May 2016, Qualifying Review Algebra, Morning

Problem 1.
(a) Suppose I is an ideal in a principal ideal domain R such that $I^2 = I$. Show that $I = (0)$ or $I = R$.
(b) Give an example of an ideal I in a commutative ring R such that $I^2 = I$ but I is not (0) or R.

Solution.
(a) Since R is a PID, we have $I = (a)$ for some $a \in R$, and so $I^2 = (a^2)$. Thus $(a) = (a^2)$, and so $ua = a^2$ for some unit u of R. If $a = 0$ then $I = (0)$. Otherwise, we can divide by a and we find $u = a$, so $I = (u) = R$.
(b) Take $R = \mathbf{C} \times \mathbf{C}$ and I to be the ideal generated by the element $(1, 0)$.

Problem 2. Suppose that A is an invertible symmetric $n \times n$ matrix with real entries. Show that there exist invertible real matrices R and S such that $I_n = RAR^t - SAS^t$, where I_n is the $n \times n$ identity matrix.

Solution. Suppose that the signature of A is $(p, n-p, 0)$, i.e., it has p positive eigenvalues and $n - p$ negative eigenvalues. Define

$$B = \begin{pmatrix} 2I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}, \quad C = \begin{pmatrix} I_p & 0 \\ 0 & -2I_{n-p} \end{pmatrix}.$$

Then we have $I = B - C$. The matrices A, B, C all have the same signature, so $B = RAR^t$ for some invertible real matrix R and $C = SAS^t$ for some invertible matrix S.

Problem 3. Let A be a 2×2 matrix with real entries. Suppose there exist non-zero vectors $v, w \in \mathbf{R}^2$ such that $\|A^n v\| \to 0$ as $n \to \infty$ and $\|A^n w\| \to \infty$ as $n \to \infty$, where $\| \cdot \|$ denotes the length of a vector. Show that A is diagonalizable over the reals, i.e., there exists an invertible real matrix S such that SAS^{-1} is diagonal.

Solution. We first note that if B is conjugate to A then there still exist vectors v', w' such that $\|B^n v'\| \to 0$ and $\|B^n w'\| \to \infty$. Indeed, if $B = SAS^{-1}$ then take $v' = Sv$ and $w' = Sw$. We have $B^n v' = S(A^n v)$, which goes to 0 because $A^n v$ does, and $B^n w' = S(A^n w)$, which goes to ∞ because $A^n w$ does. We are therefore free to replace A with a conjugate matrix throughout.

Now suppose that A has non-real eigenvalues. Then A is conjugate to a matrix of the form λR where λ is a scalar and R is a rotation matrix. However, this is impossible: if $|\lambda| \leq 1$ then w cannot exist and if $|\lambda| \geq 1$ then v cannot exist.

Next suppose that A has a repeated eigenvalue λ. If A is a scalar matrix, the reasoning in the previous paragraph applies and yields a contradiction. Otherwise, A is conjugate to

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

In fact, the reasoning in the previous paragraph still applies: if $|\lambda| \leq 1$ then w cannot exist, while if $|\lambda| \geq 1$ then v cannot exist.

We thus conclude that A has distinct real eigenvalues, and is therefore diagonalizable over the reals.

Problem 4. Suppose $a, b \in \mathbf{Q}$ and $\zeta = e^{2\pi i/3}$ is a primitive third root of unity. Let $L = \mathbf{Q}(\zeta, \sqrt[3]{a}, \sqrt[3]{b})$.

(a) Show that the field extension $L/\mathbf{Q}$ is Galois.

(b) Suppose that none of the numbers a, b, ab, ab^2 is a third power of a rational number. Show that $L/\mathbf{Q}$ has degree 18.

Solution. (a) Let K_a, K_b be the fields $\mathbf{Q}(\zeta, \sqrt[3]{a})$ and $\mathbf{Q}(\zeta, \sqrt[3]{b})$ respectively. These are the splitting fields of $x^3 - a$ and $x^3 - b$ respectively. It follows that the extensions $K_a/\mathbf{Q}$ and $K_b/\mathbf{Q}$ are Galois. Therefore, the compositum $L = K_aK_b$ is also a Galois extension over $\mathbf{Q}$.

