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 $GL_2(\mathbb{C})$ be the general linear group of 2×2 complex matrices, let H be the subgroup of $GL_2(\mathbb{C})$ consisting of non-zero multiples of the identity matrix, and let $PGL_2(\mathbb{C})$ be the quotient group $GL_2(\mathbb{C})/H$.

Let $A, B \in PGL_2(\mathbb{C})$, and assume that both elements have order n. Prove that there exist $C \in PGL_2(\mathbb{C})$ and a positive integer m such that

$$CBC^{-1} = A^m.$$

2. In this problem, as you apply Sylows Theorem, state precisely which portions you are using.

(a) Prove that there is no simple group of order 30.

(b) Suppose that G is a simple group of order 60. Determine the number of p-Sylow subgroups of G for each prime p dividing 60, then prove that G is isomorphic to the alternating group A_5.

Note: In the second part, you neednt show that A_5 is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to A_5.

3. Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

Solution:
We know that if ζ_n is a primitive n-th root of unity then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has Galois group isomorphic to the group of units in $\mathbb{Z}/n\mathbb{Z}$, with the isomorphism arising by mapping the automorphism $\zeta_n \mapsto \zeta_n^k$ to $k \in (\mathbb{Z}/n\mathbb{Z})^\times$.

In our case we have $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$. Since $5^2 = 7^2 = 11^2 = 1$, we see that this group is isomorphic to the Klein four-group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. The group can be described explicitly as $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_7, \sigma_{11}\}$ where σ_i sends $\zeta_{12} \mapsto \zeta_{12}^i$.

To determine intermediate fields we examine the fixed fields of subgroups of the Galois group. There are three subgroups, all of order two and index two, generated by the three nonidentity elements in the Galois group. To describe the fixed field associated to each we need only find a non-rational element of the fixed field since an extension of degree two is generated by any element not in the base field. We do this for each subgroup below. By the Galois correspondence this is a complete list of intermediate subfields.

- The fixed field of the subgroup generated by σ_5 is the extension $\mathbb{Q}(\zeta_{12}^3)$. Note that ζ_{12}^3 is a primitive fourth root of unity, and hence this extension has degree two. Moreover it is fixed by σ_5 since $\sigma_5(\zeta_{12}^3) = \zeta_{12}^{15} = \zeta_{12}^3$. One can also write this extension as $\mathbb{Q}(i)$.

- The fixed field of the subgroup generated by σ_7 is the extension $\mathbb{Q}(\zeta_{12}^2)$. Note that ζ_{12}^2 is a primitive sixth root of unity and hence irrational. Moreover this field is fixed by σ_7 since $\sigma_7(\zeta_{12}^2) = \zeta_{12}^{14} = \zeta_{12}^2$.

- The fixed field of the subgroup generated by σ_{11} is the extension $\mathbb{Q}(\zeta_{12}^5 + \zeta_{12}^7)$. First note that $\zeta_{12}^5 + \zeta_{12}^7$ is not rational since it is not fixed by σ_5. Indeed, we have

$$\sigma_5(\zeta_{12}^5 + \zeta_{12}^7) = \zeta_{12}^{25} + \zeta_{12}^{35} = \zeta_{12} + \zeta_{12}^{11}$$

  which is not equal to $\zeta_{12}^5 + \zeta_{12}^7$. However, this extension is fixed by σ_{11} since

$$\sigma_{11}(\zeta_{12}^5 + \zeta_{12}^7) = \zeta_{12}^{55} + \zeta_{12}^{77} = \zeta_{12}^7 + \zeta_{12}^5.$$

  Hence the extension $\mathbb{Q}(\zeta_{12}^5 + \zeta_{12}^7)$ is the fixed field of σ_{11}.

4. Let

$$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

(a) Answer the following questions with suitable justification.

i. Is R a Noetherian ring?

ii. Is R an Artinian ring?

(b) Prove that R is an integerally closed domain.

Solution:

(a)

R is Noetherian since $\mathbb{Z}[x]$ is Noetherian (by Hilbert's Basis Theorem) and quotients of Noetherian rings are again Noetherian. R is not Artinian, as evidenced by the chain of ideals $\langle 2\rangle \supset \langle 2^2\rangle \supset \langle 2^3\rangle \supset \cdots$.

(b)

We show directly that every element of R satisfies a monic polynomial with coefficients in $\mathbb{Z}$. First note that every element of R can be represented uniquely by a linear polynomial over $\mathbb{Z}$ by repeatedly applying the relation $x^2 = -x - 1$. Given such a representative $ax + b$, we see that is satisfies the monic integral polynomial $f(z) = (z - b)^2 + az - ab + a^2$. Indeed,

$$\begin{aligned} f(ax+b) &= (ax + b - b)^2 + a(ax + b) - ab + a^2 \\ &= a^2x^2 + a^2x + ab - ab + a^2 \\ &= a^2(x^2 + x + 1) \\ &= a^2 0 \\ &= 0. \end{aligned}$$

5. Let R be a commutative ring. Recall that an element r of R is nilpotent if $r^n = 0$ for some positive integer n and that the nilradical of R is the set $N(R)$ of nilpotent elements.

