QR Exam Algebra
September 3, 2018
Morning

Justify your answers.

(1) Suppose that R is a Unique Factorization Domain (UFD) and S is a subring of R containing 1 with the following property: if $a, b \in R$ are nonzero and $ab \in S$, then $a, b \in S$. Show that S is also a UFD.

(2) Suppose that the finite group G acts transitively on the set X. For a prime p, let S be a Sylow p-subgroup of G and $N(S)$ be its normalizer. Define

$$F := \{x \in X \mid g \cdot x = x \text{ for all } g \in S\}$$

as the set of points fixed by S. Prove that $N(S)$ leaves F invariant and acts transitively on F. Be sure to clearly indicate the parts of Sylow theory which you use.

(3) Suppose that R is a Principal Ideal Domain (PID), M is a finitely generated free R-module and that $f : M \times M \to R$ is a bilinear function (i.e., for every $x \in M$ the map $y \mapsto f(x, y)$ and the map $y \mapsto f(y, x)$ are R-module homomorphisms). Show that the *set of values* $\mathrm{Im}(f) := \{f(x, y) \mid x, y \in M\}$ is an ideal in R.

(4) Let ζ be a 77-th primitive root of unity.
  (a) Compute the degree of the field extension $d = [\mathbb{Q}(\zeta) : \mathbb{Q}]$.
  (b) For every divisor e of d determine the number of intermediate fields K with $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta)$ and $[K : \mathbb{Q}] = e$.

(5) Suppose that A, B are 2×2 matrices with entries in $\mathbb{Q}$ such that $A^2 = 2I$ and $B^2 = -I$. Show that A and B do not commute.

QR Exam Algebra
September 3, 2018
Afternoon

Justify your answers.

(1) What are the prime ideals in the ring $\mathbb{F}_3[x]/(x^5 + x^4 + 1)$? Which of these prime ideals are maximal?

(2) Suppose that F is a field with q elements, and E/F is a field extension of degree n with $n \geq 2$. Let $N : E \to F$ be the norm map.
 (a) Give an integer t so that $N(x) = x^t$ for all $x \in E$.
 (b) Prove that N is onto.
 (c) Prove that a nonzero subring of E is a field.
 (d) Prove that the set $U := \{x \in E \mid N(x) = 1\}$ generates E as a ring.

(3) (a) Let V be the space $\mathbb{R}^4$ of 4×1 column vectors. Show that there exists a bilinear map $\varphi : \bigwedge^2 V \times \bigwedge^2 V \to \mathbb{R}$ with the property

$$\varphi(a \wedge b, c \wedge d) = \det(a\ b\ c\ d)$$

for all (column) vectors $a, b, c, d \in V$. (Here $(a\ b\ c\ d)$ is the 4×4 matrix whose columns are a, b, c, d.)
 (b) What is the Sylvester signature of φ?

(4) Suppose F is an a field, V and W are $\mathbb{F}$-vector spaces and $T : V \to V$ and $U : W \to W$ are linear maps that have Jordan canonical forms. Assume that the Jordan canonical form of T is an $m \times m$ Jordan block with eigenvalue a, and the Jordan canonical form of U is an $n \times n$ Jordan block with eigenvalue b. Let $S : V \otimes U \to V \otimes U$ be the unique linear map with the property $S(x \otimes y) = Tx \otimes Uy$ for all $x \in V$ and $y \in U$.
 (a) Give the characteristic polynomial for S.
 (b) Give the Jordan canonical form for S in the case $a = b = 0$ and $m = n = 2$.

(5) Suppose that G_1, G_2 are groups (possibly noncommutative) and that S is a subgroup of $G := G_1 \times G_2$. Let π_i be the projection of $G_1 \times G_2$ to the i-th factor, G_i. Define $H_i := \pi_i(S), K_i := S \cap G_i$.
 (a) Prove that K_i is normal in H_i.
 (b) Prove that $H_1/K_1 \cong H_2/K_2$.

QR Exam Algebra Solutions
September 3, 2018
Morning

(1) If $a \in R$ is a unit, then $aa^{-1} = 1 \in S$, so $a, a^{-1} \in S$. So $R^\times \subseteq S^\times$. If $a \in S$ is irreducible, and $a = bc$ with $b, c \in R$, then $b, c \in S$. So b or c is a unit. This shows that a is irreducible in R. Suppose that $p_1, p_2, \ldots, p_r, q_1, \ldots, q_s$ are irreducible in S such that

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Now $p_1, \ldots, p_r, q_1, \ldots, q_s$ are also irreducible in R. Because R is a UFD, we have $r = s$ and after rearranging, p_i is equal to q_i up to a unit in R. But then p_i is equal to q_i up to a unit in S. This proves that S is a UFD.

