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. (a) Let G be a group (not necessarily finite) that contains a subgroup of index n. Show that G contains a normal subgroup N such that $n \leq [G : N] \leq n!$.

(b) Use part (a) to show that there is no simple group of order 36.

Solution:

(a)

Let $H \leq G$ have index n. Then G acts by left multiplication on the n cosets of H in G, and this induces a homomorphism $\phi : G \to S_n$. Let $N = \ker \phi$ and note N is normal. We also have that $N \leq H$ since if $a \in N$ then a fixes all cosets of H and in particular $aH = H$. Since $aH = H$ we have $ah = 1$ for some $h \in H$ and so $a = h^{-1} \in H$. This proves that $N \leq H$ and we conclude that $[G : N] \geq [G : H] = n$.

Moreover $\phi(G)$ contains no more than $n!$ elements, since $|S_n| = n!$. This fact along with the first isomorphism theorem tells us that $[G : N] = |G/N| = |\phi(G)| \leq n!$. Putting this all together we obtain $n \leq [G : N] \leq n!$ as desired.

(b)

Let G be a group of order 36. Since $36 = 2^2 \cdot 3^2$, Sylow's theorem tells us that G contains a subgroup of order 9 and hence index 4. This gives us a normal subgroup N such that $4 \leq [G : N] \leq 24$. Since the number of cosets of N is strictly between 1 and 36, we see that N is neither trivial nor equal to G. Hence G is not simple, as desired.

2. Let p be a prime, let $\mathbb{F}_p$ be the p-element field, and let $K = \mathbb{F}_p(t)$ be the field of rational functions in t with coefficients in $\mathbb{F}_p$. Consider the polynomial $f(X) = X^p - t \in K[X]$.

(a) Show that f does not have a root in K.

(b) Let E be the splitting field of f over K. Find the factorization of f over E.

(c) Conclude that f is irreducible over K.

Solution:

(a)

A root α of f must satisfy $\alpha^p = t$. We can show that no $\alpha \in K$ satisfies this. Writing

$$\alpha = \frac{\sum_{i=0}^{n} a_i t^i}{\sum_{j=0}^{m} b_j t^j}$$

with $a_i, b_j \in \mathbb{F}_p$ and using the identity $(a+b)^p = a^p + b^p$ (which holds in any field of characteristic p) we have that

$$\alpha^p = \frac{\left(\sum_{i=0}^{n} a_i t^i\right)^p}{\left(\sum_{j=0}^{m} b_j t^j\right)^p} = \frac{\sum_{i=0}^{n} a_i^p t^{ip}}{\sum_{j=0}^{m} b_j^p t^{jp}}.$$

From this we see that if the denominator and numerator of α differ in degree, then the numerator and denominator of α^p can be written so that their degrees differ by at least p, and hence they cannot cancel to be equal to t. If the degrees of the numerator and denominator are equal then the same is true of α^p and hence α^p again cannot be a degree 1 polynomial. Either way we see that $\alpha^p \neq t$ and so $X^p - t$ has no roots.

(b)

This splitting field must contain some element whose p-th power is t, namely a root of $X^p - t$. For convenience let $\sqrt[p]{t}$ denote this element. Then since E has characteristic p, we know $(a+b)^p = a^p + b^p$ for all p. This allows us to factor f as:

$$f(X) = X^p - t = \boxed{(X - \sqrt[p]{t})^p}.$$

In particular we see that $\sqrt[p]{t}$ is the only root of f and has multiplicity p.

(c)

If f were reducible over K then some product of its linear factors would have to lie in $K[X]$. In particular, there would be some integer $k < p$ so that $(X - \sqrt[p]{t})^k \in K[X]$. But applying the binomial theorem we have

$$(X - \sqrt[p]{t})^k = \sum_{i=0}^{k} \binom{k}{i} (-1)^i (\sqrt[p]{t})^i X^{k-i}$$

where we identify the integer $\binom{k}{i}$ as an element of the prime subfield of K via the homomorphism mapping $z \in \mathbb{Z}$ to $1_K + \cdots + 1_K$ (z times). Since the product above is in $K[X]$ by assumption, we have that all coefficients in this expansion are in K. In particular, $\binom{k}{1}(-1)^1(\sqrt[p]{t})^1 \in K$. But this is just $-k\sqrt[p]{t}$, and since $k < p$ we see that $-k \neq 0$ in K. Dividing by $-k$ this then implies that $\sqrt[p]{t}$ is in K, a contradiction since we saw in part (a) that no roots of f could be in K. Thus f is not reducible over K.

