QR Exam Algebra
May 2, 2018
Morning

Justify your answers.

(1) Classify all finite groups G (up to isomorphism) that have only one automorphism.

Solution. Suppose that the finite group G has only 1 automorphism. For $g \in G$, we have an automorphism $\varphi_g : G \to G$ defined by $\varphi_g(h) = ghg^{-1}$. From the assumption on G follows that φ_g is the identity, and $ghg^{-1} = h$ for all $g, h \in G$. So G is commutative. Let $\psi : G \to G$ be defined by $\psi(g) = g^{-1}$. Since ψ is the identity, we have $g^2 = 1$ for all $g \in G$. This shows that G is isomorphic to the group $(\mathbb{Z}/2\mathbb{Z})^r$. If $r \geq 2$ then we can permute the factors. So $r \leq 1$ and G is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Clearly these two groups have no non-trivial automorphisms.

(2) Suppose that F is a field, $p(x) \in F[x]$ is a separable, irreducible polynomial of degree 3 with roots $\alpha_1, \alpha_2, \alpha_3$.
   (a) Show that if the characteristic of F is not 2 or 3, then $F(\alpha_1, \alpha_2, \alpha_3) = F(\alpha_1 - \alpha_2)$.
   (b) Show that if F has characteristic 3, then it is possible that $F(\alpha_1, \alpha_2, \alpha_3) \neq F(\alpha_1 - \alpha_2)$.

Solution.
(a) Since $p(x)$ is separable, $\alpha_1, \alpha_2, \alpha_3$ are distinct. Let $K = F(\alpha_1, \alpha_2, \alpha_3)$ be the splitting field of $p(x)$. Since K/F is a splitting field of a separable polynomial, it is a Galois extension. Let G be the Galois group. Suppose that σ is a nontrivial automorphism with $\sigma(\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2$. If $\sigma = (1\ 2)$, then we have $\alpha_2 - \alpha_1 = \sigma(\alpha_1 - \alpha_2) = \alpha_1 - \alpha_2$, so $2\alpha_1 = 2\alpha_2$ and $\alpha_1 = \alpha_2$. Contradiction. If $\sigma = (1\ 3)$ then $\alpha_3 - \alpha_2 = \alpha_1 - \alpha_2$. So $\alpha_3 = 2\alpha_1$. If $\sigma = (2\ 3)$ we get a similar contradiction. If $\sigma = (1\ 2\ 3)$ then we have $\alpha_2 - \alpha_3 = \alpha_1 - \alpha_2$. By symmetry (using the transitive action of the Galois group) we must also have $2\alpha_1 = \alpha_2 + \alpha_3$. Taking the sum of the two equations we get $3\alpha_1 = 3\alpha_3$ and $\alpha_1 = \alpha_3$. Contradiction. And the case $\sigma = (1\ 3\ 2)$ is similar. We conclude that σ is the identity. By the Galois correspondence, $F(\alpha_1 - \alpha_2)$ must be the splitting field K.
(b) Note that $x^3 - x - 1$ is irreducible in $\mathbb{F}_3[x]$ because it has no root. Let $\mathbb{F}_{27} = \mathbb{F}_3[x]/(x^3 - x - 1)$ be the field with 27 element, and let $\alpha = x + (x^3 - x - 1) \in \mathbb{F}_{27}$. The Frobenius map ϕ acts by $\phi(\alpha) = \alpha^3 = \alpha + 1$ and $\phi^2(\alpha) = \phi(\alpha + 1) = \alpha + 2$, and $\phi^3(\alpha) = \alpha$. Since $\{\alpha_1, \alpha_2, \alpha_3\} = \{\alpha, \alpha + 1, \alpha + 2\}$ we have that $\alpha_1 - \alpha_2 \in \mathbb{F}_3$, but $\alpha_1 \notin \mathbb{F}_3$. We conclude that $K \neq F(\alpha_1 - \alpha_2)$.

(3) Suppose that A is a 2×2 matrix with real entries that is conjugate to its square A^2. What are the possible rational canonical forms for A?

Solution. Suppose that λ is an eigenvalue and not equal to 0 or 1. Then λ^2 an eigenvalue of A^2 and therefore of A. Now λ^4 is another eigenvalue so $\lambda^4 \in \{\lambda, \lambda^2\}$. If $\lambda^4 = \lambda^2$ then $\lambda = -1$. In that case A has eigenvalues $-1, 1$ and A^2 has eigenvalues $1, 1$ which is not possible. So $\lambda^4 = \lambda$ and $\lambda^3 - 1 = (\lambda - 1)(\lambda^2 + \lambda + 1) = 0$, so $\lambda^2 + \lambda + 1 = 0$. We conclude that $\lambda \in \{0, 1, \zeta, \zeta^2\}$ where $\zeta = e^{2\pi/3}$ is a primitive 3rd root of unity. The possible pairs of eigenvalues are $(0, 0)$, $(1, 0)$, $(1, 1)$, (ζ, ζ^2).

