2015 Algebra Prelim

September 14, 2015

1. (a) Find an irreducible polynomial of degree 5 over the field $\mathbb{Z}_2$ of two elements and use it to construct a field of order 32 as a quotient of the polynomial ring $\mathbb{Z}_2[x]$.

(b) Using the polynomial you found in part (a), find a 5×5 matrix M over $\mathbb{Z}_2$ of order 31, so that $M^{31} = I$ but $M \neq I$.

Solution:

(a)

To prove that a degree five polynomial is irreducible it suffices to show that it has no roots in $\mathbb{Z}_2$ and no quadratic factors (factors of degree three or four imply quadratic factors and roots respectively). Among all 32 degree five polynomials in $\mathbb{Z}_2[x]$ we can search for one with no linear or quadratic factors by brute force. We find quickly that $f(x) = x^5 + x^3 + 1$ has no roots (and hence no linear factors) and furthermore we can check that it is not a multiple of any of the four quadratic polynomials in $\mathbb{Z}_2[x]$:

- $f(x)$ is not a multiple of x^2 or $x^2 + x$ since it has a nonzero constant term.
- $f(x)$ is not a multiple of $x^2 + 1$ since $x^2 + 1$ has a root in $\mathbb{Z}_2$ while $f(x)$ does not.
- $f(x)$ is not a multiple of $x^2 + x + 1$ because by the Euclidean algorithm we have $f(x) = (x^2 + x + 1)(x^3 + x^2 + x) + (x + 1)$ and so $f(x)$ has nonzero remainder when divided by $x^2 + x + 1$.

We conclude that $f(x)$ has no linear or quadratic factors in $\mathbb{Z}_2[x]$ and so is irreducible. Since it is irreducible we know that $\mathbb{Z}_2[x]/\langle f(x)\rangle$ is a field, and it will have order $2^5 = 32$ since $f(x)$ has degree five. In particular this field is a 5-dimensional vector space over $\mathbb{Z}_2$.

(b)

To find a matrix of order 31 we consider $\mathbb{F}$ as a 5-dimensional vector space over $\mathbb{Z}_2$, and associate each $p(x) \in \mathbb{F}$ to the linear transformation corresponding to multiplication by $p(x)$. This yields an embedding of $\mathbb{F}$ into the ring of 5×5 matrices over $\mathbb{Z}_2$. To compute the specific matrix associated to each $p(x)$ we need to specify a basis for $\mathbb{F}$ over $\mathbb{Z}_2$. A simple one is given by $\{1, x, x^2, x^3, x^4\}$.

The group of units of $\mathbb{F}$ has order 31, a prime, and so any nonzero nonidentity element of $\mathbb{F}$ generates it. We choose x as our generator and note that x has multiplicative order 31. To associate x to a matrix we consider its action on the basis previously described. Under this basis the action of x is described by the matrix

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

where the last column arises from the relation $x^5 = x^3 + 1$ in $\mathbb{F}$. Since the embedding of $\mathbb{F}$ into the ring of 5×5 matrices preserves order we conclude that the matrix above has the same order as x, namely 31.

2. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Justify your answer.

Solution:
Let $\alpha = \sqrt{2} + \sqrt{3}$ and $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that F is Galois over $\mathbb{Q}$ and contains α, and so to determine the other roots of $\min_\alpha(\mathbb{Q})$ we need only determine the possible images of α under the elements of $\mathrm{Gal}(F/\mathbb{Q})$. There are four elements of $\mathrm{Gal}(F/\mathbb{Q})$: the identity, the map which replaces $\sqrt{2}$ by its negative, the map which replaces $\sqrt{3}$ by its negative, and the map which replaces both $\sqrt{2}$ and $\sqrt{3}$ by their negatives. From this we see quickly that the other roots of $\min_\alpha(\mathbb{Q})$ are $-\sqrt{2}+\sqrt{3}$, $\sqrt{2} - \sqrt{3}$, and $-\sqrt{2} - \sqrt{3}$. Thus we have

$$\begin{aligned}
\min_\alpha(\mathbb{Q}) &= (x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3}) \\
&= (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6}) \\
&= \boxed{x^4 - 10x + 1}.
\end{aligned}$$

3. (a) Let R be a commutative ring with no nonzero nilpotent elements. Show that the only units in the polynomial ring $R[x]$ are the units of R, regarded as constant polynomials.

(b) Find all units in the polynomial ring $\mathbb{Z}_4[x]$.

Solution: (a)
In the case that R is an integral domain the result is clear: since there are no zero divisors the product of a nonconstant polynomial with another polynomial is always nonconstant, and in particular not equal to 1. In the general case, let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a unit in $R[x]$. This implies that the image of $f(x)$ in $R/I[x]$ is also a unit for any prime ideal I of R. But when I is prime R/I is an integral domain, and so we see that $a_n, a_{n-1}, \ldots, a_1$ must be zero in R/I for all prime ideals $I \subseteq R$. Thus $a_n, a_{n-1}, \ldots, a_1$ are contained in every prime ideal of R. But the nilradical is the intersection of all prime ideals in R, and so these a_i are all in the nilradical of R. Under the assumptions of the problem R has trivial nilradical, and so $f(x) = a_0$. The only constant polynomials which are units are clearly the units of R, and so the result follows.

