some u , and L is the splitting field of the minimal polynomial f of u . The Galois group of L/\mathbb{Q} is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Problem 3. We have an isomorphism $K[A] \simeq K[x]/(f)$, where $f \in K[x]$ is the minimal polynomial of A over K . Note that $\mathbb{C}[A] = K[A] \otimes_K \mathbb{C} \simeq \mathbb{C}[x]/(f)$.

For a), note first that a product of fields is a reduced ring. This shows that if $K[A]$ is a product of fields, then $f \in K[x]$ is reduced. The converse follows from the Chinese Remainder Theorem: if $f = f_1 \cdots f_r$, where the f_i are non-associated irreducible polynomials, then

$$K[x]/(f) \simeq \prod_{i=1}^r K[x]/(f_i),$$

and each $K[x]/(f_i)$ is a field.

On the other hand, f is reduced if and only if f splits over \mathbb{C} as a product of linear factors. Therefore b) follows if we show that a matrix M over \mathbb{C} is diagonalizable if and only if its minimal polynomial is reduced, i.e. a product of distinct linear factors. It is

clear that if M is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_r$ (with suitable multiplicities), then the minimal polynomial of M is equal to $\prod_i (x - \lambda_i)$. The converse follows from the Jordan Decomposition of M : if this contains an s -bloc with λ on the diagonal and 1 above the diagonal, then $(x - \lambda)^{s-1}$ divides the minimal polynomial of M .

Alternatively, this can be seen also directly, as follows. If u is an endomorphism of a vector space V over a field such that $\prod_{i=1}^r (u - \lambda_i) = 0$ for distinct λ_i , then $V = \bigoplus_{i=1}^r \text{Ker}(u - \lambda_i)$. This in turn follows by induction on r via the following statement: if P and Q are relatively prime polynomials with coefficients in the given field such that $P(u)Q(u) = 0$, then $V = \text{Ker}(P(u)) \oplus \text{Ker}(Q(u))$. To see this, note first that $P(u)Q(u) = 0$ implies

$$\text{Im}(P(u)) \subseteq \text{Ker}(Q(u)), \quad \text{Im}(Q(u)) \subseteq \text{Ker}(P(u)).$$

On the other hand, since P and Q are relatively prime, we can find polynomials C and D such that $PC + QD = 1$. For every $v \in V$, if v_1 is the value of $C(u)$ at v and v_2 is the value of $D(u)$ at v , then

$$v = Q(u)(v_2) + P(u)(v_1) \in \text{Ker}(P(u)) + \text{Ker}(Q(u)).$$

Moreover, if both $P(u)$ and $Q(u)$ vanish on $v \in V$, then the relation $CP + DQ = 1$ implies $v = 0$. This completes the proof.

Problem 4. We can write

$$\begin{aligned} \sum_{g \in G} |X^g| &= \sum_{g \in G} \sum_{x \in X, gx=x} 1 = |\{(g, x) \in G \times X \mid gx = x\}| \\ &= \sum_{x \in X} \sum_{g \in G, gx=x} 1 = \sum_{x \in X} |G_x|, \end{aligned}$$

which gives the first equality.

Suppose now that $x = hu$ for some $u \in X$ and $h \in G$. For $g \in G$, we have $gx = x$ if and only if $ghu = hu$, which is the case if and only if $h^{-1}gh \in G_u$. Therefore $G_x = hG_u h^{-1}$. This implies that $|G_x|$ is constant, when x varies in one orbit. Moreover, the number of elements in the orbit Gu is $(G : G_u)$. We deduce that for every orbit O

$$\sum_{x \in O} |G_x| = |O| \cdot |G_x| = (G : G_x) \cdot |G_x| = |G|.$$

Hence $\sum_{x \in G} |G_x|$ is equal to $|G|$ times the number of orbits.