(c) *(Alternate irreducibility argument I found online)*
Gauss' criterion tells us that $X^p - t$ is irreducible over K if and only if it is irreducible over the integral domain $R = \mathbb{F}_p[t]$, since K is the field of fractions of R. But in R notice that $\langle t \rangle$ is a prime ideal and so $X^p - t$ satisfies Eisenstein's criterion and so $X^p - t$ is irreducible.

3. Recall that a ring A is called graded if it admits a direct sum decomposition $A = \bigoplus_{n=0}^{\infty} A_n$ as abelian groups, with the property that $A_i A_j \subseteq A_{i+j}$ for all $i, j \geq 0$.

Prove that a graded commutative ring $A = \bigoplus_{n=0}^{\infty} A_n$ is Noetherian if and only if A_0 is Noetherian and A is finitely generated as an algebra over A_0.

Solution:
Some inspiration for the forward direction drawn from: `http://www.jstor.org/stable/2045060`

Before addressing the if and only if statement it is worth justifying that A_0 is a ring, not just an abelian group. For this to be the case it suffices to show A_0 is closed under multiplication. But by the grading property we have $A_0 A_0 \subseteq A_{0+0} = A_0$ and so multiplicative closure is clear. Since A_0 is a subring of A it is indeed sensible to refer to A as an A_0-algebra.

($\Rightarrow$) Suppose that A is a Noetherian ring. Define $I = \bigoplus_{n=1}^{\infty}$ and note I is an additive subgroup of A. Given any $a_i \in A_i$ we have

$$a_i \cdot I = \bigoplus_{n=1}^{\infty} a_i A_n \subseteq \bigoplus_{n=1}^{\infty} A_{n+i} \subseteq I$$

by virtue of the grading on A and so I is invariant under the action of homogeneous elements of A. The set I is also invariant under the action of nonhomogeneous elements since $(a+b)I = aI + bI$ and so the action of any element of A on I can be split up into the action of its homogeneous components. Hence I is an ideal of A. Now notice that $A/I \cong A_0$, and since quotients of Noetherian rings are again Noetherian we conclude that A_0 is Noetherian as a ring.

Now note that each A_i is an A_0-module by virtue of the grading structure, and let π_i be the A_0-module homomorphism which projects A onto A_i. That is, $\pi_i(a)$ is the i-th homogeneous component of $a \in A$. We now argue that each A_i is finitely generated as an A_0-module. Since $A_i A$ is an ideal of A we may choose a finite generating set $\{f_1, \ldots, f_k\}$ for it. Then note that $\pi_i(A_i A) = A_i$ since $A_i A$ contains A_i. Moreover the set $\{\pi_i(f_1), \ldots, \pi_i(f_k)\}$ generates $\pi_i(A_i A)$ as an A_0-module, and hence A_i is a finitely generated A_0-module.

To argue that A is a finitely generated A_0-algebra, let $\{f_1, \ldots, f_r\}$ be a finite generating set for the ideal I (defined earlier) and let N be the maximum index so that $\pi_N(f_j) \neq 0$ for some j. That is, N is the largest index so that some f_j has a nonzero N-th homogeneous component. Then we see that $A_0 \oplus A_1 \oplus \cdots \oplus A_N$ generates A as an algebra since everything in A_i for $i \geq N$ arises by multiplication of lower degree terms in the grading. But each A_i is finitely generated as an A_0-module, and so $A_0 \oplus A_1 \oplus \cdots \oplus A_N$ is finitely generated as an A_0 module. Hence A is finitely generated as an A_0 algebra.

($\Leftarrow$) Suppose that A_0 is Noetherian as a ring and A is finitely generated over A_0 as an algebra by elements $a_1, \ldots, a_k$. Then we have $A \cong A_0[X_1, \ldots, X_k]/I$ for some ideal I of the polynomial ring $A_0[X_1, \ldots, X_k]$ (in particular I is the ideal generated by the relations that the generating elements $X_1, \ldots, X_k$ of A satisfy). Hilbert's basis theorem tells us that $A_0[X_1, \ldots, X_k]$ is a Noetherian ring, and moreover any quotient of it is also Noetherian. Hence A is Noetherian.