(b) Since L is a Galois extension over $\mathbf{Q}$, it is also Galois over $\mathbf{Q}(\zeta)$. Let G be the Galois group of the extension $L/\mathbf{Q}(\zeta)$. The extensions $K_a/\mathbf{Q}(\zeta)$ and $K_b/\mathbf{Q}(\zeta)$ have degree 1 or 3, so L is an extension of degree 1, 3 or 9 of $\mathbf{Q}(\zeta)$. If L is not an extension of degree 9 then G has order at most 3 and G is cyclic. Let σ be a generator of G. We have $\sigma(\sqrt[3]{a}) = \zeta^j \sqrt[3]{a}$ and $\sigma(\sqrt[3]{b}) = \zeta^k \sqrt[3]{b}$. It is easy to verify from this that the cube root of at least one of the elements a, b, ab, ab^2 must be invariant under σ. That cube root lies in $\mathbf{Q}(\zeta) \cap \mathbf{R} = \mathbf{Q}$.

Problem 5. Let S_3 act on $V = \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2$ by permuting the tensor factors. Show that there are infinitely many subspaces W of V that are stable by S_3 (that is, $gW \subset W$ for all $g \in S_3$).

Solution. Suppose that v is an element of V. Then the span of gv, over $g \in S_3$, is clearly an S_3-stable subspace of V and has dimension at most 6. We thus see that every vector of V is contained in a proper stable subspace of V. (Note that V has dimension 8.)

Let $W_1, \ldots, W_n$ be proper stable subspaces of V. Since $\mathbf{C}$ is an infinite field, V is not the union of $W_1, \ldots, W_n$. We can therefore pick $v \in V$ not belonging to $W_1, \ldots, W_n$. Let W_{n+1} be a proper S_3-stable subspace containing v, which exists by the first paragraph. Obviously, W_{n+1} is not equal to any W_i with $1 \leq i \leq n$, since W_{n+1} contains v and the other W_i do not. Continuing in this manner, we produce an infinite number of invariant subspaces.

May 2016, Qualifying Review Algebra, Afternoon

Problem 1. Show that every group of order $224 = 2^5 \cdot 7$ has an element of order 14.

Solution. Let G be a group of order 224 and S be the set of 7-Sylow subgroups of G. The cardinality of S divides 32 and is congruent to 1 modulo 7, so it has to be 1 or 8. Let H be a 2-Sylow subgroup of G. It has 32 elements, and it acts on S by conjugation. Let $N \in S$ be a 7-Sylow subgroup, and let U be its stabilizer subgroup in H. The H-orbit of $N \in S$ has at most 8 elements, so the stabilizer U has at least $32/8 = 4$ elements. The group U normalizes N. Let $\varphi : U \to \mathrm{Aut}(N)$ be the group homomorphism associated with the conjugation action of U on N. Since $\mathrm{Aut}(N)$ has 6 elements, and the number of elements of U is divisible by 4, the group homomorphism $\varphi : U \mapsto \mathrm{Aut}(N)$ cannot be injective. We can choose a nontrivial element of order 2 in the kernel of φ. We can also choose g be a generator of N. Then h and g commute, h has order 2 and g has order 7. Then hg has order 14.

Problem 2. Suppose that A is a 6×6 complex matrix with minimum polynomial $x^6 + x^5 - x^4 - x^3$. Determine the characteristic polynomial and minimal polynomial of A^2.

Solution. Let $p(x) = x^6+x^5-x^4-x^3 = x^3(x+1)^2(x-1)$. Since the minimum polynomial has degree 6, $p(x)$ must also be the characteristic polynomial. The Jordan normal form of A has Jordan blocks $J_3(0), J_2(-1), J_1(1)$, where $J_m(\lambda)$ is the $m \times m$ Jordan block with eigenvalue λ. The Jordan normal form of $J_3(0)^2$ has blocks $J_2(0)$ and $J_1(0)$, the Jordan normal form of $J_2(-1)^2$ is $J_2(1)$ and the Jordan normal form of $J_1(1)^2$ is $J_1(1)$. The characteristic polynomial of A^2 is $x^2 \cdot x \cdot (x-1)^2 \cdot (x-1) = x^3(x-1)^3$. The minum polynomial of A^2 is the least common multiple of $x^2, x, (x-1)^2, (x-1)$, which is $x^2(x-1)^2$.

Problem 3. Suppose A and B are invertible 2×2 complex matrices.

(a) Show that there exists a linear transformation $F\colon \mathbf{C}^2 \otimes \mathbf{C}^2 \to \mathbf{C}^2 \otimes \mathbf{C}^2$ such that $F(v \otimes w) = (Av) \otimes (Bw) - (Bv) \otimes (Aw)$.

(b) Show that the rank of F is at most 2.