Problem 5. Define $\tilde{T}: V \times V \times V \rightarrow V \otimes_F V \otimes_F V$ by $\tilde{T}(u, v, w) = w \otimes u \otimes v$. Since \tilde{T} is multilinear, the universal property of the tensor product implies the existence and uniqueness of the linear map T .

Let $\{e_i \mid 1 \leq i \leq n\}$ be a basis of V over F . The vector space $W = V \otimes V \otimes V$ has a basis given by the elements $f_{ijk} := e_i \otimes e_j \otimes e_k$, where $i, j, k \in \{1, \dots, n\}$. We define some vector subspaces W_{ijk} of W , as follows. If at least two of i, j, k are distinct, then let W_{ijk} be the 3-dimensional vector subspace of W spanned by f_{ijk}, f_{kij} , and f_{jki} . We have $(n^3 - n)/3$ such subspaces. On the other hand, we let W_{ijk} be spanned by f_{ijk} if

$i = j = k$. Therefore we get n such 1-dimensional subspaces. Note that in this way we express W as the direct sum of $\frac{n^3-n}{3} + n$ subspaces.

It is clear from the definition of T that $T(f_{ijk}) = f_{kij}$ for every i, j , and k . It follows that each subspace W_{ijk} is T -stable. Since W is the direct sum of invariant subspaces, it follows that the minimal polynomial of T is the least common multiple of the minimal polynomials corresponding to each subspace, while the characteristic polynomial is the product of the corresponding characteristic polynomials.

If $i = j = k$, then T is the identity on W_{ijk} , hence both the minimal and the characteristic polynomials on such a subspace are equal to $(x - 1)$. Suppose now that at least two of i, j , and k are distinct. In the basis given by f_{ijk}, f_{kij} , and f_{jki} , the map T is described by the matrix

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

It follows that the characteristic polynomial of $T|_{W_{ijk}}$ is equal to the determinant of the matrix

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

hence it is equal to $x^3 - 1$. This is also the minimal polynomial of $T|_{W_{ijk}}$: if $\text{char}(F) \neq 3$, this follows from the fact that $x^3 - 1$ has distinct roots (in an algebraic closure of F), while it is known that the minimal polynomial divides the characteristic polynomial, and they have the same roots. If $\text{char}(k) = 3$, then $x^3 - 1 = (x - 1)^3$, and it is enough to note that $(T - 1)^2(f_{ijk}) = f_{jki} - 2f_{kij} + f_{ijk} \neq 0$.

We deduce that the minimal polynomial of T is equal to $(x^3 - 1)$, and its characteristic polynomial is equal to $(x^3 - 1)^{\frac{n^3-n}{3}}(x - 1)^n$.

AFTERNOON

Problem 1. We denote by \sim the equivalence relation on matrices induced by multiplication with an invertible matrix, either on the left or on the right. Performing row and column operations on M , we get

$$\begin{pmatrix} 2 & 8 \\ 4 & 10 \\ 6 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 8 \\ 0 & -6 \\ 0 & -12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & -6 \\ 0 & -12 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & -6 \\ 0 & 0 \end{pmatrix}$$

This implies $M \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}$. In order to compute $\text{Hom}(M, \mathbb{Z}/3\mathbb{Z})$ we use that fact that $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is isomorphic to the subgroup of $\mathbb{Z}/n\mathbb{Z}$ consisting of elements annihilated by m , hence it is isomorphic to $\mathbb{Z}/a\mathbb{Z}$, where $a = n/\text{gcd}(m, n)$. Therefore

$$\text{Hom}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}, \quad \text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) = 0,$$

hence $\text{Hom}(M, \mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ has 9 elements.

