QR Exam Algebra
January 4, 2017
Morning

(1) Suppose that R is a commutative ring with 1 with only finitely many ideals. Suppose that $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_d$ are all maximal ideals.
   (a) Show that if $a \in \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_d$ then a is nilpotent.
   (b) Show that if the number of distinct ideals of R is not a power of 2, then R contains a nonzero nilpotent element.

(2) Suppose that G is group of order $2^4 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ with a normal 2-Sylow subgroup. Show that the center of G contains more than 1 element.

(3) We denote the field with q elements by $\mathbb{F}_q$. Let $\psi : \mathbb{F}_{3^{18}} \to \mathbb{F}_{3^{18}}$ be the map defined by $\psi(a) = a^3 - a$. For which positive integers d is the kernel of ψ^d a subfield of $\mathbb{F}_{3^{18}}$?

(4) Let D_4 be the dihedral group with 8 elements. Construct a Galois extension $K/\mathbb{Q}$ with Galois group D_4. In your example, describe explicitly all intermediate fields L with $\mathbb{Q} \subset L \subset K$ such that $L/\mathbb{Q}$ is an extension of degree 2.

(5) (a) Give an example of a nonzero finitely generated $\mathbb{Z}[X]$-module M which is torsion-free, but not free.
   (b) Give an example of a nonzero finitely generated $\mathbb{Z}[X]$-module M and two irreducible elements $f_1, f_2 \in \mathbb{Z}[X]$ such that $f_1 f_2$ kills M, but M does not decompose as a product $M_1 \times M_2$ such that f_1 kills M_1 and f_2 kills M_2.

QR Exam Algebra
January 4, 2017
Afternoon

(1) Fix a field k and A be the ring $k[X]/(X^p - 1)$. Classify all simple A-modules in the following two cases:
   (a) $k = \mathbb{Q}$;
   (b) $k = \mathbb{F}_p$, the field with p elements.
   (An A-module M is simple if it has exactly 2 submodules, namely 0 and M itself.)

(2) Let K be a separably closed field, so K does not have any finite seperable field extension other than K itself. Let L/K be a finite nontrivial extension of fields.
   (a) Show that the trace map $\mathrm{Tr} : L \to K$ is the zero map.
   (b) Give an example of such a field extension L/K.

(3) Let V_n be the space of polynomials in x of degree at most n with real coefficients. Define a linear map $\phi : V_n \to V_n$ by $\phi(f) = xf' + f''$. Show that there exists $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{R}$ and a basis $\{f_0, f_1, \ldots, f_n\}$ of V_n such that $\phi(f_i) = \lambda_i f_i$ for all $i = 0, 1, \ldots, n$.

(4) Suppose that V is a finite dimensional real vector space equipped with a symmetric bilinear form $(\cdot, \cdot)$.
   (a) Show that there exists a bilinear form $(\cdot, \cdot)_\star$ on $\bigwedge^2 V$ with the property

$$(v_1 \wedge v_2, w_1 \wedge w_2)_\star = (v_1, w_1)(v_2, w_2) - (v_1, w_2)(v_2, w_1).$$

   (b) Give the signature of $(\cdot, \cdot)_\star$ in terms of the signature of $(\cdot, \cdot)$.

(5) Show that an abelian group of order 100 cannot act faithfully on a set with 13 elements.

(1) (a) Suppose that $a \in \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_d$. Consider the chain

$$(a) \supseteq (a^2) \supseteq (a^3) \supseteq (a^4) \supseteq \cdots$$

Because there are only finitely many ideals, $(a^m) = (a^{m+1})$ for some m. It follows that $a^m = a^{m+1}b$ for some $b \in R$. We have $(1 - ab)a^m = 0$. If $1 - ab$ is not invertible, then $1 - ab \in \mathfrak{m}_r$ for some r. But then we have $a \in \mathfrak{m}_r$ and $1 = (1 - ab) + ab \in \mathfrak{m}_r$. Contradiction. So $1 - ab$ is invertible and $a^m = 0$.

