QR PROBLEMS FOR JANUARY 2017

HARM

(1) Suppose that G is a finite group and

$$G_0 = \{e\} \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

is a chain of subgroups such that the set G_i/G_{i-1} has at most 4 elements for $i = 1, 2 \ldots, n$. Prove that G is solvable.

(2) Suppose that q is a prime power, $\mathbb{F}_q$ is the field with q elements and A is an invertible $n \times n$ matrix with entries in $\mathbb{F}_q$. If the minimal polynomial of A is multiplicity free (i.e., it is not divisible by the square of an irreducible polynomial), show that A and A^q are conjugate.

(3) Suppose that $V_1, V_2 \ldots, V_r$ are nonzero subspaces of the $\mathbb{R}$-vector space V such that $V_1 + V_2 + \cdots + V_r = V$. Let $d_1, d_2, \ldots, d_r$ be the dimensions of $V_1, V_2, \ldots, V_r$ respectively. Let W be the subspace of $\bigwedge^r V$ spanned by all $w_1 \wedge w_2 \wedge \cdots \wedge w_r$ with $w_i \in V_i$ for all i. Show that

$$\dim V = d_1 + d_2 + \cdots + d_r$$

if and only if

$$\dim W = d_1 d_2 \cdots d_r.$$

(4) (a) Let $\zeta_{12} = e^{2\pi i/12}$ be a primitive 12-th root of unity. Show that $\zeta_{12}^{11} - \zeta_{12}^{7} = \sqrt{3}$.
(b) Let K be the splitting field of $X^{12} - 3$ over $\mathbb{Q}$. What is the degree of the extension $K/\mathbb{Q}$?
(c) What is the Galois group of $K/\mathbb{Q}$ and how does it act on the roots of $X^{12} - 3$?

(5) Suppose that R is an integral domain in which every ideal is finitely generated (i.e., R is noetherian), and for every $a \in R$ there exists an element $b \in R$ with $b^2 = a$. Show that R is a field.

(6) Let H be the subgroup of the symmetric group S_8 generated by the 3 elements $\sigma_1 = (1\ 2)$, $\sigma_2 = (1\ 3)(2\ 4)$ and $\sigma_3 = (1\ 5)(2\ 6)(3\ 7)(4\ 8)$. Show that H is a 2-Sylow subgroup.

(7) Suppose that V is an $\mathbb{R}$-vector space of dimension 5, and $\langle \cdot, \cdot \rangle$ is a symmetric bilinear form on V. A subspace W of V is called totally isotropic if the restriction of $\langle \cdot, \cdot \rangle$ to W is equal to 0. Suppose that the largest possible dimension of a totally isotropic subspace is 2. What are the possibilities for the signature of $\langle \cdot, \cdot \rangle$?

(8) Suppose that R is a finite commutative ring with identity. Show that there exists a ring isomorphism between R and a product $R_1 \times R_2 \times \cdots \times R_d$ of rings, such that the number of elements in R_i is a prime power for every i.

(9) Assume that L is a Galois extension of the field K with an abelian Galois group G of order $216 = 2^3 3^3$. Suppose that there are exactly 28 subfields M of L such that M is a field extension of K of degree $2^2 3^2 = 36$. Determine G.

(10) Suppose that F is a field, V is an F-vector space and $v_1, v_2, v_3, v_4 \in V$ such that

$$v_1 \otimes v_1 \otimes v_1, v_2 \otimes v_2 \otimes v_2, v_3 \otimes v_3 \otimes v_3, v_4 \otimes v_4 \otimes v_4 \in V \otimes V \otimes V$$

are linearly dependent. Show that $v_j = \lambda v_i$ for some $\lambda \in F$ and some i, j with $i \neq j$.

(1) We prove the statement by induction on n. The case $n = 0$ is clear. The group G_n acts on G_n/G_{n-1}. Let H be the kernel of this action. Then G_n/H is a subgroup of S_4. The group S_4 is solvable, so G_n/H is solvable as well. By the induction hypothesis, G_{n-1} is solvable. So H is solvable because it is contained in G_{n-1}. Since G_n/H and H are solvable, G_n is solvable.

