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. Classify all groups of order 2012 up to isomorphism. (Hint: 503 is prime.)

Solution:
Let G be a group of order 2012. We have the prime factorization $2012 = 2^2 \cdot 503$, and from Sylow's theorem we obtain a subgroup H of order 503. The number of Sylow 503-subgroups is congruent to 1 modulo 503, and also divides $2^2 = 4$. This immediately implies that H is the unique Sylow 503-subgroup, and is hence normal. We also have a subgroup K of order 4, and since H is normal we see that $G \cong H \rtimes K$. Thus the structure of G is determined by the possible semidirect products between a group of order 4 and a group of order 503.

Since 503 is prime we know H is cyclic, and since K has order 4 it is either cyclic or the Klein 4 group. Semidirect products $H \rtimes K$ will arise from a homomorphism $\phi : K \to \mathrm{Aut}(H)$, and since H is cyclic with prime order we know $\mathrm{Aut}(H)$ is cyclic of order 502. We describe the possible homomorphisms ϕ in the cases that K is cyclic or the Klein 4 group below.

- If K is cyclic and ϕ is trivial we obtain a direct product and $G \cong \mathbb{Z}_{503} \times \mathbb{Z}_4$.
- If K is cyclic and ϕ is nontrivial we note that 502 is divisible by 2 but not 4, and so there is only one possibility for ϕ, namely that it maps the elements of order 4 in K to the identity and the element of order 2 to the element of $\mathrm{Aut}(H)$ with order 2. This gives us a presentation of G as $\langle a, b \mid a^4 = b^{503} = 1 \text{ and } a^2ba^2 = b^{-1}\rangle$.
- if K is the Klein 4 group ($\mathbb{Z}_2 \times \mathbb{Z}_2$) and ϕ is trivial we obtain a direct product and $G \cong \mathbb{Z}_{503} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
- If K is the Klein 4 group and ϕ is nontrivial, we again have a single possibility, up to isomorphism. This arises from mapping one of the generators of K to the element of $\mathrm{Aut}(H)$ with order 2, and the other to the identity. This gives us a presentation $G \cong \langle a, b, c \mid a^2 = b^2 = c^{503} = 1 \text{ and } ab = ba \text{ and } aca = c^{-1} \text{ and } bcb = c\rangle$.

2. For any positive integer n, let G_n be the group generated by a and b subject to the following three relations:

$$a^2 = 1, \quad b^2 = 1, \quad \text{and} \quad (ab)^n = 1.$$

(a) Find the order of the group G_n.

(b) Classify all irreducible complex representations of G_4 up to isomorphism.

Solution:

(a)

We claim that the order is $2n$. One way to see this is to recognize that G_n is in fact the dihedral group with $a = s$ and $b = sr$, but we take a slightly more direct approach. First we argue that every element of G_n can be presented as either $(ab)^k$ or $a(ab)^k$ by reducing modulo the relation $a^2 = b^2 = 1$. Moreover we have $k \leq n$ by the relation $(ab)^n = 1$. This clearly gives us $2n$ possible words of the letters a and b which are in G.

Our next task is to prove that these $2n$ words are all distinct. Note that if $(ab)^k = (ab)^{k'}$ then we have $(ab)^{k-k'} = 1$ and so $k - k' = 0$ if we assume k and k' are both between 0 and $n-1$. This tells us that words of the form $(ab)^k$ are all distinct from one another. Likewise, words of the form $a(ab)^k$ are all distinct, cancelling a from both sides of the same equality. The only other possibility is that $a(ab)^k = (ab)^{k'}$ for some k and k' between 0 and $n-1$. By cancelling appropriately we obtain an expression of the form $b(ab)^m = 1$ for a nonnegative integer m. But we can multiply both sides of this expression on the left and right by b to obtain $a(ba)^{m-1} = b^2 = 1$. We can then multiply by a on the left and right, yielding $b(ab)^{m-2} = 1$ and so on. Repeating this process eventually yields $a = 1$ or $b = 1$, in either case a contradiction. We conclude that the $2m$ words of the form $a(ab)^k$ with $0 \leq k \leq n-1$ are distinct, and G_n contains $2n$ elements.