(a) Prove that

$$N(R) = \bigcap_{P \text{ prime}} P.$$

(Hint: Given a non-nilpotent element r of R, you may wish to construct a prime ideal that does not contain r or its powers.)

(b) Given a positive integer m, determine the nilradical of $\mathbb{Z}/(m)$.

(c) Determine the nilradical of $\mathbb{C}[x, y]/(y^2 - x^3)$.

(d) Let $p(x, y)$ be a polynomial in $\mathbb{C}[x, y]$ such that for any complex number a, $p(a, a^{3/2}) = 0$. Prove that $p(x, y)$ is divisible by $y^2 - x^3$.

Solution:

(a)

First suppose that $r \in N(R)$ and let n be a positive integer so that $r^n = 0$, and let P be a prime ideal. We may write $0 = r^n = r^{n-1}r \in P$. Since P is prime we conclude that r^{n-1} or r is in P. If r^{n-1} is in P we repeat this process inductively until we obtain $r^2 \in P$, which implies $r \in P$. In either case we have $r \in P$ and so $N(R)$ is contained in the intersection of all prime ideals.

For the reverse inclusion, we prove that if r is not nilpotent then there exists a prime ideal that does not contain it. If r is a unit then this is clear, since we may take any maximal ideal of R. If r is not a unit, then it is contaned in some maximal ideal M. Then notice that $1 - r$ Consider $1 - r$ in R. This

6. Given a finite group G, recall that its regular representation is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of G on itself and its adjoint representation is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of G on itself.

(a) Let $G = GL_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of G. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.

(b) Let H be a group of order 12. Show that its adjoint representation is reducible; that is, there is an H-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

Solution:

(a)

We claim that G is isomorphic to S_3. First note that a matrix is in G if and only if its rows are linearly independent. The number of ways to create such a matrix is exactly six: the first row must be nonzero, for which there are three choices, and the second row must be nonzero and not equal to the first, leaving us two choices. Hence $|G| = 6$. Moreover, G is not abelian since we have on the one hand

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

while on the other we have

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

The only nonabelian group of order 6 is S_3, so we have $G \cong S_3$.

Since G is not abelian, it must have an irreducible representation of dimension two or greater. Moreover, the sum of the squares of dimensions of irreducible representations is $|G| = 6$. We see quickly that the only possibility satisfying both these requirements is that G has three irreps, two of dimension 1 and one of dimension 2. We describe these irreps below.

- There is the trivial representation V_0 of dimension one, on which G acts as identity.
- There is the alternating representation V_1 of dimension one, on which the even permutations in G act as multiplication by -1 and odd permutations act as identity.
- There is an irrep V_2 of dimension two, on which the action of G is necessarily nonabelian. If we can describe any nonabelian action of G on a two dimensional vector space we will necessarily have described V_2 since there is only one irrep of dimension two, and a nonabelian representation of dimension two cannot be decomposed as the sum of two 1-dimensional representations. To describe the action of G on V_2, recall that we may present S_3 as $\langle a, b \mid a^2 = b^3 = 1 \text{ and } aba = b^{-1}\rangle$. Fix a basis $\{v_1, v_2\}$ for V_2 and let a act by fixing v_1 and negating v_2. Let b act as $v_1 \mapsto \zeta_3 v_1$ and $v_2 \mapsto \zeta_3^2 v_2$ where $\zeta_3 \in \mathbb{C}$ is a primitive third root of unity. One can quickly verify that this action satisfies the relation $a^2 = b^3 = 1$ in G, and with a little more computation we see that it also satisfies $aba = b^{-1}$ since

$$aba \cdot v_1 = ab \cdot v_2 = a \cdot \zeta_3^2 v_2 = \zeta_3^2 v_1 = b^{-1} \cdot v_1$$

and

$$aba \cdot v_2 = ab \cdot v_1 = a \cdot \zeta_3 v_1 = \zeta_3 v_2 = b^{-1} \cdot v_2.$$

We see also that $ab \cdot v_1 = \zeta_3 v_2$ while $ba \cdot v_1 = \zeta_3^2 v_2$ so that the action of G is nonabelian. Hence the described action of G on V_2 yields the unique irreducible representation of G of dimension two.

The regular representation of G decomposes as a sum of all irreps with each appearing as many times as its dimension. Thus we have that the regular representation is isomorphic to $V_0 \oplus V_1 \oplus V_2 \oplus V_2$.

(b)
Recall that $\mathbb{C}[H]$ is a vector space with basis given by the elements of H. Let v_e be the vector associated to the identity element in H, and consider the subspace of $\mathbb{C}[H]$ spanned by v_e. Note that this is a nonzero subspace and that since H has order larger than two it is a proper subspace of $\mathbb{C}[H]$. We see also that it is H-invariant, since

$$h \cdot v_e = v_{heh^{-1}} = v_{hh^{-1}} = v_e$$

for all $h \in H$. Thus the adjoint representation is reducible.

