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 $\mathbb{Z}_4[x]$.

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. (a) 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 $\mathbb{C}[x]$.

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)

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