2015 Algebra Prelim

September 14, 2015

INSTRUCTIONS: Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in

1. Let $\mathbb{Q}^\times$ be the nonzero elements of $\mathbb{Q}$, a group under multiplication.
(a) Prove that the additive group of $\mathbb{Q}$ has no maximal proper subgroups.
(b) Is the same statement true for the multiplicative group $\mathbb{Q}^\times$?

2. Let V be a finite-dimensional vector space over a field F of characteristic 0. Let $B : V \times V \to F$ be a non-degenerate, skew-symmetric bilinear form. (In particular, we have $B(x, y) = B(y, x)$ for all $x, y \in V$.) If U is a subset of V , let

$$U^\perp = \{v \in V \mid B(u, v) = 0 \text{ for all } u \in U\}.$$

(a) Let U be a subspace of V . Prove that $U^\perp$ is a subspace of V and that

$$\dim_F(U) + \dim_F(U^\perp) = \dim_F(V).$$

(b) Prove that there exists a subspace W of V such that $W^\perp = W$.

3. (a) Suppose that G is a finitely-generated group. Let n be a positive integer. Prove that G has only finitely many subgroups of index n.
(b) Let p be a prime number. If G is any finitely-generated abelian group, let $t_p(G)$ denote the number of subgroups of G of index p. Determine the possible values of $t_p(G)$ as G varies over all finitely-generated abelian groups.

4. Suppose that G is a finite group of order 2013. Prove that G has a normal subgroup N of index 3 and that N is a cyclic group. Furthermore, prove that the center of G has order divisible by 11. (You will need the factorization $2013 = 3 \cdot 11 \cdot 61$.)

Solution:
Note: Dummit and Foote section 5.5 is of some relevance to this problem.

Since $2013 = 3 \cdot 11 \cdot 61$, we know that there exist Sylow subgroups H and K of order 11 and 61 respectively. We claim that K is in fact unique and hence normal. By Sylow's theorem we know that the number of Sylow 61-subgroups is congruent to 1 modulo 61, and the number of such subgroups divides $3 \cdot 11 = 33$. The only possibility is that K is the unique Sylow 61-subgroup and is normal in G. This implies that HK is a subgroup of G with order $11 \cdot 61$, and hence index 3. Since 3 is the smallest prime dividing G any subgroup of index 3 is normal, so HK is normal.

To prove that HK is cyclic, we recognize that its order is the product of two primes and hence it is a semidirect product of the cyclic groups H and K. Such a semidirect product arises from a homomorphism $\phi : H \to \mathrm{Aut}(K)$. Since K has order 61 we have that $\mathrm{Aut}(K) \cong \mathbb{Z}/60\mathbb{Z}$. But $|H| = 11$ does not divide 60, so the only homomorphism ϕ is the zero homomorphism, giving us that $HK \cong H \times K$. Since HK is a direct product of cyclic groups with relatively prime orders it must be cyclic itself.

We next prove the center of G has order divisible by 11. Letting H' be a cyclic subgroup of G with order 3, we recognize that since HK is normal in G we have $G \cong HK \rtimes H'$. To see that the center of G has order divisible by 11, it suffices to show that H (which has order 11) is in the center of G. Note that H is in the center of HK since we have already argued that HK is cyclic. Thus it suffices to show that the elements of H and H' commute. First we prove that H is normal in G. By Sylow's theorem we know that the number of Sylow 11-subgroups is congruent to 1 modulo 11. Moreover this number divides $3 \cdot 61$. But neither 3, 61, nor $3 \cdot 61 = 183$ are congruent to 1 modulo 11, so H is the unique Sylow 11-subgroup of G and hence normal.

Since H is normal in G, H' acts on H by conjugation. This action arises from a homomorphism $H' \to \mathrm{Aut}(H)$. But $\mathrm{Aut}(H)$ has order 10, while H' has order 3. Since 3 does not divide 10, the only such homomorphism is trivial, and H' acts trivially by conjugation on H. In particular all elements of H' commute with elements of H, and so $H \leq Z(G)$. By Lagrange's theorem $Z(G)$ has order divisible by 11.

5. Let V be a finite dimensional vector space over $\mathbb{C}$. Let $n = \dim_{\mathbb{C}}(V)$. Let $T : V \to V$ be a linear map. Suppose that the following statement is true.

For every $c \in \mathbb{C}$, the subspace $\{v \in V \mid T(v) = cv\}$ of V has dimension 0 or 1.

Prove that there exists a vector $w \in V$ such that $\{w, T(w), \dots, T^{n-1}(w)\}$ is a linearly independent set.

Solution:

The condition on T implies that T has n distinct eigenvalues $\lambda_1, \dots, \lambda_n$ with associated eigenvectors $v_1, \dots, v_n$ which form a basis for V. We claim that choosing $w = v_1 + \cdots + v_n$ makes $\{w, T(w), \dots, T^{n-1}(w)\}$ a linearly independent set. Note that

$$T^i(w) = \lambda_1^i v_1 + \cdots + \lambda_n^i v_n$$

and so to argue that $\{w, T(w), \dots, T^{n-1}(w)\}$ is linearly independent it suffices to argue that the matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_n^2 \\ \vdots & & \ddots & \vdots \\ \lambda_1^{n-1} & \lambda_2^{n-1} & \cdots & \lambda_n^{n-1} \end{bmatrix}$$

has linearly independent rows, i.e. that it is invertible. This is a Vandermonde matrix, and its determinant is given by

$$\prod_{1 \leq i < j \leq n} (\lambda_j - \lambda_i).$$

Since $\lambda_j \neq \lambda_i$ when $j \neq i$, we see that this determinant is nonzero and so the matrix is invertible. Hence $\{w, T(w), \dots, T^{n-1}(w)\}$ forms a linearly independent set.

