QR Exam Algebra
September 9, 2017
Morning

Justify your answers. The complex numbers, the real numbers and the finite field with p elements will be denoted by $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{F}_p$ respectively.

(1) Suppose that $f(X) \in \mathbb{F}_2[X]$ is a square-free polynomial of degree 5 with coefficients in $\mathbb{F}_2$, and K is the splitting field of $f(X)$. What are the possibilities for the Galois group of the field extension $K/\mathbb{F}_2$?

(2) Suppose that V and W are nonzero finite dimensional $\mathbb{R}$-vector spaces. The vector space V is equipped with a symmetric bilinear form $(\cdot,\cdot)_V$ and W is equipped with a symmetric bilinear form $(\cdot,\cdot)_W$.

(a) Show that there exists a symmetric bilinear form $(\cdot,\cdot)_{V\otimes W}$ on $V\otimes W$ such that $(v_1 \otimes w_1, v_2 \otimes w_2)_{V\otimes W} = (v_1, v_2)_V (w_1, w_2)_W$ for all $v_1, v_2 \in V$ and $w_1, w_2 \in W$.

(b) Assume that $(\cdot,\cdot)_V$ and $(\cdot,\cdot)_W$ are positive definite. Show that $(\cdot,\cdot)_{V\otimes W}$ is positive definite as well.

(3) Let R be a commutative ring with 1 and M an ideal of R.

(a) Show that, if M is both *maximal* and *principal*, then there is no ideal I of R such that $M \supsetneqq I \supsetneqq M^2$.

(b) Give an example of a commutative ring R, a *maximal* ideal M (but not necessarily principal) of R and an ideal I with $M \supsetneqq I \supsetneqq M^2$.

(4) Define

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

(a) Suppose that A is a complex 4×4 matrix with $AB = 0$. Describe the possibilities for the Jordan normal form of A.

(b) Suppose that A is a complex 4×4 matrix with $AB = BA = 0$. Describe the possibilities for the Jordan normal form of A.

(5) Suppose that G is a finite group with whose order is divisible by the prime number p and σ is an automorphism of G such that σ^p is the identity. Show that G has an element g of order p with $\sigma(g) = g$.

QR Exam Algebra
September 9, 2017
Afternoon

Justify your answers. The complex numbers, the real numbers and the finite field with p elements will be denoted by $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{F}_p$ respectively.

(1) Suppose that A is a complex 5×5 matrix with minimal polynomial $X^5 - X^3$.
   (a) What is the characteristic polynomial of A^2?
   (b) What is the minimal polynomial of A^2?

(2) Let $G = \mathrm{GL}_n(\mathbb{F}_p)$ be the group of invertible $n \times n$ matrices with coefficients in $\mathbb{F}_p$, where p is prime. Then G acts by left multiplication on the $\mathbb{F}_p$-vector space $(\mathbb{F}_p)^n$ consisting of all n-high column vectors with entries in $\mathbb{F}_p$. This induces an action of G on the set S of chains of $\mathbb{F}_p$-vector spaces $0 \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots \subsetneqq V_n = (\mathbb{F}_p)^n$ in which $\dim V_i = i$.
   (a) Determine the size of S.
   (b) Describe the stabilizer in G of the chain in which V_i consists of all n-high column vectors whose bottom $n - i$ entries are all zero.

(3) Let $K = \mathbb{Q}(\sqrt[6]{3}, i)$.
   (a) What is the degree of the field extension $K/\mathbb{Q}$?
   (b) Show that $K/\mathbb{Q}$ is a Galois extension. What is the Galois group of this extension?

(4) For which nonnegative integers a, b is the ring $\mathbb{Z}[X]/(bX - a)$ an integral domain?

(5) Let G be a finite group without any proper characteristic subgroup. This means that for every subgroup H with $\{1\} \subsetneqq H \subsetneqq G$ there exists an automorphism σ of G such that $\sigma(H) \neq H$. Show that there is a simple group L and a positive integer k such that $G \cong \prod_{i=1}^{k} L$ is isomorphic to the direct product of k copies of L.

