January 2016, Qualifying Review, Morning Exam

Problem 1. Let p be a prime number and let $1 \leq n < p^2$ be an integer. Show that every p-Sylow subgroup of S_n is abelian.

Solution. Suppose that $n < p^2$. Using division with remainder we can write $n = pq + r$ with $0 \leq r < p$ and $q = \lfloor \frac{n}{p} \rfloor$. The number $n!$ has exactly q prime factors p, so Sylow subgroups of S_n have p^q elements. Let H be the group generated by

$$(1\ 2\ \cdots\ p), (p+1\ p+2\ \cdots\ 2p), \ldots, (p(q-1)+1\ p(q-1)+2\ \cdots\ pq).$$

This is an abelian subgroup of S_n with p^q elements. Therefore, H is a p-Sylow subgroup. Since all p-Sylow subgroups are conjugate, all p-Sylow subgroups are abelian.

Problem 2. Let A be a 5×5 matrix with complex entries. Suppose that the set of all eigenvectors of A, together with the zero vector, forms a two-dimensional subspace of $\mathbf{C}^5$. What are the possible Jordan normal forms of A?

Solution. Let λ be an eigenvalue for A. If there is another eigenvalue μ and v and w are eigenvectors with eigenvalues λ and μ respectively, then $v, w \in S$ but $v + w \notin S$. So S cannot be a subspace. Therefore, λ is the only eigenvalue of A. All the Jordan blocks in the Jordan normal form of A have eigenvalue λ. Now S is the kernel of $A - \lambda I$. Since $A - \lambda I$ has a 2 dimensional kernel, A has exactly 2 Jordan blocks. The possible Jordan normal forms for A are

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 1 & 0 \\ 0 & 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix} \text{ and } \begin{pmatrix} \lambda & 1 & 0 & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 \\ 0 & 0 & \lambda & 0 & 0 \\ 0 & 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & 0 & \lambda \end{pmatrix}$$

where λ is any complex number. For the normal forms above, the space S is clearly a 2-dimensional subspace. So the same is true for any matrix that is conjugate to one of these Jordan normal forms.

Problem 3. Let p be a prime number and let $d \in \mathbf{F}_p$ be a non-square. Show that the set of matrices of the form

$$\begin{pmatrix} a & b \\ db & a \end{pmatrix}$$

with $a, b \in \mathbf{F}_p$ forms a field (under matrix addition and multiplication).

Solution. Let K be the set of such matrices. It is clearly closed under addition. It is easily verified to be closed under multiplication. Since

$$\det \begin{pmatrix} a & b \\ db & a \end{pmatrix} = a^2 - db^2$$

is non-zero if a or b is non-zero (since d is not a square), all the non-zero matrices in K are invertible. Thus K is a domain. It is clear that K has p^2 elements, and is therefore a field (since a finite domain is a field).

Problem 4. Let $R = \mathbf{C}[t^2, t^3]$, considered as a subring of $\mathbf{C}[t]$, and let $I \subset R$ be the ideal (t^2, t^3). Compute the dimension of $I \otimes_R R/I$ as a complex vector space.

Solution. We have $M \otimes_R R/I = M/IM$ for any R-module M, so in particular $I \otimes_R R/I = I/I^2$. We have $I^2 = (t^2, t^3)^2 = (t^4, t^5, t^6)$. Thus I/I^2 has t^2, t^3 as a basis, and is two dimensional.

Problem 5. Suppose that G is a finite group with exactly three conjugacy classes. Show that G is isomorphic to S_3 or $\mathbf{Z}/3\mathbf{Z}$.

Solution. Let $C_1 = \{e\}$, C_2 and C_3 be the conjugacy classes and assume without loss of generality that $|C_2| \leq |C_3|$. The cardinality $|C_i|$ divides $|G|$, say $|G| = d_i|C_i|$. We have

$$|G| = |C_1| + |C_2| + |C_3| = \frac{|G|}{d_1} + \frac{|G|}{d_2} + \frac{|G|}{d_3}$$

and $d_1 \geq d_2 \geq d_3$.

$$\frac{3}{d_3} \geq \frac{1}{d_1} + \frac{1}{d_2} + \frac{1}{d_3} = 1.$$

and $d_3 \leq 3$. It follows that $d_3 = 3$ or $d_3 = 2$. If $d_3 = 3$ then we must have $d_1 = d_2 = 3$. In this case, G has $d_1 = 3$ elements, so G is isomorphic to $\mathbf{Z}/3\mathbf{Z}$.

If $d_3 = 2$, then we must have $d_1 = 6$ and $d_2 = 3$. In this case the group has 6 elements and is not commutative. So G must be isomorphic to S_3.

January 2016, Qualifying Review, Afternoon Exam

Problem 1. Let A be an $n \times n$ complex matrix. Recall that its characteristic polynomial is defined by $\chi_A(t) = \det(tI - A)$, where I is the identity matrix. Prove the identity

$$\chi_{A^2}(t^2) = \chi_A(t)\chi_{-A}(t).$$

Solution. We have

$$\begin{aligned}\chi_{A^2}(t^2) &= \det(t^2 I - A^2) \\ &= \det((tI - A)(tI + A)) \\ &= \det(tI - A)\det(tI - (-A)) \\ &= \chi_A(t)\chi_{-A}(t).\end{aligned}$$

Here I denotes the identity matrix.

Problem 2. Let G be a finite group of cardinality $2^n m$, with m odd, that contains an element of order 2^n. Show that all order 2 elements of G are conjugate.