Case $(0, 0)$. If the invariant factors are x^2, then the rational canonical form is

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

and $A^2 = 0$ is not conjugate to A. Contradiction. So the invariant factors are x, x. So $A = 0$ and the rational canonical form is

$$R_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Case $(0, 1)$. The invariant factors are $x(x - 1) = x^2 - x$, the rational canonical form is

$$R_2 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

Case $(1, 1)$. The invariant factors are $(x-1), (x-1)$ or $(x-1)^2 = x^2 - 2x + 1$ and the possible rational canonical forms are

$$R_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad R_4 = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}$$

Case (ζ, ζ^2). In this case, the minimum polynomial must be $(x - \zeta)(x - \zeta^2) = x^2 + x + 1$ and the rational canonical form is

$$R_5 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

For each i we verify that the rational canonical form of R_i^2 is equal to R_i.

(4) Let R be the ring

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$$

and $I = (5)$ be the ideal of R generated by 5. Write $R/(5)$ as a product of fields.

Solution. We have $R \cong \mathbb{Z}[x]/(x^3 - 2)$ and $R/(5) \cong \mathbb{F}_5[x]/(x^3 - 2)$. Now $x^3 - 2$ has a root, namely $3 = -2$, so $x^3 - 2 = (x + 2)(x^2 - 2x - 1)$. We verify that $x^2 - 3x - 1$ does not have a root in in $\mathbb{F}_5$. So we have

$$R/(5) \cong \mathbb{F}_5[x]/(x + 2) \times \mathbb{F}_5[x]/(x^2 - 2x - 1) \cong \mathbb{F}_5 \times \mathbb{F}_{25}.$$

(5) Suppose that p, q, r are distinct prime numbers, and $\Phi_{qr}(x) \in \mathbb{Z}[x]$ is the qr-th cyclotomic polynomial. For which p, q, r is $\Phi_{qr}(x)$ irreducible as a polynomial in $\mathbb{F}_p[x]$ after reducing its coefficients modulo p?

Solution. Let $\phi : K \to K$ be the Frobenius automorphism $\alpha \mapsto \alpha^p$ that generates the Galois group $K/\mathbb{F}_p$. Let d be the order of the congruence class $p + (qr)$ in $\mathbb{Z}/(qr)^\times = \mathbb{Z}/(q)^\times \times \mathbb{Z}/(r)^\times = \mathbb{Z}/(q-1) \times \mathbb{Z}/(r-1)$. The polynomial

$$f(x) = (x - \alpha)(x - \alpha^p) \cdots (x - \alpha^{p^{d-1}})$$

is invariant under ϕ, so it lies in $\mathbb{F}_p[x]$. Also, $f(x)$ is irreducible because the Galois group acts transitively on the roots. So $f(x)$ is the minimum polynomial of α, and must divide $\Phi_{qr}(x)$. Now $\Phi_{qr}(x)$ is irreducible if and only if $f(x) = \Phi_{qr}(x)$ and this is true if and only if $d = (q-1)(r-1)$. If $d = (q-1)(r-1)$ then $\mathbb{Z}/(q-1) \times \mathbb{Z}/(r-1)$ is cyclic, and $q-1$ and $r-1$ are relatively prime. In particular, $q = 2$ or $r = 2$. Suppose $q = 2$. Then $d = (q-1)(r-1) = (r-1)$ if and only if $p + (r)$ generates $\mathbb{Z}/(r)^\times$.

QR Exam Algebra
May 2, 2018
Afternoon

Justify your answers.

(1) Let $K/\mathbb{Q}$ be a field extension, and suppose that $\alpha, \beta \in K$ satisfy $K = \mathbb{Q}(\alpha, \beta)$ and $\alpha^2 = \beta^3$.
   (a) Show that if $\beta \in \mathbb{Q}(\alpha)$ then $[K : \mathbb{Q}] < \infty$.
   (b) If $[K : \mathbb{Q}] = \infty$, show that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}(\alpha^2)$.