4. Let R be a ring with the property that $a^2 = a$ for all $a \in R$.
(a) Compute the Jacobson radical of R.
(b) What is the characteristic of R?
(c) Prove that R is commutative.
(d) Prove that if R is finite, then R is isomorphic (as a ring) to $(\mathbb{Z}/2\mathbb{Z})^d$ for some d.

Solution:
Part (d) uses ideas from `http://www.math.washington.edu/~mitchell/Algh/jac.pdf`.

(a)
We claim that the Jacobson radical is trivial. Recall that if $x \in J(R)$ then $1 + x$ is a unit. We will show this is true only of $x = 0$. To prove this it suffices to show that 1 is the only unit in R. If $a \in R$ is a unit, then we have $aa^{-1} = 1$, but using the identity $a^2 = a$ we obtain

$$1 = aa^{-1} = a^2a^{-1} = a(aa^{-1}) = a(1) = a.$$

Thus $a = 1$ is the only unit in R, and the only element of the Jacobson radical is 0.

(b)
The characteristic is two. Given $a \in R$ we have $a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$. Subtracting $a + a$ from both sides we obtain $0 = a + a$.

(c)
Let $a, b \in R$. Then $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$. Subtracting $a + b$ from both sides we have $0 = ab + ba$ which implies $ab = -ba$. Since R has characteristic two we have $-ab = ab$, and so $ab = ba$ and R is commutative.

(d)
We show that if R is finite and $a^2 = a$ for all $a \in R$, then $R \cong (\mathbb{Z}/2\mathbb{Z})^d$. We proceed by induction on the size of R. If $|R| = 2$ then $R = \mathbb{Z}/2\mathbb{Z}$ is the only nontrivial ring clearly and we are done.

For $|R| > 2$, we first show that every minimal nonzero ideal I is a direct summand of R. From part (a) we have $J(R) = 0$ and so there must be some maximal ideal M that does not contain I, and minimality of I implies $I \cap M = 0$. Since M is maximal we also have $I + M = R$. Hence $R = I \oplus M$ as rings. Then $M \cong R/I$ is a ring of cardinality strictly less than R all of whose elements satisfy the relation $a^2 = a$. Hence $R = I \oplus (\mathbb{Z}/2\mathbb{Z})^d$ by inductive hypothesis. Now, $R/M \cong I$ is a field, but the only field satisfying $a^2 = a$ for all a is $\mathbb{Z}/2\mathbb{Z}$. Hence we have $R \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^d \cong (\mathbb{Z}/2/\mathbb{Z})^{d+1}$ as desired.

5. Let R be a commutative ring and let M be an R-module.

(a) Let $x \in R$ be a nonzero divisor. Compute $\mathrm{Tor}_i^R(R/(x), M)$ for $i \geq 0$.

(b) Show that M is a flat R-module if and only if $\mathrm{Tor}_1^R(M, N) = 0$ for all R-modules N.

(c) Conclude that if R is a PID and M is a finitely generated R-module, then M is flat if and only if M is free.

Solution:

(a)

6. Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Show that the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ has no nontrivial finite subgroups.

7. Let C_p denote the cyclic group of prime order p.

(a) Show that C_p has two irreducible representations over $\mathbb{Q}$ (up to isomorphism), one of dimension 1 and one of dimension $p-1$.

(b) Let G be a finite group, and let $\rho : G \to GL_n(\mathbb{Q})$ be a representation of G over $\mathbb{Q}$. Let $\rho_{\mathbb{C}} : G \to GL_n(\mathbb{C})$ denote ρ followed by the inclusion $GL_n(\mathbb{Q}) \to GL_n(\mathbb{C})$. Thus $\rho_{\mathbb{C}}$ is a representation of G over $\mathbb{C}$, called the complexification of ρ. We say that an irreducible representation ρ of G is absolutely irreducible if its complexification remains irreducible over $\mathbb{C}$.

Now suppose G is abelian and that every representation of G over $\mathbb{Q}$ is absolutely irreducible. Show that $G \cong (C_2)^k$ for some k (i.e., is a product of cyclic groups of order 2).