Solution. The group G contains a cyclic group of order 2^n. Since all 2-Sylow subgroups are conjugate, all 2-Sylow subgroups myst be cyclic of order 2^n. Suppose that a, b are elements of order 2. There exists 2-Sylow subgroups A and B such that $a \in A$ and $b \in B$. There exists an element $g \in G$ such that $gAg^{-1} = B$. Now gag^{-1} is an element of order 2 in B. Because B is cyclic of order 2^n, it has exactly 1 element of order 2, namely b. Therefore $gag^{-1} = b$.

Problem 3. Let V be the vector space of 3×3 real matrices. Define a bilinear form $\langle \cdot, \cdot \rangle$ on V by

$$\langle A, B \rangle = \operatorname{trace}(AB - AB^t).$$

Show that $\langle \cdot, \cdot \rangle$ is symmetric and compute its signature.

Solution. We have

$$\begin{aligned}\langle A, B \rangle &= \operatorname{trace}(AB - AB^t) \\ &= \operatorname{trace}(AB) - \operatorname{trace}(AB^t) \\ &= \operatorname{trace}(BA) - \operatorname{trace}((BA^t)^t) \\ &= \operatorname{trace}(BA) - \operatorname{trace}(BA^t) \\ &= \operatorname{trace}(BA - BA^t) \\ &= \langle B, A \rangle\end{aligned}$$

and so the form is symmetric.

We now compute the signature. We can write $V = W \oplus Z$ where W is the 6-dimensional space of symmetric matrices, and Z is the 3-dimensional space of skew-symmetric matrices. If $B \in W$ then $\langle A, B \rangle = \operatorname{trace}(A(B - B^t)) = 0$. So W lies in the kernel of the bilinear form. So the sign 0 has multiplicity at least 6. If we restrict the bilinear form to Z, we get $\langle A, A \rangle = \operatorname{trace}(A^2 - AA^t) = -2\operatorname{trace}(AA^t) < 0$ for every nonzero $A \in Z$. The sign $-$ has multiplicity 3 and the sign 0 has multiplicity 6.

Problem 4. Let R be a commutative ring with identity such that $IJ = I \cap J$ for all ideals I and J. Show that every prime ideal of R is maximal.

Solution. Let $\mathfrak{p}$ be a prime ideal of R, and put $\overline{R} = R/\mathfrak{p}$. We claim $\overline{I} \cap \overline{J} = \overline{I} \cdot \overline{J}$ for all ideals $\overline{I}$ and $\overline{J}$ of $\overline{R}$. To see this, let $\overline{I}$ and $\overline{J}$ be given, and let I and J be their inverse images in R. Let $\overline{x} \in \overline{I} \cap \overline{J}$, and let x be a lift of $\overline{x}$ to R. Then x belongs to $I \cap J = IJ$, and so $\overline{x}$ belongs to $\overline{I} \cdot \overline{J}$. Thus $\overline{I} \cap \overline{J} \subset \overline{I} \cdot \overline{J}$, and the reverse inclusion is clear.

Let $a \in \overline{R}$ be non-zero. Then $(a^2) = (a)(a) = (a) \cap (a) = (a)$, and so $a = ba^2$ for some b. Since $\overline{R}$ is a domain and a is non-zero, we find $1 = ba$, and so a is a unit. Thus $\overline{R}$ is a field, and so $\mathfrak{p}$ is maximal.

Problem 5. Let $K = \mathbf{Q}(a)$ where a is an algebraic number satisfying $a^2 = 13 + 2\sqrt{13}$. Show that $K/\mathbf{Q}$ is Galois with group $\mathbf{Z}/4\mathbf{Z}$.

Solution. Since $13 + 2\sqrt{13}$ is not a square in $\mathbf{Q}(\sqrt{13})$, we see that $K/\mathbf{Q}$ is a degree 4 extension. The element a is a root of the quartic polynomial $f(x) = (x^2 - 13)^2 - 52$, and so this is its minimal polynomial by degree considerations. Let L be the splitting field of f. The roots of f in L are $\pm a$ and $\pm b$, where $b^2 = 13 - 2\sqrt{13}$.

Let σ be an automorphism of L that restricts to the identity on $\mathbf{Q}(\sqrt{13})$. Then $\sigma(a) = \pm a$ and $\sigma(b) = \pm b$. We have $(ab)^2 = 13^2 - 4 \cdot 13 = 13 \cdot 9$, and so $ab = \pm 3\sqrt{13}$. Thus $\sigma(ab) = ab$, and so either $\sigma(a) = a$ and $\sigma(b) = b$, in which case σ is the identity on L, or $\sigma(a) = -a$ and $\sigma(b) = -b$. We have thus shown that $\mathrm{Gal}(L/\mathbf{Q}(\sqrt{13}))$ has order at most 2. Thus $\mathrm{Gal}(L/\mathbf{Q})$ has order at most 4. But $L/\mathbf{Q}$ is Galois and has degree at least 4. We conclude that $L/\mathbf{Q}$ has degree exactly 4, and thus coincides with K. In particular, K is Galois.

Suppose that $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ is non-trivial on $\mathbf{Q}(\sqrt{13})$. Then $\sigma(ab) = -ab$ by the observations of the previous paragraph. Since σ permutes the roots of f, we see that $\sigma(a)$ must be $\pm a$ or $\pm b$. Since $\sigma(a^2) \neq a^2$, we cannot have $\sigma(a) = \pm a$. Thus $\sigma(a) = \pm b$; suppose (without loss of generality) $\sigma(a) = b$. Then $\sigma(b) = \pm a$, and since $\sigma(ab) = -ab$ we must have $\sigma(b) = -a$. Thus $\sigma^2(a) = \sigma(b) = -a$ and so σ^2 is not the identity. It follows that $\mathrm{Gal}(K/\mathbf{Q})$ has an element of order > 2, and is therefore cyclic of order 4.