(b)
We saw in part (a) that if $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a unit then $a_n, \ldots, a_1$ must be contained in the nilradical of R, and it is also clear that a_0 must be a unit in R. We will show that these conditions on the a_i are sufficient for $f(x)$ to be a unit. Recall that the sum of a nilpotent element and a unit is again a unit in any commutative ring, and notice that all $a_i x^i$ are nilpotent for $1 \leq i \leq n$ as long as each a_i is nilpotent in R. In fact $f(x) - a_0$ is nilpotent, since it is the sum of finitely many nilpotent elements. Then we can write $f(x)$ as the sum of a nilpotent element and a unit: $f(x) = (f(x) - a_0) + a_0$. We conclude that the units in $R[x]$ are exactly

$$(R[x])^\times = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_0 \text{ is a unit in } R, \text{ and } a_i \text{ is nilpotent in } R \text{ for } 1 \leq i \leq n\}$$

The ring $\mathbb{Z}_4$ has nilradical $\{0, 2\}$ and its units are $\{1, 3\}$. Thus the units in $\mathbb{Z}_4[x]$ are those such that the constant coefficient is odd and all other coefficients are even.

4. Let p and q be two distinct primes. Prove that there is at most one nonabelian group of order pq (up to isomorphisms) and describe the pairs (p, q) such that there is no non-abelian group of order pq.

5. (a) Let L be a Galois extension of a field K of degree 4. What is the minimum number of subfields there could be strictly between K and L? What is the maximum number of such subfields? Give examples where these bounds are attained.

(b) How do these numbers change if we assume only that L is separable (but not necessarily Galois) over K?

Solution:
(a)
If L is Galois over K of degree four, then we know $\mathrm{Gal}(L/K)$ has four elements. The number of nontrivial proper subgroups of $\mathrm{Gal}(L/K)$ is exactly the number of intermediate fields strictly between L and K by the Galois correspondence. There are only two groups of order four: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. The former has a single intermediate subgroup generated by 2. The latter has three subgroups of order 2, generated by $(1,0)$, $(0,1)$ and $(1,1)$. Thus we see that the smallest number of intermediate fields is 1, while the largest is 3 (and in fact we can never have exactly 2).

An extension in which there is a single intermediate field is $\mathbb{Q}(\zeta)$ where ζ is a primitive 5th root of unity. This extension is Galois since it is the splitting field of $x^4 + x^3 + x^2 + 1$ over $\mathbb{Q}$. The Galois group of this extension cyclically permutes the set $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ (in this order), and the single intermediate field is $\mathbb{Q}(\zeta + \zeta^3)$ which is equal to $\mathbb{Q}(\zeta^2 + \zeta^4)$. An extension with three intermediate fields is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$. The intermediate fields in this case are the quadratic extensions $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$.

(b)
For L to be separable but not Galois, it must be the case that L is not normal. Thus we seek an extension which is separable but which contains an element whose minimal polynomial over K does not split in L.

6. Let R be a commutative algebra over $\mathbb{C}$. A derivation of R is a $\mathbb{C}$-linear map $D : R \to R$ such that (i) $D(1) = 0$, and (ii) $D(ab) = D(a)b + aD(b)$ for all $a, b \in R$.

(a) Describe all derivations of the polynomial ring $\mathbb{C}[x]$.

(b) Let A be the subring (or $\mathbb{C}$-subalgebra) of $\mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ generated by all derivations of $\mathbb{C}[x]$ and the left multiplications by x. Prove that $\mathbb{C}[x]$ is a simple left A-module. Note that the inclusion $A \to \mathrm{End}_{\mathbb{C}}(\mathbb{C}[x])$ defines a natural left A-module structure on $\mathbb{C}[x]$.

Solution:

(a)

We first claim that $D(x^n) = nx^{n-1}D(x)$. When $n = 0$ this is clear since we have $D(x^0) = D(1) = 0$. For general n we proceed by induction. Applying (ii) when $n \geq 1$ we have

$$\begin{aligned} D(x^n) &= xD(x^{n-1}) + x^{n-1}D(x) \\ &= x((n-1)x^{n-2}D(x)) + x^{n-1}D(x) && \text{(By inductive hypothesis)} \\ &= nx^{n-1}D(x) \end{aligned}$$

as desired. Since D is a $\mathbb{C}$-linear map this rule is sufficient to specify the action of D on all elements of $\mathbb{C}[x]$. Thus we see that a derivation D is uniquely determined by the value of $D(x)$, on which there is no restriction. That is, every derivation is obtained by specifying $D(x) = f(x)$ and extending the action of D to all of $\mathbb{C}[x]$ via $\mathbb{C}$-linearity and the identity $D(x^n) = nx^{n-1}D(x)$.