(2) Let $g \in N(S)$ and $x \in F$. Then $g \cdot x$ is fixed by S since $(Sg) \cdot x = (gS) \cdot x = g \cdot x$. So, $N(S)$ stabilizes F. Given two points $x, y \in F$, there is $g \in G$ so that $g \cdot x = y$. Since S fixes x, gSg^{-1} fixes y, so S is also a Sylow group of G_y, the stabilizer of y in G. Therefore, by Sylow's theorem applied to G_y, there exists $h \in G_y$ so that $S = h(gSg^{-1})h^{-1}$. This means that $w := hg \in N(S)$. So $w^{-1} \in N(S)$. We now calculate that $w^{-1}(y) = g^{-1}h^{-1}(y) = g^{-1}(y) = x$. It follows that x, y are in the same orbit of $N(S)$ acting on F.

(3) Let I be the ideal generated by $\mathrm{Im}(f)$. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be any two bases for M. Form the Gram matrix $A := (f(y_j, x_i))$. Then I is just the R-span of the entries of A. A basic theorem says that there are scalars $r_1, \ldots, r_n$ and invertible matrices P, Q so that r_i divides r_{i+1} for $i = 1, \ldots, n-1$ and PAQ is the diagonal matrix

$$D := \begin{pmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_n \end{pmatrix}.$$

The previous paragraph applied to D instead of A makes it obvious that I is just the principal ideal generated by r_1. There exist $x, y \in M$ so that $f(x, y) = r_1$. We conclude that $I = \mathrm{Im}(f)$ since any element of I has the form $cr_1 = f(cx, y) \in \mathrm{Im}(f)$, for $c \in R$.

(4)

(a) $d = [Q(\zeta) : \mathbb{Q}] = \phi(77) = \phi(7 \cdot 11) = (7-1)(11-1) = 60 = 2^2 \cdot 3 \cdot 5$.

(b) The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $G = (\mathbb{Z}/77\mathbb{Z})^\times = (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/10\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/3 \times \mathbb{Z}/5$. The subgroups of G are of the form $H = P_2 \times P_3 \times P_5$. where $P_2 = 0$, $P_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$ or P_2 is one of the 3 subgroups of order 2. $P_3 = 0$ or $P_3 = \mathbb{Z}/3\mathbb{Z}$ and $P_5 = 0$ or $P_5 = \mathbb{Z}/5\mathbb{Z}$. Using the Galois correspondence we get the following table:

$e = [\mathbb{Q}(\zeta)^H/\mathbb{Q}]$	$\lvert H\rvert$	$\lvert P_2\rvert$	$\lvert P_3\rvert$	$\lvert P_3\rvert$	number of intermediate fields
1	60	4	3	5	1
3	20	4	1	5	1
5	12	4	3	1	1
15	4	4	1	1	1
2	30	2	3	5	3
6	10	2	1	5	3
10	6	2	3	1	3
30	2	2	1	1	3
4	15	1	3	5	1
12	5	1	1	5	1
20	3	1	3	1	1
60	1	1	1	1	1

(5) Suppose that A and B commute. After we conjugate A and B with the same matrix C we may assume without loss of generality that

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

Then we set

$$B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.$$

Since B has trace 0, we have $w = -x$. From the equation

$$\begin{pmatrix} z & -x \\ 2x & 2y \end{pmatrix} = AB = BA = \begin{pmatrix} 2y & x \\ -2x & z \end{pmatrix}$$

follows that $x = 0$ and $z = 2y$. Now we have

$$B^2 = \begin{pmatrix} 2y^2 & 0 \\ 0 & 2y^2 \end{pmatrix}$$

This cannot be $-I$. Contradiction.

QR Exam Algebra Solutions
September 3, 2018
Afternoon

Justify your answers.

(1) Let $p(x) = x^5 + x^4 + 1$. Prime ideals in $\mathbb{F}_3[x]/(p(x))$ correspond to ideals in $\mathbb{F}_3[x]$ that contain $p(x)$. Such ideals are generated by prime divisors (which are the same as irreducible divisors since $\mathbb{F}_3[x]$ is a PID). We factor $p(x)$. Since $p(1) = 0$ we get a factorization $p(x) = (x-1)q(x)$ where $q(x) = x^4 - x^3 - x^2 - x - 1$. Also $q(1) = 0$ so we have a factorization $q(x) = (x-1)(x^3 - x + 1)$. So we get $p(x) = (x-1)q(x) = (x-1)^2(x^3 - x + 1)$. The prime divisors of $p(x)$ (up to a unit) are $x - 1$ and $x^3 - x + 1$. So the prime ideals of $\mathbb{F}_3[x]/(p(x))$ are the ideal generated by $x - 1 + (p(x))$ and the ideal generated by $x^3 - x + 1 + (p(x))$. These ideals are also maximal, because the quotient with respect to these ideals are finite integral domains which are fields.