7. Let M, N be finitely generated modules over $\mathbb{Z}$. Recall that $\mathrm{Ann}(M)$ is the ideal in $\mathbb{Z}$ defined as follows:

$$\mathrm{Ann}(M) = \{a \in \mathbb{Z} \mid am = 0 \text{ for any } m \in M\}$$

Prove that $M \otimes_{\mathbb{Z}} N = 0$ if and only if $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$.

Solution:

($\Leftarrow$) Since $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$ we have $1 = a + b$ where a annihilates M and b annihilates N. Then for any simple tensor $m \otimes n$ in $M \otimes_{\mathbb{Z}} N$ we see that

$$\begin{aligned} m \otimes n &= 1(m \otimes n) \\ &= (a+b)(m \otimes n) \\ &= am \otimes n + m \otimes bn \\ &= 0 \otimes n + m \otimes 0 \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

Since all simple tensors are zero we conclude that $M \otimes_{\mathbb{Z}} N = 0$.

($\Rightarrow$) For $n \in \mathbb{Z}$ let $\mathbb{Z}_n$ denote the $\mathbb{Z}/n\mathbb{Z}$. For this implication we use the fact that $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_{(m,n)}$ where (m, n) denotes the greatest common divisor of m and n. One can prove this by considering the homomorphism $\phi : \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \to \mathbb{Z}_{(m,n)}$ mapping $m \otimes n \mapsto mn$ and proving that it is an isomorphism. Importantly, one notes that this is valid even when m or n is zero, and that $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$ is zero if and only if m and n are relatively prime.

Since M and N are finitely generated we may write $M = \bigoplus \mathbb{Z}_{m_i}$ and $N = \bigoplus \mathbb{Z}_{n_j}$ where both direct sums are finite and all m_i and n_j are nonnegative integers. Then, using the fact that tensor products distribute over direct sums, we obtain that

$$\begin{aligned} M \otimes_{\mathbb{Z}} N &= \left(\bigoplus \mathbb{Z}_{m_i}\right) \otimes \left(\bigoplus \mathbb{Z}_{n_j}\right) \\ &\cong \bigoplus \mathbb{Z}_{m_i} \otimes \mathbb{Z}_{n_j} \\ &\cong \bigoplus \mathbb{Z}_{(m_i, n_j)} \end{aligned}$$

where the sums in the final two lines run over all pairs (i, j). We see immediately that $M \otimes_{\mathbb{Z}} N$ is zero only if $(n_i, m_j) = 1$ for all i, j. To see that $\mathrm{Ann}(M)$ and $\mathrm{Ann}(N)$ are comaximal it suffices to find $a \in \mathrm{Ann}(M)$ and $b \in \mathrm{Ann}(N)$ so that a and b are relatively prime. We claim that choosing a to be the product of all m_i and b to be the product of all n_j suffices. Indeed, a and b are relatively prime since all m_i and n_j are pairwise relatively prime. Moreover a annihilates M since it annhilates all $\mathbb{Z}_{m_i}$. Similarly, b annihilates each $\mathbb{Z}_{n_j}$ and hence all of N. We conclude that $\mathrm{Ann}(M)$ and $\mathrm{Ann}(N)$ are comaximal, i.e. $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$.

8. Let R be a commutative integral domain. Show that the following are equivalent: (a) R is a field; (b) R is a semi-simple ring; (c) Any R-module is projective.

Solution:
$(a) \Rightarrow (b)$ The submodules of R are exactly its ideals. If it is a field the only ideals are 0 and R, so that R is a simple (and hence semi-simple) right.

$(b) \Rightarrow (a)$ We claim that R is in fact simple, and hence a field. Suppose not, so that we may write $R = S \oplus \overline{S}$ for proper nonzero subrings S and $\overline{S}$. Then let $s \in S$ and $\overline{s} \in \overline{S}$ be nonzero and observe that $(s, 0) \times (0, \overline{s}) = (0, 0) = 0_R$ so that $(s, 0)$ and $(0, \overline{s})$ are zero divisors in R. This is a contradiction to the fact that R is an integral domain. Hence R is a simple commutative ring, i.e. a field.

$(a) \Rightarrow (c)$ Every module over a field is free. Free modules are projective and so property (c) follows. More directly, let P and M be R-modules and let $\phi : M \to P$ be a surjective R-module homomorphism. Since R is a field we may think of ϕ as an R-linear transformation of vector spaces. Let $\mathcal{B}$ be a basis for P and for every $v \in \mathcal{B}$ let $\hat{v}$ be an element of M such that $\phi(\hat{v}) = v$. Note that the map $v \mapsto \hat{v}$ extends to a linear map $\psi : P \to M$. We also clearly have $\psi \circ \phi = \mathrm{Id}_P$, which implies that P is a projective R-module by definition.

$(c) \Rightarrow (a)$ Let I be an ideal of R and consider the short exact sequence $0 \to I \to R \to R/I \to 0$. Since R/I is projective this sequence splits and we obtain $R \cong R/I \oplus I$ as R-modules and also as rings. But if both R/I and I are nonzero, we obtain a zero divisor in R in the same manner as the proof of $(b) \Rightarrow (a)$. Hence either R/I or I is zero, i.e. $I = 0$ or $I = R$. Hence R has no nonzero proper ideals, and is a field.