(b)

First, we know that G_4 has 8 elements by part (a). Second, we know it has at least one 1-dimensional representation, the trivial representation. We also see that G_4 is nonabelian by considering the elements a and ab. We have

$$(ab)a = (ab)a(ab)^4 = (ab)b(ab)^3 = a(ab)^3 \neq a(ab)$$

since by part (a) the representation of elements of G_4 of the form $a(ab)^k$ are unique. Hence not all irreducible representations of G_4 will be 1-dimensional. The sum of squares of dimensions of irreducible representations of G_4 will be equal to 8, and so there will be exactly one 2-dimensional irrep and none of higher dimension. We conclude that there are five irreps of G_4, four with dimension 1 and one with dimension 2. We classify these below.

The 1-dimensional representations of G_4 are homomorphisms $G_4 \to \mathbb{C}^\times$. We see that a and b must map to either ± 1 since they have order 2, and there are clearly four possibilities for mapping a and b to ± 1. Each of these possibilities yields a distinct 1-dimensional representation of G_4 and since we have already concluded there are four total 1-dimensional representations this accounts for everything.

Next we consider the 2-dimensional irrep V of G_4. Let $\{v_1, v_2\}$ be a basis for V. If we can find an action of a and b on V which is not commutative we will be done, since such an action cannot be decomposed as a direct sum of 1-dimensional representations. Let a act by switching v_1 and v_2, and let b act by fixing v_1 while mapping $v_2 \mapsto -v_2$. Note that a^2 and b^2 both act as identity, satisfying the relations $a^2 = b^2 = 1$ in G_4. The element ab acts by mapping $v_1 \mapsto v_2$ and $v_2 \mapsto -v_1$. One can verify that this action has order exactly 4 and so satisfies the relation $(ab)^4$. This proves that the described action of a and b on V is a valid representation of G_4. Note that $a(ab) = b$ does not fix v_2, but $(ab)a$ does, and so this action of G_4 is not commutative. We conclude that this representation is irreducible.

The following list summarizes all irreps of G_4:

- The trivial representation, in which a, b act as identity on $\mathbb{C}$.
- The representation in which a acts by negation on $\mathbb{C}$ and b acts as identity.
- The representation in which a acts as identity on $\mathbb{C}$ while b acts by negation.
- The representation in which a and b both act by negation on $\mathbb{C}$.
- The representation $V = \mathbb{C}^2$ with basis $\{v_1, v_2\}$ in which a switches v_1 and v_2, while b fixes v_1 and negates v_2. Intuitively, this corresponds to the geometric action of the dihedral group of order 8 (i.e. G_4) on a square embedded in the plane.

3. Let R be a (commutative) principal ideal domain, let M and N be finitely generated free R-modules, and let $\phi : M \to N$ be an R-module homomorphism.

(a) Let K be the kernel of ϕ. Prove that K is a direct summand of M.

(b) Let C be the image of ϕ. Show by example (specifying R, M, N and ϕ) that C need not be a direct summand of N.

Solution:

(a)

Note that $\phi(M)$ is a submodule of a free module over a PID, and hence free. In particular, $\phi(M)$ is projective and so the short exact sequence $0 \to \ker\phi \to M \to \phi(M) \to 0$ splits and we have $M \cong \ker\phi \oplus \phi(M)$ and $\ker\phi$ is a direct summand of M.

(a) *(A more direct proof)*

Note that $\phi(M)$ is a free module by virtue of being a finitely generated torsion free module over a PID. Let $\{e_1, \ldots, e_n\}$ be a basis for $\phi(M)$ over R and for $1 \le i \le n$ let e_i' be an element of M so that $\phi(e_i') = e_i$. Letting M' be the submodule of M generated by $\{e_1', \ldots, e_n'\}$ we claim that $M = \ker\phi \oplus M'$. Note immediately that $\ker\phi$ and M' intersect trivially since no e_i' is in the kernel of ϕ.

To see that $M = \ker\phi \oplus M'$ it then suffices to show that every element of M can be written as $k + m'$ for $k \in \ker\phi$ and $m' \in M'$. By the universal property of free modules the map $e_i \mapsto e_i'$ can be extended to an R-module homomorphism $\psi : \phi(M) \to M$. For any $m \in M$ write $m = (m - \psi(\phi(m)) + \psi(\phi(m))$. Note that $\phi \circ \psi$ is the identity on $\phi(M)$, and so we have

$$\phi(m - \psi(\phi(m))) = \phi(m) - \phi(m) = 0$$

i.e. $(m - \psi(\phi(m))$ is in the kernel of ϕ. We also have $\psi(\phi(m)) \in M'$, and so we have written m in the form $k + m'$ as desired. This proves that $M = \ker\phi \oplus M'$ and $\ker\phi$ is a direct summand of M as desired.