   Solution: If $\beta = 0$ then $\alpha = 0$ so $K = \mathbb{Q}$, whence the conclusion of (a) holds and the hypothesis of (b) does not hold. Henceforth assume $\beta \neq 0$, and put $\gamma := \alpha/\beta \in K$. Then $\gamma^2 = \beta$ and $\gamma^3 = \alpha$, so $K = \mathbb{Q}(\gamma)$. Suppose that $[K : \mathbb{Q}] = \infty$, or equivalently that γ is transcendental over $\mathbb{Q}$. For any rational function $f(X) \in \mathbb{Q}[X]$ of degree $n > 0$, write $f(X) = a(X)/b(X)$ where a, b are coprime polynomials in $\mathbb{Q}[X]$ with $\max(\deg a, \deg b) = n$, and put $t := f(\gamma)$, which is transcendental over $\mathbb{Q}$. Then γ is a root of the degree-n polynomial $m(X) := a(X) - t \cdot b(X)$ in $(\mathbb{Q}(t))[X]$. This polynomial is irreducible in $(\mathbb{Q}[t])[X]$ since its t-degree is 1 and $\gcd(a, b) = 1$, so by Gauss's lemma it is irreducible in $(\mathbb{Q}(t))[X]$. Thus $[\mathbb{Q}(\gamma) : \mathbb{Q}(t)] = \deg m = n$. Plainly $L := \mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta)$ contains $\mathbb{Q}(\alpha^2)$, so that $[K : L] \leq [K : \mathbb{Q}(\alpha^2)] = [\mathbb{Q}(\gamma) : \mathbb{Q}(\gamma^6)] = 6$. But $[K : L]$ is divisible by both $[K : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\gamma) : \mathbb{Q}(\gamma^3)] = 3$ and $[K : \mathbb{Q}(\beta) = [\mathbb{Q}(\gamma) : \mathbb{Q}(\gamma^2)] = 2$, and hence by 6, so $[K : L] = 6$ and thus $L = \mathbb{Q}(\alpha^2)$. This proves (b). Moreover, since $[K : L] = 6 \neq 3 = [K : \mathbb{Q}(\alpha)]$, we have $\beta \notin \mathbb{Q}(\alpha)$, yielding the contrapositive of (a).

(2) Let G be a finite subgroup of the group $\mathrm{GL}_n(\mathbb{Q})$ of invertible n-by-n matrices with rational coefficients. Prove that every prime p which divides the order of G must satisfy $p \leq n + 1$.

   Solution. By Cauchy's theorem, G contains an element A of order p. By Cayley–Hamilton, A is killed by its characteristic polynomial $f_A(x)$, which is a degree-n polynomial in $\mathbb{Q}[x]$. Thus the minimal polynomial $m_A(x)$ of A is a nonconstant monic polynomial in $\mathbb{Q}[x]$ which divides $f_A(x)$. But $m_A(x)$ also divides $x^p - 1$, and is not $x - 1$, so it must be either $x^p - 1$ or $(x^p - 1)/(x - 1)$ (since the latter polynomial is irreducible in $\mathbb{Q}[x]$). Therefore $p - 1 \leq \deg m_A \leq \deg f_A = n$.

(3) Let $R := K[X, Y]$ be the polynomial ring in two variables over the field K. Show that the ideal $M := \langle X, Y \rangle$ of R can be written as the union of prime ideals of R which are properly contained in M.

   Solution. Here M consists of all elements of R having zero constant term. For any nonzero $f \in M$, we may write f as the product of irreducible polynomials in R, at least one of which must have zero constant term and hence must be in M. Since R is a

unique factorization domain, the ideal generated by any such irreducible polynomial p is a prime ideal, and this prime ideal contains f and must be properly contained in M since it cannot contain both X and Y because p cannot divide both X and Y. Thus R is the union of the collection of all such prime ideals $\langle p \rangle$.

(4) Let H and J be subgroups of the finite group G such that the indices $[G : H]$ and $[G : J]$ are coprime. Show that every element of G can be written as hj for some $h \in H$ and $j \in J$.

Solution. Since $[G : H \cap J] = [G : H] \cdot [H : H \cap J]$, in particular $[G : H \cap J]$ is divisible by $[G : H]$, and similarly by $[G : J]$, so $[G : H \cap J]$ is divisible by the lcm of $[G : H]$ and $[G : J]$, which is $[G : H] \cdot [G : J]$ since these indices are coprime. The subset $HJ := \{hj \colon h \in H, j \in J\}$ of G has cardinality

$$\frac{\#H \cdot \#J}{\#(H \cap J)} = \frac{\#G \cdot [G : H \cap J]}{[G : H] \cdot [G : J]},$$

which is a multiple of $\#G$ and hence must equal $\#G$, so $HJ = G$.

(5) Show that the tensor product of $\mathbb{Z}$-modules $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

Solution. For any $a, b \in \mathbb{Q}$, we can write $a = m/n$ with $m, n \in \mathbb{Z}$ and $n \neq 0$, so that

$$(a + \mathbb{Z}) \otimes (b + \mathbb{Z}) = n \cdot ((a + \mathbb{Z}) \otimes (b/n + \mathbb{Z})) = ((na) + \mathbb{Z}) \otimes (b/n + \mathbb{Z}) = \\ = (m + \mathbb{Z}) \otimes (b/n + \mathbb{Z}) = (0 + \mathbb{Z}) \otimes (b/n + \mathbb{Z}) = 0.$$

Because the module $(\mathbb{Q}/\mathbb{Z}) \otimes_Z (\mathbb{Q}/\mathbb{Z})$ is generated by such elements, it is equal to 0.