QR Exam Algebra
September 9, 2017
Morning Solutions

(1) Let d be the degree of the extension $K/\mathbb{F}_2$. The Galois group is cyclic of order d. Note that there are two irreducible polynomials of degree 1 (X and $X+1$), one irreducible polynomial of degree 2 (X^2+X+1) and for each $d \geq 3$ there is at least 1 irreducible polynomial. The possibilities of the degrees of the factors of f are

(a) $1, 1, 3$;
(b) $2, 3$;
(c) $1, 4$;
(d) 5.

The value of d is the least common multiple of the degrees of the factors, and has to be 3, 6, 4 or 5 respectively.

(2) (a) For fixed $v_2 \in V$ and $w_2 \in W$, the map

$$(v_1, w_1) \mapsto (v_1, v_2)_V (w_1, w_2)_W$$

is bilinear. By the universal property of tensor product, there exists a linear map

$$\psi_{v_2,w_2} : V \otimes W \to \mathbb{R}$$

such that

$$\psi_{v_2,w_2}(v_1 \otimes w_1) = (v_1, v_2)_V (w_1, w_2)_W.$$

The map $V \times W \to \mathrm{Hom}(V \otimes W, \mathbb{R})$ given by $(v_2, w_2) \mapsto \psi_{v_2,w_2}$ is bilinear, so there exists a linear map $\psi' : V \otimes W \to \mathrm{Hom}(V \otimes W, \mathbb{R})$ with

$$\psi'(v_2 \otimes w_2) = \psi'_{v_2,w_2}.$$

Now we define

$$(a_1, a_2)_{V \otimes W} = \psi'(a_1)(a_2).$$

Note that $(a_1, a_2)_{V\otimes W}$ is linear in a_2 because $\psi'(a_1)$ is linear, and it is linear in a_1 because ψ' is linear. To show symmetry, note that

$$\Big(\sum_i v_i \otimes w_i, \sum_j v_j \otimes w_j\Big)_{V\otimes W} = \sum_{i,j} (v_i \otimes w_i, v_j' \otimes w_j')_{V \otimes W} =$$

$$= \sum_{i,j} (v_i, v_j')_V (w_i, w_j')_W = \sum_{i,j} (v_j', v_i)_V (w_j', w_i) = \Big(\sum_j v_j' \otimes w_j', v_i \otimes w_i\Big)_{V \otimes W}.$$

(b) We can choose a basis $v_1, v_2, \ldots, v_n$ of V such that $(v_i, v_j)_V = \delta_{i,j}$ (Kronecker delta function) for all i, j. We can also choose a basis $w_1, \ldots, w_m$ of W such that $(w_i, w_j)_W = \delta_{i,j}$. With respect to the basis $v_i \otimes w_j$ with $1 \leq i \leq n$ and $1 \leq j \leq m$, the bilinear form $(\cdot, \cdot)_{V\otimes W}$ is the usual inner product, so it is positive definite.

(3) (a) Since A has rank at most 2, its Jordan normal form must also have rank at most 2. On the other hand, if J is a matrix in Jordan normal form and J has rank at most 2, then there exists an invertible matrix such that $C\,\mathrm{im}(B) \subseteq \ker(J)$. So

$C^{-1}JCB = 0$. If we take $A = C^{-1}JC$, then $AB = 0$ and J is the Jordan normal form of A. The possible Jordan normal forms of rank ≤ 2 are:

(i)

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\lambda_1, \lambda_2 \in \mathbb{C}$;

(ii)

$$\begin{pmatrix} \lambda_1 & 1 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\lambda_1 \in \mathbb{C}$;

(iii)

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\lambda_1 \in \mathbb{C} \setminus \{0\}$;

(iv)

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

(v)