Solution:

Note: Looked up the second irrep here `http://arxiv.org/pdf/1001.0462.pdf`

(a)

The trivial representation is 1-dimensional and clearly irreducible. To determine the representation of degree $p-1$, consider the field extension $\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity. Recall that $\mathbb{Q}(\zeta_p)$ is $p-1$-dimensional vector space over $\mathbb{Q}$ since the minimal polynomial of ζ_p is $x^{p-1} + x^{p-2} + \cdots + x + 1$. Let $a \in C_p$ be a generator for the group and consider the action of C_p on $\mathbb{Q}(\zeta_p)$ given by $a \cdot v = \zeta_p v$. That is, we define a to act as multiplication by ζ_p and extend to the rest of C_p. This action clearly defines a representation of C_p on $\mathbb{Q}(\zeta_p)$.

We claim that this $p-1$-dimesional representation is irreducible. To prove this we show that it is a simple $\mathbb{Q}C_p$-module. To show it is simple it suffices to generate the $\mathbb{Q}$-basis $\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$ from any nonzero $a \in \mathbb{Q}(\zeta_p)$. Since $\mathbb{Q}(\zeta_p)$ is a field there exists a^{-1} which can be expressed as

$$a^{-1} = q_1 + q_2\zeta_p + q_3\zeta_p^2 + \cdots + q_{n-1}\zeta_p^{p-2}$$

for q_i a rational number. But then the action of $q_1 + q_2 a + q_3 a^2 + \cdots + q_{n-1}a^{p-2} \in \mathbb{Q}C_p$ on a will yield 1. Hence every nonzero submodule of $\mathbb{Q}(\zeta_p)$ contains 1. But then it must also contain $a \cdot 1 = \zeta_p$, $a^2 \cdot 1 = \zeta_p^2$, etc, and hence contains a basis for $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ as a vector space. Since $\mathbb{Q} \subseteq \mathbb{Q}C_p$ this basis generates all of $\mathbb{Q}(\zeta_p)$ as a $\mathbb{Q}C_p$ module, and hence any nonzero submodule is all of $\mathbb{Q}(\zeta_p)$. This proves that $\mathbb{Q}(\zeta_p)$ is simple, and hence the representation we have constructed is irreducible.

To see that it is unique, let V be the trivial representation and W be the $p-1$ dimensional representation we have constructed. Then $V \oplus W$ is a p-dimensional representation. We are working over a field of characteristic zero, and hence the regular representation decomposes as a direct sum of irreducibles and the irreducibles are unique up to isomorphism. The regular representation has dimension p, and so we see that $V \oplus W$ is the regular representation, by virtue of being the only p-dimensional representation we can construct which contains both irreducible representations that we have found. Hence the two irreducible representations we have found are the only irreducible representations.

(b)

Since G is abelian we may write it as a product of cyclic groups. To prove that all of these cyclic groups have order two it suffices to show that every element of G has order two. We know that all irreducible complex representations of G are 1-dimensional, and if all $\mathbb{Q}$ irreducible representations are absolutely irreducible it follows that they must also have dimension one.

Now consider the action of elements of G on a 1-dimensional $\mathbb{Q}$-representation. Since the representation is 1-dimensional elements of G act by scalar multiplication. It is clear that elements

of G must correspond to multiplication by roots of unity, since for any $g \in G$ we have $g^{|G|} = 1$ acting as the identity. But the only roots of unity available in $\mathbb{Q}$ are ± 1. Hence every element of G acts as multiplication by ± 1 in every irreducible representation. The complexifications of these representations are irreducible, and their direct sum yields an isomorphic copy of the group algebra $\mathbb{C}G$. But every element of G has an order two action on this direct sum, by virtue of having an order two action on each component of it. This representation is faithful, and so we conclude that every element of G has order two. Hence $G \cong (C_2)^k$ for some k.

8. Let G be a finite group and $\mathbb{Z}[G]$ the integral group algebra. Let $\mathcal{Z}$ be the center of $\mathbb{Z}[G]$. For each conjugacy class $C \subset G$, let $P_C = \sum_{g \in C} g$.

(a) Show that the elements P_C form a $\mathbb{Z}$-basis for $\mathcal{Z}$. Hence $\mathcal{Z} \cong \mathbb{Z}^d$ as an abelian group, where d is the number of conjugacy classes in G.

(b) Show that if a ring R is isomorphic to $\mathbb{Z}^d$ as an abelian group, then every element in R satisfies a monic integral polynomial. (**Hint**: Let $\{v_1, ..., v_d\}$ be a basis of R and for a fixed non-zero $r \in R$, write $rv_i = \sum_j a_{ij} v_j$. Use the Hamilton-Cayley theorem.)