(2) (a) The Galois group of E/F is cyclic of order n, generated by the map $x \mapsto x^q$, whence $t = 1 + q + q^2 + \cdots + q^{n-1}$.

(b) Clearly $N0 = 0$. If x is a generator for the cyclic group $E^\times := E \setminus \{0\}$, $Nx = x^{1+q+q^2+\cdots+q^{n-1}}$. The exponent is a divisor of $q^n - 1$ so the kernel of the group homomorphism N on the group $E^\times$ has order $1 + q + q^2 + \cdots + q^{n-1}$. Since $q - 1 = (q^n - 1)/(1 + q + q^2 + \cdots + q^{n-1})$, (i) follows from the formula $|\operatorname{Im}(f)| = |H/\operatorname{Ker}(f)|$ for a homomorphism f from a finite group H to another group.

(c) If R is a finite integral domain with $1 \neq 0$, $0 \neq a \in R$, then the map $x \mapsto ax$ is an injection of R into R. Since R is finite, it is a bijection. Therefore, there exists $b \in R$ so that $ab = 1$. So, R is a field. The statement (c) follows.

(d) From (b), we know that U has cardinality $1 + q + q^2 + \cdots + q^{n-1}$, for $n \geq 2$. Since $0 \in S$, S has cardinality at least $2 + q^{n-1}$. A subring of a finite field is a field, by (c). Therefore, E contains S as a subfield and so there exists an integer $m \geq 1$ so that $|E| = |S|^m$, i.e., $m = \dim_S(E)$. It suffices to prove $m = 1$. We have the inequality $q^n \geq (2 + q^{(n-1)})^m > q^{(n-1)m}$, whence $n > m(n-1)$ and (since $n \geq 2$), $\frac{n}{n-1} > m$ implies $m = 1$, and the result is proved.

(3) (a) Since the determinant is multi-linear, there exists a unique linear map $\psi : V \otimes V \otimes V \otimes V \to \mathbb{R}$ with $\psi(a \otimes b \otimes c \otimes d) = \det(a\ b\ c\ d)$. Since the determinant is alternating, ψ factors through $\gamma : \bigwedge^2 V \otimes \bigwedge^2 V \to \mathbb{R}$. with the property $\gamma((a \wedge b) \otimes (c \wedge d)) = \det(a\ b\ c\ d)$. For φ we can take the decomposition

$$\bigwedge^2 V \times \bigwedge^2 V \to \bigwedge^2 V \otimes \bigwedge^2 V \to \mathbb{R}$$

(b) In terms of the basis $(e_1 \wedge e_2, e_3 \wedge e_4, e_1 \wedge e_3, -e_2 \wedge e_4, e_1 \wedge e_4, e_2 \wedge e_3)$ we get the matrix

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

This matrix has eigenvalue 1 with multiplicity 3 and -1 with multiplicity 3. So the signature is $(3, 3, 0)$ (3 positive eigenvalues, 3 negative eigenvalues and no zero eigenvalues).

(4) (a) Use filtrations on V and U with 1-dimensional factors to get the characteristic polynomial to be $(x - ab)^{mn}$.

(b) Take a basis e_1, e_2 for V which gives the JCF matrix for T on V. Similarly a basis f_1, f_2 for U on W. Then $(T \otimes U)^2$ annihilates every standard basis element $e_i \otimes f_j$, so the minimal polynomial divides x^2. So the JCF is a block diagonal sum of $J(0, 1)$s and $J(0, 2)$s. If we order the basis thusly $e_1 \otimes f_1$, $e_1 \otimes f_2$, $e_2 \otimes f_1$, $e_2 \otimes f_2$, it is obvious that the kernel of $T \otimes U$ has dimension 3. Therefore the JCF is a block diagonal sum of two $J(0, 1)$ and one $J(0, 2)$.

(5) (a) Since G_i is normal in G, S normalizes $K_i = S \cap G_i$. Also, for $i \neq j$, G_j normalizes any subgroup of G_i, so SG_j normalizes K_i. Since $SG_j = \pi_i(S) \times G_j$, $H_i = \pi_i(S)$ normalizes K_i.

(b) For each i, the homomorphism $S \to H_i/K_i$, defined by $x \mapsto_\pi (x)K_i \in H_i/K_i$ for $x \in S$, is onto and has kernel $K_1 \times K_2$. Therefore each H_i/K_i is isomorphic to $S/(K_1 \times K_2)$, whence (b) holds.