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

(b) If $AB = BA = 0$ then A must be of the form

$$A = \begin{pmatrix} 0 & 0 & a & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & c & d \end{pmatrix}.$$

The characteristic polynomial is $X^3(X-d)$, so the Jordan normal form can have at most 1 nonzero eigenvalue (counted with multiplicity). Also, if $A^2 = 0$ then me must have $d = 0$ and $bc = 0$ and it follows that A has rank at most 1. In view of part (a), the only possibilities are
The Jordan normal form of A can be

(i)

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\lambda_1 \in \mathbb{C}$ or

(ii)

$$\begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

with $\lambda_1 \in \mathbb{C}$.

(c)

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

case (i) appears when $b = c = 0$ and $a = 1$, case (ii) appears when $a = b = c = 0$ and case (iii) appears when $a = d = 0$ and $b = c = 1$.

(4) (a) Suppose that $M = (m)$. and $(m) = M \supsetneq I \supsetneq M^2 = (m^2)$. Let $I' = \{a \in R \mid am \in I\}$ and $M' = \{a \in R \mid am \in M^2\}$. We have $M \subseteq M' \subseteq I' \subseteq R$ so $I' = M$ or $I' = R$. If $I' = R$ then we have $m \in I$ and $I = M$. If $I' = M$ then for for every $b \in I$ we can write $b = ma$ with $a \in I' = M$, so $b \in M^2$ and we conclude that $I = M^2$.

(b) For example $R = \mathbb{C}[X, Y]$, $M = (X, Y)$, $I = (X^2, Y)$ and $M^2 = (X^2, XY, Y^2)$.

(5) Let H be the subgroup of all elements $g \in G$ with $\sigma(g) = g$. The group $\langle \sigma \rangle$ acts on G and its orbits have 1 or p elements (because the orbit size has to divide the order of $\langle \sigma \rangle$). So $G \setminus H$ is a union of orbits of size p, and $|G \setminus H| = |G| - |H|$ is divisible by p. Since $|G|$ is divisible by p, we conclude that $|H|$ is divisible by p. By Cauchy's theorem, H has an element of order p.

QR Exam Algebra
September 9, 2017
Afternoon Solutions

(1) The minimum polynomial is equal to the characteristic polynomial. The matrix A must be conjugate to

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

and A^2 is conjugate to

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

(a) The characteristic polynomial of A^2 (and B^2) is $X^3(X-1)^2$.
(b) The minumum polynomial of A^2 (and B^2) is $X^2(X-1)$.

(2) (a) For every i V_i/V_{i-1} is a 1-dimensional subspace of $\mathbb{F}_p)^n/V_{i-1} \cong \mathbb{F}_p^{n-i+1}$ and the number of choices for this is $(p^{n-i+1}-1)/(p-1)$. These one dimensional subspaces uniquely determine the chain, so the total number of chains is

$$\frac{p^n-1}{p-1} \cdot \frac{p^{n-1}-1}{p-1} \cdots \frac{p-1}{p-1}.$$

(b) The stabilizer consists of the invertible upper triangular matrices.

(3) (a) Let $L = \mathbb{Q}(\sqrt[6]{3})$. The field extension $L/\mathbb{Q}$ has degree 6 because the minimum polynomial $X^6 - 3$ is irreducible by Eisenstein's criterion. The extension K/L has degree 2 because $i^2 \in L$ and $i \notin L$. So $[K : \mathbb{Q}] = [K : L] \cdot [L : \mathbb{Q}] = 2 \cdot 6 = 12$.
(b) Let $\zeta = (1+\sqrt{3}i)/2$ be the primitive 6-th root of unity and let M be the splitting field of $X^6 - 3$. Then M contains $\sqrt[6]{3}$ and $\zeta\sqrt[6]{3}$ and therefore ζ. Now M also contains $\sqrt{3}$ and $i = (2\zeta - 1)/\sqrt{3}$. So M contains K. On the other hand, K contains ζ and $\sqrt[6]{3}$ and therefore it contains M. We conclude that $K = M$. So $K = M$ is a splitting field and this implies that $K/\mathbb{Q}$ is Galois. The Galois group is the dihedral group D_6 with 12 element. More precisely, the Galois group $K/\mathbb{Q}(\zeta)$ is generated by an automorphism σ of order 6 that sends $\sqrt[6]{3}$ to $\zeta\sqrt[6]{3}$. Let τ be complex conjugation. This is another automorphism of $K/\mathbb{Q}$. Note that $\tau\sigma\tau^{-1} = \sigma^{-1}$. Now τ and σ generate the dihedral group D_6.