6. This question concerns an extension K of $\mathbb{Q}$ such that $[K : \mathbb{Q}] = 8$. Assume that $K/\mathbb{Q}$ is Galois and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Furthermore, assume that G is nonabelian.

(a) Prove that K has a unique subfield F such that $F/\mathbb{Q}$ is Galois and $[F : \mathbb{Q}] = 4$.

(b) Prove that F has the form $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ where d_1 and d_2 are nonzero integers.

(c) Suppose that G is the quaternionic group. Prove that d_1 and d_2 are positive integers.

Solution:

(a)

Since the extension is Galois we know $|G| = 8$. Since G is nonabelian it is isomorphic to either D_8 or Q_8. Each of these has a unique normal subgroup of order 2 (generated by r^2 and -1 respectively). By the Galois correspondence, these unique subgroups of order 2 (i.e. index 4) correspond to Galois extensions $F/\mathbb{Q}$ which have degree 4.

(b)

The Galois group of $F/\mathbb{Q}$ is G/N where N is the unique normal subgroup of index 4 described in (a). We claim that G/N is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. If $G \cong D_8$, then this is clear since we are taking a quotient which reduces the only elements of G with order greater than 2 to elements of order 2 (these elements are r and r^3). If $G \cong Q_8$ then we again are left with elements only of order 2 since $i^2 = j^2 = k^2 = -1$. Hence $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Since $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ we may choose two subgroups of G/N with index 2 which intersect trivially. Each of yields distinct quadratic extensions of $\mathbb{Q}$, which are necessarily of the form $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ with d_1 and d_2 integers. These extensions intersect trivially and hence their composite field is an extension of order 4, namely F. Thus we have $F = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

(c)

Since K is Galois and finite over $\mathbb{Q}$ it is the splitting field of some polynomial f. Since roots of f come in conjugate pairs, if f has complex roots then complex conjugation is an element of G. Complex conjugation is an automorphism of order 2, and if G is the quaternionic group, then it has a unique element of order 2. Since N (as descbribed in (b)) is the subgroup generated by this element we see that in G/N complex conjugation reduces to the identity. Hence the fixed field of N is totally real, i.e. F is a real extension. This implies that d_1 and d_2 are positive.

7. Let $R = \mathbb{C}[x_1, ..., x_n]$ be the polynomial ring over $\mathbb{C}$ in n indeterminates $x_1, ..., x_n$. Let S_n be the n-th symmetric group. If $\sigma \in S_n$, then we can identify σ with the automorphism of R defined as follows: $\sigma(c) = c$ for all $c \in \mathbb{C}$, and $\sigma(x_i) = x_{\sigma(i)}$ for all i, $1 \leq i \leq n$. Suppose that G is any subgroup of S_n. Let

$$S = R^G = \{r \in R \mid \sigma(r) = r \text{ for all } \sigma \in G\}.$$

Prove that S is a finitely-generated $\mathbb{C}$-algebra.

Solution:

For every $\gamma \subseteq \{1, 2, \ldots, n\}$ define

$$f_\gamma = \sum_{\sigma \in G} \sigma \left(\prod_{i \in \gamma} x_i \right).$$

That is, f_γ is the sum of all elements in the orbit of the monomial $\prod_{i \in \gamma} x_i$ under the action of G on R. We claim that the set of all f_γ generate R^G as an algebra. To see that this is the case, we show that every element of R^G is a polynomial combinator of the various f_γ. We proceed by induction on the degree of $r \in R^G$. In the base case that $\deg(r) = 0$ the result follows trivially since r is constant, and hence in any $\mathbb{C}$-algebra.

Otherwise let $\deg(r) = n > 0$. Then write r as a sum of monomials with coefficients from $\mathbb{C}$ and consider all degree n monomials which appear in this sum. Since $r = \sigma(r)$ for all $\sigma \in G$ we see that

8. This question concerns the polynomial ring $R = \mathbb{Z}[x, y]$ and the ideal $I = (5, x^2 + 2)$ in R.

(a) Prove that I is a prime ideal of R and that R/I is a PID.

(b) Give an explicit example of a maximal ideal of R which contains I. (Give a set of generators for such an ideal.)

(c) Show that there are infinitely many distinct maximal ideals in R which contain I.

Solution:

(a)

Note that

$$R/I = \mathbb{Z}[x, y]/(5, x^2 + 2) \cong (\mathbb{Z}/5\mathbb{Z})[x, y]/(x^2 + 2).$$

The polynomial $x^2 + 2$ is irreducible over $\mathbb{Z}/5\mathbb{Z}$ (having no roots) and so $\mathbb{Z}/5\mathbb{Z}[x]/(x^2 + 2)$ is a field. Let F denote this field and observe that

$$R/I \cong F[y].$$

This is a polynomial ring over a field, and so is a PID. Since R/I is an integral domain we conclude that I must be prime.

(b)

The ideal $J = (5, x^2 + 2, y)$ is maximal since the quotient by this ideal is just $F[y]/(y) \cong F$, a field.

(c)

For any prime $p \in \mathbb{Z}$ not equal to 5 let $J_p = (5, x^2 + 2, py)$. Clearly the various J_p are distinct since the smallest positive integer n for which $ny \in J_p$ is always p and the various p are distinct. Moreover, since $p \neq 5$ for J_p we have p and 5 relatively prime so that p is invertible mod 5. Thus $(py) = (y)$ as ideals in $F[y]$. We then have that $R/J_p \cong F[y]/(yp) = F[y]/(y) \cong F$, so R/J_p is a field and J_p is maximal.