May 2017, Qualifying Review Algebra, Morning

Problem 1. How many isomorphism classes of abelian groups of order 6^4 are there?

Solution. For an integer $n \geq 1$, let $S(n)$ be the set of isomorphism classes of abelian groups of order n^4. First suppose that $n = p$ is prime. By the structure theorem for finite abelian groups, every abelian group of order p^4 is uniquely isomorphic to a product

$$\mathbf{Z}/p^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{e_k}\mathbf{Z}$$

where $e_1 \geq e_2 \geq \cdots \geq e_k \geq 1$ and $e_1 + \cdots + e_k = 4$. Thus $\#S(p)$ is the number of sequences $(e_1, \ldots, e_k)$ that are non-increasing and sum to 4, i.e., the number of partitions of 4. There are exactly five such sequences, so $\#S(p) = 5$ for all p.

Now suppose that p and q are distinct primes. If G is an abelian group of order $(pq)^4$ then by the Chinese Remainder Theorem G canonically decomposes as $G_1 \times G_2$, where G_1 has order p^4 and G_2 has order q^4. We thus see that $S(pq)$ is in bijection with $S(p) \times S(q)$, and therefore has $5 \cdot 5 = 25$ elements. In particular, taking $p = 2$ and $q = 3$, we see that there are 25 isomorphism classes of abelian groups of order 6^4.

Problem 2. Let $\zeta_n = e^{2\pi i/n}$ be a primitive n^{th} root of unity.

(a) For which positive integers n does $\mathbf{Q}(\zeta_n)$ contain $\sqrt{2}$?
(b) For which positive integers n does $\mathbf{Q}(\zeta_n)$ contain $\sqrt[3]{2}$?

Solution. (a) We have $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, and so $\mathbf{Q}(\zeta_8)$ contains $\sqrt{2}$. It follows that $\mathbf{Q}(\zeta_n)$ contains $\sqrt{2}$ whenever $8 \mid n$, since then $\mathbf{Q}(\zeta_8) \subset \mathbf{Q}(\zeta_n)$. Suppose now that $\sqrt{2} \in \mathbf{Q}(\zeta_n)$. Then $\sqrt{2}$ belongs to $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_8) = \mathbf{Q}(\zeta_{\gcd(n,8)})$. Since $\sqrt{2}$ does not belong to $\mathbf{Q}(\zeta_4) = \mathbf{Q}(\sqrt{-1})$, we see that $\gcd(n, 8) = 8$, and so n is divisible by 8. Thus $\mathbf{Q}(\zeta_n)$ contains $\sqrt{2}$ if and only if n is divisible by 8.

(b) Since $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is a Galois extension with abelian Galois group, every subextension is also abelian over $\mathbf{Q}$. Since $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is not abelian, we see that $\sqrt[3]{2}$ is not contained in $\mathbf{Q}(\zeta_n)$ for any n.

Problem 3. Suppose that A and B are complexe, invertible $n \times n$ matrices with $AB + BA = 0$. Show that there exists a complex, invertible $n \times n$ matrix C such that $A + CAC = 0$.

Solution. We made a change to this problem at the last minute, which makes it fairly trivial: one can just take C to be $\sqrt{-1}$ times the identity matrix! The following is the solution we had in mind when making the problem:

Without loss of generality, we may assume that A is in Jordan normal form. Let $J_1, \ldots, J_r$ be the Jordan blocks. Since $-A = BAB^{-1}$ is conjugate to A, we see that $-J_i$ is conjugate to a Jordan block J_k of A. Since A is invertible, none of its eigenvalues are 0, and so J_k is distinct from J_i. We may thus assume that J_{2k+1} is conjugate to $-J_{2k+2}$ for each k. It now suffices to consider the case of two Jordan blocks, since we can just work two blocks at a time. Thus

$$A = \begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix}$$

for some Jordan block J. Putting

$$C = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

we find $A + CAC = 0$, as required.

Problem 4. Let V be the set of 2×2 real matrices, thought of as a 4-dimensional real vector space. For a real number λ, define a symmetric bilinear form $\langle\,,\,\rangle$ on V by

$$\langle A, B \rangle = \lambda \operatorname{Tr}(AB) + \operatorname{Tr}(AB^t)$$

Here Tr is trace and B^t is the transpose of B. For which λ is this form positive definite?