(4) Let $R = \mathbb{Z}[X]/(bX - a)$. We distinguish the following cases:
(a) If $a = b = 0$ then $R = \mathbb{Z}[X]$ which is an integral domain.
(b) If $b = 0$ and $a = 1$ then $R = 0$ is not an integral domain. (because in an integral domain $1 \neq 0$).
(c) If $b = 0$ and $a = p$ is prime, then $R = \mathbb{F}_p[X]$ is an integral domain.

(d) If $b = 0$ and a is not prime then R has zero divisors and is not an integral domain.
(e) Suppose that $b > 0$ and $d = \gcd(a, b) \neq 1$. We can write $a = a'd$ and $b = b'd$. In R we have $d(b'X - a') = 0$ and $d, b'X - a' \neq 0$. So R has zero divisors and is not an integral domain.
(f) Suppose that $b > 0$ and $\gcd(a, b) = 1$. Define a ring homomorphism $\varphi : \mathbb{Z}[X] \to \mathbb{Q}$ by $\varphi(f(X)) = f(\frac{a}{b})$. The kernel is generated by $bX - a$. Indeed if $f(X)$ is a polynomial in the kernel, then $f(\frac{a}{b}) = 0$ so we can factor $f(X) = g(X)(bX - a)$ with $g(X) \in \mathbb{Q}[X]$. By Gauß' Lemma, $g(X)$ has integer coefficients and $f(X)$ lies in the ideal $(bX - a)$. By the first isomorphism theorem, $R = \mathbb{Z}[X]/(bX - a)$ is isomorphic to the image of φ, which is an integral domain because it is a subring of the integral domain $\mathbb{Q}$.

(5) Suppose that G is not trivial. Let L be a nontrivial normal subgroup of G. We may assume that L does not have a nontrivial subgroup that is normal in G and properly contained in L. For every automorphism σ of G, $\sigma(L)$ is also a normal subgroup. Suppose that

$$\{\sigma(L) \mid \sigma \text{ is an automorphism of } G\} = \{L_1, L_2, L_3, \ldots, L_d\},$$

where $L_1, L_2, \ldots, L_d$ are distinct normal subgroups of G. By induction on r we show that $L_1 L_2 \cdots L_r$ is isomorphic to L^s for some s. The case $r = 1$ is clear. Suppose that $L_1 L_2 \cdots L_r \cong L^s$. Then $(L_1 L_2 \cdots L_r) \cap L_{r+1}$ is a normal subgroup of L_{r+1} and must be isomorphic to L_{r+1} or $\{1\}$. In the first case, we have $L_1 L_2 \cdots L_{r+1} = L_1 L_2 \cdots L_r \cong L^s$. In the second case, $L_1 L_2 \cdots L_r$ and L_{r+1} are normal subgroups of $L_1 L_2 \cdots L_{r+1}$ with a trivial intersection, so $L_1 L_2 \cdots L_{r+1} = (L_1 L_2 \cdots L_r) \times L_{r+1} \cong L^s \times L = L^{s+1}$. Suppose that N is a normal subgroup of L that is not equal to L. Then $N \times \{0\}^{s-1} \subset L^s$ is a normal subgroup. By minimality of L, we see that N must be trivial. This proves that L is simple.