(2) Suppose that the characteristic polynomial $c(X)$ of A is irreducible. Then we have $c(A^q) = c(A)^q = 0$ So the minimal polynomial of A^q divides $c(X)$ and must therefore be $c(X)$. So A and A^q have the same invariant factors, namely just $c(X)$. This shows that A and A^q are conjugate. More generally, if the minimal polynomial of A does not have multiplicities, then the elementary divisors are all irreducible. With respect to some basis, A has a block diagonal form with diagonal blocks $A_1, A_2, \ldots, A_r$ each with an irreducible characteristic polynomial. Now A_i and A_i^q are conjugate for all i, so A and A^q are conjugate.

(3) We have a surjective linear map

$$\varphi : V_1 \oplus V_2 \oplus \cdots \oplus V_r \to V$$

defined by $\varphi(v_1, \ldots, v_r) = v_1 + \cdots + v_r$ and a surjective linear map

$$\psi : V_1 \otimes V_2 \otimes \cdots \otimes V_r \to W$$

with the property $\psi(v_1 \otimes v_2 \otimes \cdots \otimes v_r) = v_1 \wedge v_2 \wedge \cdots \wedge v_r$.

We have to show that φ is injective if and only if ψ is injective.

Suppose φ is not injective. Choose $(v_1, v_2, \ldots, v_r)$ in the kernel. Then $v_1 + v_2 + \cdots + v_r = 0$, After permuting $V_1, \ldots, V_r$ we may assume without loss of generality $v_1, \ldots, v_s$ are nonzero, and $v_{s+1} = \cdots = v_r = 0$. Choose $v_j' \in V_j$ nonzero for $j = s+1, \ldots, r$. We have $v_1 + \cdots + v_s = 0$, so

$$\psi(v_1 \otimes \cdots \otimes v_s \otimes v_{s+1}' \otimes \cdots \otimes v_r') = v_1 \wedge \cdots \wedge v_s \wedge v_{s+1}' \wedge \cdots \wedge v_r' = 0$$

so ψ is not injective.

Suppose that φ is injective (and hence an isomorphism). We can choose a basis $v_{i,1}, v_{i,2}, \ldots, v_{i,d_i}$ of V_i for all i. Then $v_{i,1}, \ldots, v_{i,d_1}, v_{2,1}, \ldots, v_{2,d_2}, \ldots, v_{r,d_r}$ is a basis of V, and

$$\varphi(v_{1,j_1} \otimes v_{2,j_2} \otimes \cdots \otimes v_{r,j_r}) = v_{1,j_1} \wedge v_{2,j_2} \wedge \cdots \wedge v_{r,j_r}$$

is a basis of W if j_k ranges from 1 to d_k for all i. This shows that φ is injective.

(4) (a) Note that $\zeta_{12}^3 = \zeta_4 = i$, $\zeta_{12}^4 = \zeta_3 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ and $\zeta_{12}^8 = \zeta_3^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i$. So we have

$$\zeta_{12}^{11} - \zeta_{12}^7 = \zeta_{12}^8\zeta_{12}^3 - \zeta_{12}^4\zeta_{12}^3 = (-\tfrac{1}{2} - \tfrac{1}{2}\sqrt{3}i)i - (-\tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}i)i = \sqrt{3}.$$

(b) The splitting field is $K = \mathbb{Q}(\sqrt[12]{3}, \zeta_{12})$. Let $M = \mathbb{Q}(\zeta_{12})$. Then we have $\sqrt{3} \in M$, so $\sqrt[12]{3}$ satisfies the equation $X^6 - \sqrt{3} = 0$ over M. This shows that $[K : M] \leq 6$. Also $[M : \mathbb{Q}] = \phi(12) = 4$. It follows that

$$[K : \mathbb{Q}] = [K : M][M : \mathbb{Q}] \leq 6 \cdot 4 = 24.$$

On the other hand, let $L = \mathbb{Q}(\sqrt[12]{3})$. Because of Eisenstein's criterion, $X^{12} - 3$ is irreducible over $\mathbb{Q}$, so $[L : \mathbb{Q}] = 12$. Since ζ_{12} is not real, it does not lie in L, so $[K : L] \geq 2$ and $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] \geq 2 \cdot 12 = 24$. We conclude that $[K : \mathbb{Q}] = 12$.