Using the fact that the tensor product commutes with direct sums, and $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\text{gcd}(m, n)\mathbb{Z}$, we get

$$M \otimes M \simeq \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\oplus 5} \oplus (\mathbb{Z}/6\mathbb{Z})^{\oplus 3}.$$

Problem 2. If $g \in N_G(S)$, then $gSg^{-1} = S$, hence both P and gPg^{-1} are Sylow p -subgroups of S . By Sylow's Theorem, there is $x \in S$ such that $gPg^{-1} = xPx^{-1}$. Therefore $g^{-1}x \in N_G(P) \subseteq S$, and we deduce $g \in S$. This shows that $N_G(S) = S$, the reverse inclusion being trivial.

Note that by Sylow's theorem, the number of Sylow p -subgroups of G is equal to $[G: N_G(P)]$, and it is congruent to 1 mod p . If S is a subgroup of G , then we clearly have $N_S(P) \subseteq N_G(P)$. Moreover, if $S \supseteq N_G(P)$, then we also have $N_G(P) \subseteq N_S(P)$: if $x \in N_G(P)$, then $x \in S$, hence $x \in N_S(P)$. Therefore in this case $N_G(P) = N_S(P)$. Since P is also a Sylow p -subgroup of S , applying Sylow's Theorem in S , we get

$$[S: N_G(P)] = [S: N_S(P)] \equiv 1 \pmod{p}.$$

Suppose now that T is a subgroup of G containing S . Applying the above argument to T , we deduce $[T: N_G(P)] \equiv 1 \pmod{p}$. Putting these two facts together, and using $[T: S] = [T: N_G(P)]/[S: N_G(P)]$, we get $[T: S] \equiv 1 \pmod{p}$.

Problem 3. 1) By Gauss's lemma, the irreducibility in $K(t)[x]$ is equivalent to the irreducibility in $K[t, x]$, or in $K(x)[t]$, noting in each case that the coefficients are relatively prime; the irreducibility in $K(x)[t]$ is clear since the degree of the polynomial is 1.

2) Let x be a root of f , and set $s = x^2/(1-x)$, which is a p^{th} root of t . Then f has two distinct roots, the roots of the separable equation $X^2 - sX + s = 0$ over $K(s)$. The splitting field is a quadratic extension of $K(s)$, which has degree $2p$ over K .

Problem 4. The implication a) \Rightarrow b) is general, since the only ideals in a DVR are the ideals generated by powers of a uniformizing parameter. For b) \Rightarrow c), if the linear term of F vanishes, the images x and y of X and Y in R give a basis for $\mathfrak{m}/\mathfrak{m}^2$ over K , where \mathfrak{m} is the maximal ideal of R , so \mathfrak{m} cannot be a principal ideal. For c) \Rightarrow a), if $a_{0,1} \neq 0$, then $F = YU - H(X)$, where U is a power series with nonvanishing constant term, and $H(X)$ is a power series in X alone with vanishing constant term. Since U is a unit, we can change variables from (X, Y) to (X, YU) , so we may assume $F = Y - H(X)$, in which case $R \cong K[[X]]$, which is a DVR with uniformizing parameter X .

Problem 5. i) It suffices to find a 2-dimensional subspace W on which ω is nondegenerate. For then V is the direct sum of W and W^\perp . (This is true for any nondegenerate bilinear form, since $W \cap W^\perp = \{0\}$, and W^\perp is the intersection of $\dim(W)$ hyperplanes.) Since ω must be nondegenerate on W^\perp , the conclusion follows by induction. Take any nonzero vector u , and, by the nondegeneracy, take any vector v with $\omega(u, v) \neq 0$. Since u cannot be a multiple of v , the span of u and v is the required W .

ii) By the nondegeneracy of the form, any hyperplane W has the form v^\perp for some nonzero v . Since $\omega(v, v) = 0$, v is contained in W , so W^\perp is contained in v^\perp , as required.

iii) Since W^\perp is defined by $\dim(W)$ linear equations, we have $\dim(W^\perp) \geq \dim(V) - \dim(W)$. Combined with the inequality $\dim(W) \geq \dim(W^\perp)$ (since $W \supset W^\perp$), the conclusion follows.