Solution. We choose the basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} e_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

of V. Calculating the matrix $(\langle e_i, e_j \rangle)$ gives

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

The eigenvalues are $1+\lambda, 1+\lambda, 1+\lambda, 1-\lambda$, which are all positive exactly when $-1 < \lambda < 1$.

Problem 5. Let p be a prime number and let n be a positive integer.

(a) Show that there is a positive integer m, depending on p and n, such that if A is an invertible $n \times n$ matrix with entries in $\mathbf{F}_p$ that is diagonalizable over the algebraic closure $\overline{\mathbf{F}}_p$ then $A^m = \mathrm{id}_n$.

(b) Determine the minimal positive m in (a) when $p = 3$ and $n = 4$.

Solution. For (a), one can simply take m to be the order of $\mathrm{GL}_n(\mathbf{F}_p)$: since this is a finite group, any element of it has order dividing the order of the group. For the sake of answering part (b), we will give a more detailed analysis. Suppose that A is as in (a), and let $\lambda_1, \dots, \lambda_n$ be its eigenvalues. Since each λ_i satisfies the characteristic polynomial of A, which is a degree n polynomial with coefficients in $\mathbf{F}_p$, it belongs to an extension of $\mathbf{F}_p$ of degree at most n. Since the multiplicative group $\mathbf{F}_{p^k}^\times$ has order $p^k - 1$, we see that $\lambda_i^{p^k-1} = 1$ for some $1 \le k \le n$. It follows that we can take m to be the lcm of the numbers $p^k - 1$ for $1 \le k \le n$. Note that this is significantly smaller than the order of $\mathrm{GL}_n(\mathbf{F}_p)$.

We claim that this is the minimal positive value for m, for any p and n. To see this, it suffices to show that for each $1 \le k \le n$ there is a matrix A as in (a) such that A has order $p^k - 1$. Thus let k be given. The multiplicative group $\mathbf{F}_{p^k}^\times$ is cyclic. Let λ be a generator. There is an injective ring homomorphism $i \colon \mathbf{F}_{p^k} \to M_k(\mathbf{F}_p)$: given $x \in \mathbf{F}_{p^k}$ multiplication by x defines a linear endomorphism of $\mathbf{F}_{p^k}$, which we think of as a k-dimensional $\mathbf{F}_p$-vector space, and thus (after picking a basis) gives a $k \times k$ matrix with $\mathbf{F}_p$ coefficients. Let B be the matrix $i(\lambda)$. Then B has order $p^k - 1$. Now put

$$A = \begin{pmatrix} B & 0 \\ 0 & \mathrm{id}_{n-k} \end{pmatrix}$$

Then A is an $n \times n$ matrix with coefficients in $\mathbf{F}_p$ and has order $p^k - 1$. This proves the claim.

We thus see that the answer to (b) is the lcm of the numbers $3^k - 1$ for $1 \leq k \leq 4$, i.e., $\operatorname{lcm}(2, 8, 26, 80)$. This is 1040.

May 2017, Qualifying Review Algebra, Afternoon

Problem 1. Let G be a finite group and let p be a prime number. Show that the following conditions are equivalent:

(a) The group G acts transitively on a set X such that the cardinality of X is at least 2 and relatively prime to p.
(b) The order of G is not a power of p.

Solution. Suppose (b) holds. Let P be a p-Sylow subgroup of G and let $X = G/P$. Then G acts transitively on X by left multiplication. The cardinality of X is relatively prime to P (since P is a p-Sylow) and greater than 1 (since $G \neq P$).

Now suppose (a) holds, and let X be given as in (a). Let H be the stabilizer of a point of X. Then G/H is in bijection with X, and so the cardinality of X divides the order of G. This proves (b).

Problem 2. Suppose that R is a commutative ring with 1, and $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of R such that every element of $R \setminus (\mathfrak{p} \cup \mathfrak{q})$ is a unit. Show that at least one of $\mathfrak{p}$ or $\mathfrak{q}$ is maximal.