(c) Let us order the roots as $\sqrt[12]{3}, \zeta_{12}\sqrt[12]{3}, \ldots, , \zeta_{12}^{11}\sqrt[12]{3}$. Then the Galois group is generated by a 12-cycle (1 2 3 $\cdots$ 12) and complex conjugation, which is (2 12)(3 11)(4 10)(5 9)(6 8). So the Galois group is the dihedral group of order 24.

(5) Suppose that $a \in R$ is nonzero. We construct a sequence $a_0, a_1, a_2, \ldots$ by $a_0 = a$, $a_{n+1}^2 = a_n$ for all $n \geq 0$. Let $I = (a_0, a_1, a_2, \ldots)$. Then I is finitely generated and for some k, I is generated by $a_0, a_1, \ldots, a_k$. But then I is generated by a_k. In particular, we have $a_{k+1} = ba_k$ for some $b \in R$ and $a_k = a_{k+1}^2 = b^2 a_k^2$. Since a_k is nonzero, we can cancel and get $1 = b^2 a_k$. This shows that a_k is a unit, and therefore a is a unit because it is a power of a_k. Every nonzero element in R is a unit, so R is a field.

(6) we have $8! = 2^7 \cdot (7 \cdot 3 \cdot 5 \cdot 3)$. So a 2-Sylow subgroup is a subgroup with 2^7 elements. We have $\sigma_1' = \sigma_2\sigma_1\sigma_2 = (3\ 4)$. The group generated by σ_1, σ_1' has order 4 and does not contain σ_2, and σ_2 normalizeds the subgroup of order 4. So the group H_1 generated by σ_1 and σ_2 has $2^3 = 8$ elements. Let $H_2 = \sigma_3 H_1 \sigma_3$. Then $H_1 \times H_2$ is a subgroup of 2^6 elemetns. Now σ_3 does not lie in $H_1 \times H_2$, so $H/(H_1 \times H_2)$ has order 2, and H has order 2^7 elements.

(7) Suppose that the signature is $(a, b, 5-a-b)$. There exists a subspace A of dimension a on which $\langle \cdot, \cdot \rangle$ is positive definite. Suppose that the restriction of $\langle \cdot, \cdot \rangle$ to W is trivial. If $A \cap W$ contains a nonzero vector, then $\langle v, v \rangle = 0$ because $v \in W$ and $\langle v, v \rangle > 0$ because $v \in A$. Contradiction, so $A \cap W = 0$, and $\dim W \leq 5 - a$. Similarly $\dim W \leq 5 - b$ so $2 = \dim W \leq 5 - \max\{a, b\}$. This shows that $\max\{a, b\} \leq 3$. On the other hand, the matrix of $\langle \cdot, \cdot \rangle$ with respect to some basis $v_1, \ldots, v_n$ is

$$\begin{pmatrix} I_a & 0 & 0 \\ 0 & -I_b & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

If $s = \min\{a, b\}$, and U is the span of $v_1 + v_{a+1}, \ldots, v_s + v_{a+s}, v_{a+b+1}, \ldots, v_5$ then the restriction of $\langle \cdot, \cdot \rangle$ to U is trivial, and $2 \geq \dim U = s + 5 - a - b = 5 - \max\{a, b\}$. This shows that $\max\{a, b\} \geq 3$. We conclude that $\max\{a, b\} = 3$.

We have the following possibilities. $(3, 0, 2), (0, 3, 2), (3, 1, 1), (1, 3, 1), (3, 2, 0), (0, 3, 0)$.