(b) Suppose that R does not contain a nonzero nilpotent element. Then by part (a), $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_r = (0)$. Since $\mathfrak{m}_i + \mathfrak{m}_j = R$ for $i \neq j$, we have

$$R = R/\mathfrak{m}_1 \times R/\mathfrak{m}_2 \times \cdots \times R/\mathfrak{m}_d$$

because of the Chinese Remainder Theorem. Each field $R/\mathfrak{m}_i$ has exactly 2 ideals, and R has 2^d ideals.

(2) Let S be the 2-Sylow subgroup of G. The group G acts on S by conjugation. The center $Z(S)$ of S is a characteristic subgroup of S (i.e., it is fixed by any automorphism). So $Z(S)$ is also normalized by G. The groups G and G/S act on $Z(S)$ by conjugation. This yields a group homomorphism $\gamma : G/S \to \mathrm{Aut}(Z(S))$. We have $Z(S) \cong \mathbb{Z}/2\mathbb{Z}^d$ where $1 \leq d \leq 3$. The cardinality of $\mathrm{Aut}(Z(S))$ is $(2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3)$, $(2^3 - 1)(2^3 - 2)(2^3 - 2^2)$, $(2^2 - 1)(2^2 - 2)$ or $(2 - 1)$. All these numbers are realtively prime to $|G/Z(S)| = 11 \cdot 13 \cdot 17 \cdot 19$. So the image of γ is trivial, and G/S and G act trivially on $Z(S)$ by conjugation. This implies that $Z(G) = Z(S)$ is nontrivial.

(3) We can view $\mathbb{F}_{3^{18}}$ as an $\mathbb{F}_3$-vector space. The Frobenius map $\phi : \mathbb{F}_{3^{18}} \to \mathbb{F}_{3^{18}}$ is $\mathbb{F}_3$-linear and has order 18. So ϕ satisfies the polyonomial $X^{18} - 1 = (X - 1)^9(X + 1)^9$. The eigenvalues of ϕ are 1 and -1. The Jordan normal form of ϕ has Jordan blocks with eigenvalues 1 and -1. The $\ker(\phi^2 - I)$ is the field $\mathbb{F}_{3^2}$, which is 2-dimensional. This implies that there is one 9×9 Jordan block with eigenvalue 1, and one 9×9 Jordan block with eigenvalue -1. From this it is clear the the dimension of the kernel of $\psi^d = (\phi - I)^d$ is equal to d if $d \leq 9$ and equal to 9 if $d \geq 9$. For $d \geq 9$, $\ker(\psi^d) = \ker(\psi^9) = \ker(\phi^9 - I) = \mathbb{F}_{3^9}$ is a subfield. For $d = 3$, $\ker(\psi^3) = \mathbb{F}_{3^3}$ is a subfield, and for $d = 1$, $\ker(\psi) = \mathbb{F}_3$ is a subfield. The field $\mathbb{F}_{3^{18}}$ has a subfield of order 3^d if and only if d divides 18. So for $d = 4, 5, 6, 7, 8$ there is no subfield with 3^d elements and the kernel of ψ^d is not a subfield. For $d = 2$, the kernel of ψ^2 has 9 elements, but is not equal to the field $\mathbb{F}_{3^2}$. Indeed, if $a \in \mathbb{F}_9 \setminus \mathbb{F}_3$, then we have $\psi^2(a) = (\phi^2 + \phi + I)(a) = (\phi - I)(a) \neq 0$. So $\ker(\psi^d)$ is a subfield for $d = 1$, $d = 3$ and $d \geq 9$.

(4) Let $K = \mathbb{Q}(\sqrt[4]{2}, i)$ be the splitting field of $X^4 - 2$. Then $K/\mathbb{Q}$ is clearly a Galois extension. Since $X^4 - 2$ is irreducible of degree 4 by Eisenstein's criterion, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ has degree 4. Since i is not real, $i \notin \mathbb{Q}(\sqrt[4]{2})$ and $K/\mathbb{Q}(\sqrt[4]{2})$ is an extension of degree 2. The extension $K/\mathbb{Q}$ has degree $4 \cdot 2 = 8$. Let $\alpha_k = i^{k-1}\sqrt[4]{2}$ for $k = 1, 2, 3, 4$. Then complex conjugation σ corresponds to the permutation $(2\ 4)$. There exists an automorphism τ that sends α_1 to α_2. We may replace τ by $\tau\sigma$ and assume that $\tau(i) = i$. Then τ is the permutation $(1\ 2\ 3\ 4)$. Now σ and τ generate a Dihedral group D_4 of order 8. Every subgroup of D_4 of index 2 contains τ^2. The group $D_4/\langle \tau^2 \rangle$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with generators τ and σ. The quadratic extension L have to be$K^{\langle \tau \rangle} = \mathbb{Q}(i)$, $K^{\langle \tau\sigma \rangle} = \mathbb{Q}(i\sqrt{2})$ or $K^{\langle \tau^2, \sigma \rangle} = \mathbb{Q}(\sqrt{2})$.