Solution. (a) Define a linear map $f\colon \mathbf{C}^2 \times \mathbf{C}^2 \to \mathbf{C}^2 \otimes \mathbf{C}^2$ by $f(v, w) = (Av) \otimes (Bw) - (Aw) \otimes (Bv)$. Then it is easy to verify that f is bilinear. So there exists a linear map $F\colon \mathbf{C}^2 \otimes \mathbf{C}^2 \to \mathbf{C}^2 \otimes \mathbf{C}^2$ that satisfies $F(v \otimes w) = f(v, w)$ for all $v, w \in \mathbf{C}^2$.

(b) It is clear that $F(v \otimes v)$ is an anti-symmetric tensor in $\mathbf{C}^2 \otimes \mathbf{C}^2$. The space $\bigwedge^2(\mathbf{C}^2)$ of anti-symmetric tensors has dimension 1. The subspace of $\mathbf{C}^2 \otimes \mathbf{C}^2$ spanned by pure tensors of the form $v \otimes v$ is the space $\mathrm{Sym}^2(\mathbf{C}^2)$ of symmetric tensors, which has dimension 3 (one can see this simply by taking v to be e_1, e_2, and $e_1 + e_2$, where e_1 and e_2 are a basis for $\mathbf{C}^2$). Thus F induces a map $\mathrm{Sym}^2(\mathbf{C}^2) \to \bigwedge^2(\mathbf{C}^2)$, the kernel of which has dimension at least 2. Thus the kernel of F has dimension at least 2, and so the rank of F is at most 2.

Problem 4. Let F be the field $\mathbf{C}(x_1, \ldots, x_n)$. Let S_n act on this field by permuting the variables, and let $E = F^{S_n}$ be the fixed field. Suppose that $\Phi \in E[T]$ is a polynomial of degree at most $n-1$ such that $\Phi(x_i) = \Phi(x_j)$ for all $1 \le i, j \le n$. Show that Φ is constant.

Solution. Let $a = \Phi(x_1)$, an element of F. If $\sigma \in S_n$ then $a^\sigma = \Phi(x_{\sigma(i)}) = \Phi(x_1) = a$. Thus a belongs to E, and so the polynomial $\Psi(T) = \Phi(T) - a$ still has coefficients in E. But

$\Psi(x_1) = 0$ and x_1 has degree n over E, and so $\Psi(T) = 0$, which shows that Φ is constant. (If x_1 had degree $< n$ over E then the Galois closure of $E(x_1)$ would have degree $< n!$, but the Galois closure if clearly F, which has degree $n!$.)

Problem 5. Consider the polynomial $p(x) = x^9 + 1 \in \mathbf{F}_2[x]$.

(a) Show that $p(x)$ splits over the field $\mathbf{F}_{64}$.

(b) Show that $p(x) = (x+1)(x^2+x+1)(x^6+x^3+1)$ is the irreducible factorization of p. (It is enough to show that the three factors are irreducible, you don't have to do the multiplication!)

(c) How many units does the ring $\mathbf{F}_2[x]/(p(x))$ have?

Solution. (a) $p(x)$ divides $x^{64} - x$ and $x^{64} - x$ factors over $\mathbf{F}_{64}$ into linear factors.

(b) Obviously $x+1$ is irreducible, and x^2+x+1 is irreducible because it is quadratic but does not have a root. Let α be a root of x^6+x^3+1.The Frobenius automorphism ϕ generates the Galois group of $\mathbf{F}_{64}$ over $\mathbf{F}_2$ and has order 6. Now, α is not a root of $x^4 + x$ or $x^8 + x$ because these polynomials are relatively prime to $x^6 + x^3 + 1$. Therefore, α does not lie in any proper subfield of $\mathbf{F}_{64}$. So the degree of α over $\mathbf{F}_2$ is 6 and $x^6 + x^3 + 1$ is irreducible.

(c) By the Chinese Remainder Theorem,

$$\mathbf{F}_2[x]/(p(x)) \cong \mathbf{F}_2 \times \mathbf{F}_2[x]/(x^2+x+1) \times \mathbf{F}_2[x](x^6+x^3+1) \cong \mathbf{F}_2 \times \mathbf{F}_4 \times \mathbf{F}_{64}$$

and

$$\mathbf{F}_2[x]/(p(x))^\star \cong \mathbf{F}_2^\star \times \mathbf{F}_4^\star \times \mathbf{F}_{64}^\star$$

so there are $1 \cdot (4-1) \cdot (64-1) = 3 \cdot 63 = 189$ units.