(8) Consider the ring homomorphism $\varphi : \mathbb{Z} \to R$ with $\varphi(1) = 1_R$. Then the kernel is a principal ideal (n) where n is a positive integer. We can write $n = p_1^{k_1} \cdots p_r^{k_r}$ where $p_1, \ldots, p_r$ are distinct (positive) primes and $k_1, \ldots, k_r$ are positive integers. Let $\mathfrak{p}_i$ be the ideal in R generated by $p_i^{k_i}$. Then we have $\mathfrak{p}_i + \mathfrak{p}_j = R$ for $i \neq j$. By the Chinese Remainder Theorem, we get:

$$R \cong R/(0) \cong R/(\mathfrak{p}_1 \cdots \mathfrak{p}_r) \cong R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_r.$$

The ring $R_i = R/\mathfrak{p}_i$ is a finite $\mathbb{Z}/(p_i^{k_i})$-module. Moreover, we have a chain

$$0 \subset p_i^{k_i - 1} R_i \subset p_i^{k_i - 2} R_i \subset \cdots \subset p_i R_i \subset R_i$$

such that $p_i^{j-1} R_i / p_i^j R_i$ is an R/p_i-module for all j. It follows that $p_i^{j-1} R_i / p_i^j R_i$ is a finite dimensional $\mathbb{F}_{p_i}$-vector space, hence its cardinality is a power of p_i. We conclude that

$$|R_i| = \prod_{j=1}^{k_i} |p_i^{j-1} R_i / p_i^j R_i|$$

is a power of p_i as well.

(9) Let G be the Galois Group. Then $G = G_2 \times G_3$ where G_2 and G_3 are abelian groups of order $2^3 = 8$ and $3^3 = 27$. There are 3 possiblities for G_2, namely $\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$ and $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. There are 3 possibilities for G_3, namely $\mathbb{Z}/27$, $\mathbb{Z}/9 \times \mathbb{Z}/3$ and $\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$. A field M corresponds to a subgroup H of G of order 6. We can write $H = H_2 \times H_3$ where $H_2 \subset G_2$ has order 2 and $H_3 \times G_3$ has order 3. The number of choices for H_2 are

$\mathbb{Z}/8$	1
$\mathbb{Z}/4 \times \mathbb{Z}/2$	3
$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$	7

The number of choices for H_3 are

$\mathbb{Z}/27$	1
$\mathbb{Z}/9 \times \mathbb{Z}/3$	4
$\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$	13

To count the number of subgroups, note that H_2 and H_3 are cyclic. For example, to count the number of possibilities of $H_3 \subseteq \mathbb{Z}/9 \times \mathbb{Z}/3$, we see that there are 3 elements a in $\mathbb{Z}/9$ with $3a = 0$, and 3 elements b in $\mathbb{Z}/3$ with $3b = 0$. So there are 9 pairs (a, b) with $3(a, b) = 0$. If we exclude the identity, then there are $9 - 1$ choices. But for every subgroup isomorphic to $\mathbb{Z}/3$ there are 2 choices for a generator, so there are $8/2 = 4$ subgroups of $\mathbb{Z}/9 \times \mathbb{Z}/3$ of order 3.

If there are $28 = 7 \cdot 4$ choices for H, then the group must be

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/3 \cong \mathbb{Z}/18 \times \mathbb{Z}/6 \times \mathbb{Z}/2.$$

(10) Suppose that

$$\lambda_1 v_1 \otimes v_1 \otimes v_1 + \lambda_2 v_2 \otimes v_2 \otimes v_2 + \lambda_3 v_3 \otimes v_3 \otimes v_3 + \lambda_4 v_4 \otimes v_4 \otimes v_4 = 0.$$

If v_4 is not a multiple of v_1, v_2, v_3 then there exist $f_1, f_2, f_3 \in V^\star$ with $f_i(v_i) = 0$ and $f_i(v_4) = 1$. If we apply $f_1 \otimes f_2 \otimes f_3$ we get $\lambda_4 = 0$. By symmetry, if f_j is not a multiple of f_i for all $i \neq j$, then $\lambda_j = 0$.