(5) (a) Take $M = (2, X) \subseteq \mathbb{Z}[X]$. Since $\mathbb{Z}[X]$ is free and therefore torsion-free, so is the ideal M. If M is free then we have $(2, X) = (f)$ for some polynomial f. But then f divides 2 and X. But then f has to be a constant dividing X and therefore has to be equal to ± 1. It follows that $1 \in (2, X)$. But it is easy to see that this is not the case. $\mathbb{Z}[X]/(2, X)$ is isomorphic to the field $\mathbb{F}_2$.

(b) Let $M = \mathbb{Z}[X]/(2X)$, $f_1 = 2$ and $f_2 = X$. Clearly, $2X$ kills M. Suppose that $M = M_1 \times M_2$ with $2M_1 = XM_2 = 0$. Then we can write $1 = a_1 + a_2$ with $2a_1, Xa_2 \in (2X)$. It follows that $2X = 2X(a_1 + a_2) = (2a_1)X + (Xa_2)2 \in (2X)(2, X)$ and $1 \in (2, X)$. Contradiction.

(1) (a) If $k=\mathbb{Q}$, then $X^p-1=(X-1)(X^{p-1}+X^{p-2}+\cdots+1)$ is the factorization into irreducibles, and we have

$$R=k[X]/(X^p-1)\cong k[X]/(X-1)\times k[X]/(X^{p-1}+X^{p-2}+\cdots+1)=k\times L$$

is a product of 2 fields. Now k and L are simple modules. If M is a simple module, then we can choose $a\in M$ nonzero, and the map $f\mapsto fa$ gives a surjective module homomorphism $R\to M$. The only quotients of R are k and L.

(b) If $k=\mathbb{F}_p$, then $X^p-1=(X-1)^p$. Now k is a simple R-module. If M is any simple module then we have a surjective module homomorphism $R\to M$. The kernel is a maximal ideal, and has to be $(X-1)$. This shows that M is isomorphic to the module k.

(2) Let p be the characteristic of the field K.

(a) Suppose that L/K is a nontrivial extension. Let $a\in L$ and define $M=K(a)$. If $L\neq M$, then we have $\operatorname{Tr}_{L/M}(a)=[L:M]a=0$ because $[L:M]$ is divisible by p. We have $\operatorname{Tr}_{L/K}(a)=\operatorname{Tr}_{M/K}\operatorname{Tr}_{L/M}(a)=0$. Suppose that $L=M$ and $[L:K]=p^r$. Let $f(X)$ be the minimum polynomial of a. Since the extension is inseperable we have $f'(X)=0$. In particular, the coefficient of X^{p^r-1}, which is $-\operatorname{Tr}(a)$ is equal to 0.

(b) Let F be the algebraic closure of the field $\mathbb{F}_2(X)$, and let $K\subset F$ be the separable closure of $\mathbb{F}_2(X)$. It consists of all $a\in F$ such that $F_2(X,a)/F_2(X)$ is separable. Let $L=K(X^{1/p})$. Then L/K is a inseperable, nontrivial extension.