(c) Let $\pi : G \to GL(V)$ be an irreducible representation of G (over $\mathbb{C}$). Show that $\pi(P_C)$ acts on V as multiplication by the scalar

$$\frac{|C|\chi_\pi(C)}{\dim V},$$

where $\chi_\pi(C)$ is the value of the character χ_π on any element of C.

(d) Conclude that $|C|\chi_\pi(C)/\dim V$ is an algebraic integer.

Solution:

(a)

First note that P_C is in the center since we have $gP_Cg^{-1} = P_C$ for all g, and the various g form a basis for $\mathbb{Z}[G]$ as an algebra. Then suppose that $z = \sum_{g \in G} z_g g$ is in $\mathcal{Z}$, where each z_g is an integer. Then we have that $hzh^{-1} = z$ for all $h \in G$. In particular this means that

$$\sum_{g \in G} z_g hgh^{-1} = \sum_{g \in G} z_g g$$

for all h. Now, the various g are linearly independent over $\mathbb{Z}$, and so we may equate coefficients between the two sums above. This tells us that g and hgh^{-1} have the same coefficients in the sums, and so if g and g' are conjugate we must have $z_g = z_{g'}$. In particular we may write

$$z = \sum_C z_C P_C$$

where the sum above is over all conjugacy classes C. Hence z is in the $\mathbb{Z}$-span of the various P_C and we conclude $\mathcal{Z} = \text{span}_{\mathbb{Z}}\{P_C \mid C \text{ a conjugacy class}\}$. To see that the various P_C form a basis it suffices to notice that conjugacy classes are disjoint and hence the P_C are linearly independent over $\mathbb{Z}$.

(b)

Let $\{v_1, \ldots, v_d\}$ be a basis for R over $\mathbb{Z}$ as a group. Then for any $r \in R$ the action $r \cdot x = rx$ is R-linear, and so we may write $rv_i = \sum_j a_{ij} v_j$ for all i where a_{ij} is an integer. Indeed, the action of R corresponds to a $d \times d$ matrix with entries from $\mathbb{Z}$. By Hamilton-Cayley (isn't it usually written Cayley-Hamilton?) we then have that this matrix satisfies a monic polynomial with coefficients from $\mathbb{Z}$, namely its characteristic polynomial. But this means that r satisfies the same polynomial, since the matrix is simply an alternate notation for expressing r as a $\mathbb{Z}$-linear transformation.

(c)

Since we are working over the algebraically closed field $\mathbb{C}$ and V is irreducible, Schur's Lemma implies that every element of G acts as multiplication by a scalar on V. In particular π maps elements of G to scalar multiples of the identity matrix. Thus we may write $\pi(g) = \lambda_g I$ for all $g \in G$ where $\lambda_g \in \mathbb{C}$. Then notice that

$$\chi_\pi(g) = \text{trace}(\pi(g)) = \text{trace}(\lambda_g I) = \lambda_g \dim V.$$

and for all $g \in G$ we have $\lambda_g = \chi_\pi(g)/\dim V$. Since conjugate elements have matrices with the same trace every $g \in C$ acts as multiplication by the same scalar, which is $\chi_\pi(C)/\dim V$. Then we have that

$$\begin{aligned}\pi(P_C) &= \pi\left(\sum_{g\in C} g\right) \\ &= \sum_{g\in C} \pi(g) \\ &= \sum_{g\in C} \frac{\chi_\pi(C)}{\dim V} I \\ &= \frac{|C|\chi_\pi(C)}{\dim V} I.\end{aligned}$$

Thus $\pi(P_C)$ acts as multiplication by the desired scalar.

(d)
We have that P_C is an element of the center of $\mathbb{Z}[G]$, which we have proven is isomorphic to $\mathbb{Z}^d$. Hence P_C satisfies a monic polynomial with integer coefficients. Considering $\mathbb{Z}[G]$ as a ring of matrices, we see that the matrix associated to P_C (namely $\pi(P_C)$) must satisfy the same polynomial. This is equivalent to stating that eigenvalues of $\pi(P_C)$ are roots of this polynomial. The only eigenvalue of $\pi(P_C)$ is $|C|\chi_\pi(C)/\dim V$, and so the result follows.