(b)

Let $M \subseteq \mathbb{C}[x]$ be a nonzero submodule of the A-module $\mathbb{C}[x]$. To prove $\mathbb{C}[x]$ is simple it suffices to show that $M = \mathbb{C}[x]$. Our approach will be to first show $\mathbb{C} \subseteq M$ and then use multiplication by x to generate all of $\mathbb{C}[x]$.

Let $f \in M$ be nonzero, and if necessary multiply f by x so that it is nonconstant. The result is of course still in M since M is invariant under the action of A. We may then write

$$f = \sum_{i=0}^{n} a_i x^i$$

where $n \geq 1$ and $a_n \neq 0$. Letting $D \in A$ be the usual polynomial derivative, we can applying D a total of $n-1$ times to f to obtain a nonzero polynomial of degree exactly one which is again in M. Let $g = b_0 + b_1 x$ denote this polynomial. Then for any $c \in \mathbb{C}$, let D_c denote the derivation defined by $D(x) = c/b_1$ and observe that

$$D_c(g) = D_c(b_0) + b_1 D_c(x) = 0 + b_1(c/b_1) = c$$

is an element of M. Hence $\mathbb{C} \subseteq M$. Since M is invariant under multiplication by x we also have that $cx^n \in M$ for any $n \geq 0$ and $c \in \mathbb{C}$. Closure of M under addition then gives us that $M = \mathbb{C}[x]$. Thus $\mathbb{C}[x]$ is a simple A-module, as desired.

7. Let G be a non-abelian group of order p^3 with p a prime.

(a) Determine the order of the center Z of G.

(b) Determine the number of inequivalent complex 1-dimensional representations of G.

(c) Compute the dimensions of all the inequivalent irreducible representations of G and verify that the number of such representations equals the number of conjugacy classes of G.

Solution: (a) By Langrange's Theorem there are four candidates for the order of Z: $1, p, p^2$, and p^3. Since G is nonabelian we can rule out the last possibility. Groups of order p^n always have nontrivial center, so we can also rule out 1. This leaves p and p^2. Recall that the center of a group is always normal. If $|Z| = p^2$, then G/Z has p elements and is cyclic. But the quotient by the center being cyclic implies that G is abelian, a contradiction. Hence the only possible order for Z is $\boxed{p}$.

(b) There are exactly $|G/[G,G]|$ complex 1-dimensional representations. To see why this is the case, observe that a complex 1-dimensional representation of G is a group homomorphism $\rho : G \to \mathbb{C}^\times$. Since $\mathbb{C}^\times$ is abelian, the commutator $[G,G]$ must be in the kernel of ϕ (otherwise the image of $\rho(G)$ would not be abelian). Hence ρ is in essence a representation of the abelian group $G/[G,G]$, in the sense that any 1-dimensional representation of $G/[G,G]$ can be uniquely extended to a representation of G. The number of complex representations of an abelian group is simply the number of elements in the group and all representations are automatically 1-dimensional, so it follows that there are $|G/[G,G]|$ 1-dimensional representations of G.

Thus we seek to compute $|G/[G,G]|$. Recall that the commutator is the smallest normal subgroup H so that G/H is abelian. Note that G/Z has order p^2 and is abelian, so we have $[G,G] \leq Z$. But since G is nonabelian we know $[G,G]$ is nontrivial and it follows that $Z = [G,G]$ since $|Z|$ is prime. We then have that $|G/[G,G]| = p^2$, and there are $\boxed{p^2}$ irreducible complex 1-dimensional representations of G.

(c) From part (b) we have p^2 total 1-dimensional representations. Recall that the dimension of a representation always divides the order of G, and so the remaining representations have dimension p, p^2 or p^3. Moreover, the sum of squares of the dimensions of all irreducible representations equals $|G| = p^3$. The 1-dimensional representations account for a total of p^2 in this sum, and so if $d_1, \ldots, d_k$ are the degrees of the higher dimensional irreducible representations we must have $p^3 = p^2 + d_1^2 + \cdots + d_k^2$ or equivalently

$$p^2(p-1) = d_1^2 + \cdots + d_k^2.$$

Since each d_i is a multiple of p we see that this is only possible if $d_i = p$ and $k = p-1$. Hence there are $p-1$ irreducible representations of dimension greater than one. In total we obtain $\boxed{p^2 + p - 1}$ irreducible representations.

To verify that this is the number of conjugacy classes in G we use the class equation. If $C_1, \ldots, C_l$ are the conjugacy classes of size greater than one in G we have that $p^3 = p + \sum_{i=1}^{l} |C_i|$ or equivalently

$$p(p^2 - 1) = \sum_{i-1}^{l} |C_i|.$$

Moreover each $|C_i|$ is a multiple of p, since it must divide p^3 and is not equal to 1. We see immediately that $|C_i| = p$ for all i, and $l = p^2 - 1$. The total number of conjugacy classes is then $p^2 - 1 + p = p^2 + p - 1$, since the only other conjugacy classes are of size one, arising from elements of Z. This concludes the proof.

8. Prove that every finitely generated projective module over a commutative noetherian local ring is free.