(3) Let us choose the basis $1,x,x^2,\ldots,x^n$ of V_n. With respect to this basis, ϕ has the matrix

$$\begin{pmatrix} 0 & 0 & 2 & 0 & 0 & \cdots\\ 0 & 1 & 0 & 6 & 0 & \cdots\\ 0 & 0 & 2 & 0 & 12 & \cdots\\ 0 & 0 & 0 & 3 & 0 & \cdots\\ 0 & 0 & 0 & 0 & 4 & \cdots\\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

So the matrix is upper triangular with diagonal entries $0,1,2,\ldots,n$. The diagonal entries are the eigenvalues and they are all distinct. This implies that ϕ is diagonalizable. This means that there exists a basis $f_0,f_1,\ldots,f_n$ with $\phi(f_i)=\lambda_i f_i$. The eigenvalues $\lambda_0,\lambda_1,\ldots,\lambda_n$ are equal to $0,1,\ldots,n$.

(4) (a) For fixed $v_1,v_2\in V$, define $f_{v_1,v_2}:V\times V\to\mathbb{R}$ by

$$f_{v_1,v_2}(w_1,w_2)=(v_1,w_1)(v_2,w_2)-(v_1,w_2)(v_2,w_1).$$

It is easy to see that f_{v_1,v_2} is bilinear. Also $f_{v_1,v_2}(w,w)=0$, so it is also alternating. So there exists a unique linear function $F_{v_1,v_2}:\bigwedge^2 V\to\mathbb{R}$ such that

$$F_{v_1,v_2}(w_1\wedge w_2)=(v_1,w_1)(v_2,w_2)-(v_1,w_2)(v_2,w_1).$$

Similarly, using this unqueness, we see that the map $V\times V\to(\bigwedge^2 V)^\star$ defined by

$$(v_1,v_2)\mapsto F_{v_1,v_2}$$

is bilinear and alternating. So there exists a linear map $\psi : \bigwedge^2 V \to (\bigwedge^2 V)^\star$ such that

$$\psi(v_1 \wedge v_2) = F_{v_1,v_2}.$$

If $a, b \in \bigwedge^2 V$, then we define $(a,b)_\star = \psi(a)(b) \in \mathbb{R}$. It is now clear that $(\cdot,\cdot)_\star$ is bilinear, and

$$(v_1 \wedge v_2, w_1 \wedge w_2)_\star = \psi(v_1 \wedge v_2)(w_1 \wedge w_2) = F_{v_1,v_2}(w_1 \wedge w_2) = (v_1, w_1)(v_2, w_2) - (v_1, w_2)(v_2, w_1).$$

(b) Suppose that the signature of $(\cdot,\cdot)$ is (p,q,r) (p positive, q negative, r zero eigenvalues) where $p, q, r = n$. Let $a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q, c_1, c_2, \ldots, c_r$ be an orthogonal basis with $(a_i, a_i) = 1$, $(b_j, b_j) = -1$ and $(c_k, c_k) = 0$ for all i, j, k. A basis of $\bigwedge^2 V$ is given by

vector	index range	cardinality	sign
$a_i \wedge a_j$	$(1 \le i < j \le p)$	$\binom{p}{2}$	$+1$
$a_i \wedge b_j$	$(1 \le i \le p, 1 \le j \le q)$	pq	-1
$a_i \wedge c_j$	$(1 \le i \le p, 1 \le j \le r)$	pr	0
$b_i \wedge b_j$	$(1 \le i < j \le q)$	$\binom{q}{2}$	$+1$
$b_i \wedge c_j$	$(1 \le i \le q, 1 \le j \le r)$	qr	0
$c_i \wedge c_j$	$(1 \le i < j \le r)$	$\binom{r}{2}$	0

So the signature of $(\cdot,\cdot)_\star$ is $(\binom{p}{2} + \binom{q}{2}, pq, pr + qr + \binom{r}{2})$.

(5) Suppose that G is an abelian group of order 100 acting faithfully on a set with 13 elements. This gives an injective group homomorphism $\phi : G \to S_{13}$. Let H be the 5-Sylow subgroup of G. Since 13! has only 2 factors 5, the image $\phi(H)$ is a 5-Sylow subgroup. Since the 5-Sylow subgroup is unique up to conjugation, we may assume without loss of generality that $\phi(H)$ is generated by (1 2 3 4 5) and (6 7 8 9 10). The centralizer of $\phi(H)$ in S_{13} is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times S_3$ and has 150 elements. The image $\phi(G)$ has 100 elements. On the other hand, $\phi(G)$ is contained in the centralizer of $\phi(H)$ and its order has to divide 150. Contradiction.