(b)

Let $R = M = N = \mathbb{Z}$, and consider the map $x \mapsto 2x$. Then we have that $C = 2\mathbb{Z}$. But $2\mathbb{Z}$ is a proper submodule of $\mathbb{Z}$ and it also intersects every nonzero submodule of $\mathbb{Z}$ nontrivially. Hence it is not a direct summand.

4. Let G be an abelian group. Prove that the group ring $\mathbb{Z}[G]$ is noetherian if and only if G is finitely generated.

5. Let $M_3(\mathbb{R})$ be the 3×3-matrix algebra over the real numbers $\mathbb{R}$. For any $b \in \mathbb{R}$ let $B \in M_3(\mathbb{R})$ be the matrix $\begin{pmatrix} 1 & b & 0 \\ b & 1 & b \\ 0 & b & 1 \end{pmatrix}$. Find the set of numbers b so that the matrix equation $X^2 = B$ has at least one, and only finitely many, solutions in $M_3(\mathbb{R})$.

6. Determine the Galois groups of the following polynomials over $\mathbb{Q}$.
(a) $f(x) = x^4 + 4x^2 + 1$
(b) $f(x) = x^4 + 4x^2 - 5$

Solution:
(a)
The roots of $f(x)$ are $\pm\sqrt{-2 \pm \sqrt{3}}$. Let $\alpha = \sqrt{-2+\sqrt{3}}$ and $\beta = \sqrt{-2-\sqrt{3}}$ so that the roots of f are $\pm\alpha$ and $\pm\beta$. We claim that the splitting field of f is $K = \mathbb{Q}(\alpha)$. Note that this is certainly contained in the splitting field of f since it is a simple extension by a root of f. To see that this extension contains all roots of f, note that

$$\alpha^{-1} = \left(\sqrt{-2+\sqrt{3}}\right)^{-1} = \sqrt{-2-\sqrt{3}} = \beta$$

and so K contains $\pm\alpha$ and $\pm\beta$. Now, $f(x)$ is irreducible over $\mathbb{Q}$ by the rational roots theorem, and so this simple extension has degree four. We conclude that the Galois group of f has order 4, and is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We claim that the Galois group is in fact $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. To prove this it suffices to exhibit two automorphisms of K over $\mathbb{Q}$ with order two. One is given by $\alpha \mapsto -\alpha$ and $\beta \mapsto -\beta$. Since f is irreducible there must also be an automorphism ϕ sending $\alpha \mapsto \beta$. Note that for this automorphism we must have

$$\phi(\beta) = \phi(\alpha^{-1}) = \phi(\alpha)^{-1} = \beta^{-1} = \alpha$$

and so ϕ has order two. Hence the Galois group of f is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b)
The four roots of f in this case are $\pm\sqrt{-2 \pm 3}$, i.e. ± 1 and $\pm\sqrt{-5}$. The splitting field of f is then simply $\mathbb{Q}(\sqrt{-5})$, a quadratic extension. This implies that the Galois group of f is simply $\mathbb{Z}/2\mathbb{Z}$, with its nonidentity permutation mapping $\sqrt{-5} \mapsto -\sqrt{-5}$.

7. Prove that if A is a finite abelian group, then $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) \cong A$. (Here $\mathrm{Ext}^1_{\mathbb{Z}}(-,-)$ is also sometimes written as $\mathrm{Ext}(-,-)$.

8. Let A be the $\mathbb{C}$-algebra $\mathbb{C}[x, y]$, and define algebra automorphisms σ and τ of A by

$$\sigma(x) = y, \quad \sigma(x) = y$$

and

$$\tau(x) = x, \quad \tau(y) = \zeta y,$$

where $\zeta \in \mathbb{C}$ is a primitive third root of unity (namely, $\zeta \neq 1$ and $\zeta^3 = 1$). Let G be the group of algebra automorphisms of A generated by σ and τ. Define

$$A^G = \{f \in A \mid \phi(f) = f \text{ for all } \phi \in G\}.$$

Then A^G is a subalgebra of A – you do not need to prove this. Describe the algebra A^G by finding a set of generators and a set of relations.