Solution. If $\mathfrak{q}$ is maximal there is nothing to do, so assume this is not the case. Note that $\mathfrak{p}$ is not contained in $\mathfrak{q}$, as otherwise every element of $R \setminus \mathfrak{q}$ would be a unit, which would imply that $\mathfrak{q}$ is maximal. Let $\mathfrak{m}$ be a proper ideal properly containing $\mathfrak{q}$. Pick $a \in \mathfrak{q} \setminus \mathfrak{p}$ and $b \in \mathfrak{m} \setminus \mathfrak{q}$. Since b is not a unit and does not belong to $\mathfrak{q}$, it must belong to $\mathfrak{p}$. We thus see that $a + b$ does not belong to $\mathfrak{p}$ (as $b \in \mathfrak{p}$ and $a \notin \mathfrak{p}$) and also does not belong to $\mathfrak{q}$ (similar reason), and is therefore a unit. However, both a and b belong to $\mathfrak{m}$, and so $a+b$ belongs to $\mathfrak{m}$, a contradiction.

Problem 3. Suppose that K is a field of characteristic $\neq 2$ and $L = K(\beta)$ is a field extension of K with $\beta^2 + \beta^{-2} \in K$. Show that L/K is a Galois extension.

Solution. We have

$$(X - \beta)(X + \beta)(X - \beta^{-1})(X + \beta^{-1}) = X^4 - (\beta^2 + \beta^{-2})X^2 + 1 \in K[X].$$

Clearly, L is the splitting field of this polynomial, and thus L/K is a normal extension. If $\beta = \pm\beta^{-1}$ then L/K is quadratic, and thus Galois (as the characteristic is not 2); otherwise, the above polynomial has distinct roots, and thus L/K is separable, and thus Galois.

Problem 4. Suppose that V is a real vector space of dimension n.

(a) Show that there exists a linear map $\varphi \colon \bigwedge^2 V \to \mathrm{Hom}(V^*, V)$ such that

$$\varphi(a \wedge b)(f) = f(a)b - f(b)a$$

for all $a, b \in V$.
(b) Suppose n is odd. Show that no element of the image of φ is invertible.

Solution. (a) Consider the map

$$\varphi_0 \colon V \times V \to \mathrm{Hom}(V^*, V), \qquad \varphi_0(a, b)(f) = f(a)b - f(b)a.$$

This function is bilinear and alternating. Thus, by the universal property of exterior powers, φ_0 induces the desired linear map φ.

(b) Let $e_1, \dots, e_n$ be a basis for V and let $e_1^*, \dots, e_n^*$ be the dual basis of V^*. Consider the matrix $A(v)$ for $\varphi(v)\colon V^* \to V$ in this basis, where $v \in \bigwedge^2 V$. We first treat the case $v = a \wedge b$. We have

$$\varphi(a \wedge b)(e_i^*) = e_i^*(a)b - e_i^*(b)a.$$

The (i, j) entry $A(a \wedge b)$ is the coefficient of e_j in the above vector, which is computed by applying e_j^* to it. We thus see that the (i, j) entry is

$$e_i^*(a)e_j^*(b) - e_i^*(b)e_j^*(a).$$

This is anti-symmetric in i and j, and so $A(a \wedge b)$ is a skew-symmetric matrix. Since every element of $\bigwedge^2 V$ is a linear combination of elements of the form $a \wedge b$, we see that $A(v)$ is skew-symmetric for all $v \in \bigwedge^2 V$. Since n is odd, any skew-symmetric $n \times n$ matrix is singular, and so $A(v)$ is singular for all v.

Problem 5. Let $V = \{1, 2, 3, 4, 5, 6, 7, 8\}$. A *matching* on V is a set $\{E_1, E_2, E_3, E_4\}$ where each E_i is a two-element subset of V such that $V = E_1 \cup E_2 \cup E_3 \cup E_4$. Let $\mathcal{M}$ be the set of matchings. The group S_8 naturally acts on $\mathcal{M}$, and the action is transitive. Let $G \subset S_8$ be the stabilizer of some matching. How many orbits does G have on $\mathcal{M}$?

Solution. Let $G \cong S_4 \ltimes S_2^4$ be the stabilizer of $\{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}\}$. Suppose that $\mathcal{F} = \{F_1, F_2, F_3, F_4\}$ is a matching. We draw a graph on 8 vertices, with an edge between a and b whenever $\{a, b\}$ is equal to E_i or F_i for some i. Every vertex had degree 2. The graph is a union of disjoint cycles of even length. Two matchings $\mathcal{F}$ and $\mathcal{F}'$ lie in the same G orbit if and only if the corresponding graphs have the same cycle lengths. So the number of orbits is equal to the number of partitions of 8 into even numbers, which is the number of partitions of 4. There are 5 partitions of 4, so there are 5 orbits.