SPRING 2013 ALGEBRA COMPREHENSIVE EXAM

Problems: Choose 5.

(1) Let p be a prime number and let G be a p-group acting on a finite set S. Prove that the number of fixed points of the action is congruent to $|S|$ modulo p.

(2) Write down a complete list of all abelian groups of order 270.

(3) Let R be a Noetherian ring. Prove that a surjective homomorphism $\phi : R \to R$ must be an isomorphism.

(4) Let R be a subring of a commutative ring S, and suppose the additive group S/R is finite of order n. If m is an integer relatively prime to n, prove that R/mR and S/mS are isomorphic rings.

(5) Let q be a prime power and let $\mathbb{F}_q$ be a finite field of order q. Prove that every element of $\mathrm{GL}_2(\mathbb{F}_q)$ has order dividing either $q^2 - 1$ or $q^2 - q$.

(6) Let p be a prime number, and let $\mathbb{F}_p$ be the field with p elements. How many elements of $\mathbb{F}_p$ have cube roots in $\mathbb{F}_p$?

(7) Let V be a finite-dimensional complex vector space of dimension n and let T be a linear transformation from V to itself. Prove that $V = \ker(T^n) \oplus \mathrm{im}(T^n)$. Find an example where $V \neq \ker(T) \oplus \mathrm{im}(T)$.

Date: January 17, 2013.

Solutions.

(1) Let $s_1, \ldots, s_t$ represent the different orbits and let $F \subset S$ be the set of fixed points for the action. Then $s_i \in F$ iff $|G \cdot s_i| = 1$. Also, $|G \cdot s_i| = [G : G_{s_i}]$ divides $|G| = p^k$, so it is either 1 (if s_i is a fixed point) or a power of p (otherwise). Since the orbits partition G, we have

$$|S| = \sum_{i=1}^{t} [G : G_{s_i}] \equiv |F| \pmod{p}.$$

(2) The structure theorem for finite abelian groups says that every finite abelian group is uniquely isomorphic to a direct sum of cyclic subgroups of prime-power order. Thus the following three groups are the only abelian groups of order $270 = 2 \cdot 5 \cdot 3^3$ up to isomorphism:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{27}$$

(3) Let $I_n = \ker \phi^n$. Then since R is Noetherian, the ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ must stabilize, i.e., there exists n so that $I_n = I_{n+1}$. Let $x \in \ker(\phi)$. Since ϕ^n is surjective, there exists y such that $\phi^n(y) = x$. Then $0 = \phi(x) = \phi^{n+1}(y)$, so $y \in I_{n+1} = I_n$ which implies that $x = \phi^n(y) = 0$. Thus ϕ is injective and hence an isomorphism.

(4) Let $\phi : S/mS \to R/mR$ be multiplication by n, which is well-defined since S/R is an abelian group of order n with respect to addition. Since $(m, n) = 1$, we may choose integers a and b such that $am+bn = 1$. To see that ϕ is surjective, note that for every $r \in R$ the coset $\overline{br} \in S/mS$ maps to the coset $\bar{r} \in R/mR$, as $r = (am + bn)r = n(br) + a(mr)$. To see that ϕ is injective, suppose $\phi(\bar{s}) = 0 \in R/mR$ with $s \in S$, i.e., $ns \in mR$. Then $s = (am + bn)s = a(ms) + b(ns) \in mS$.

(5) Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$ and let f be its characteristic polynomial, which is a monic polynomial of degree 2 with coefficients in $\mathbb{F}_q$. If f has distinct roots then A is diagonalizable over either $\mathbb{F}_q$ or a quadratic extension F of $\mathbb{F}_q$. Since $|\mathbb{F}_q^*| = q - 1$ and $|F^*| = q^2 - 1$, the order of a diagonal matrix with entries in $\mathbb{F}_q$ or F divides $q^2 - 1$. If f has a repeated root a then $a \in \mathbb{F}_q$ and A is similar to a 2×2 Jordan block

$$J = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \text{ with } a \in \mathbb{F}_q^*, b \in \mathbb{F}_q.$$

If $n = q(q - 1)$ then

$$J^n = \begin{bmatrix} a^n & na^{n-1}b \\ 0 & a^n \end{bmatrix} = I$$

as desired.

(6) If $p = 2$ then the answer is 2. We may therefore suppose that p is odd. Clearly 0 always has a cube root. Since $\mathbb{F}_p^*$ is cyclic, there exists $a \in \mathbb{F}_p^*$ such that every element can be represented as a^k for some integer k. The homomorphism $\phi(x) = x^3$ from $\mathbb{F}_p^*$ can then be rewritten as $\phi(a^k) = a^{3k}$. If $(3, p-1) = 1$, i.e., if $p \equiv 2 \pmod 3$, then we see that ϕ is surjective, so all p elements of $\mathbb{F}_p$ have cube roots. If $p \equiv 1 \pmod 3$ then the image of ϕ consists of all elements of the form a^{3k} with $1 \le k \le (p-1)/3$, so there are $1+(p-1)/3 = (p+2)/3$ elements which have cube roots.

(7) Consider a basis of V in which the matrix A representing T is in Jordan canonical form. We can write $V = \oplus W_i$ where each W_i is T-invariant and the restriction of T to W_i is represented by an elementary Jordan block J_i. It therefore suffices to prove the result when $A = J_i$ is an elementary Jordan block of size $\dim W_i \le n$. If J_i corresponds to the eigenvalue zero, then $J_i^n = 0$ and thus $\ker(J_i^n) = W_i$ and $\mathrm{im}(J_i^n) = 0$. Otherwise, J_i is invertible and therefore so is J_i^n, and we have $\ker(J_i^n) = 0$ and $\mathrm{im}(J_i^n) = W_i$.

An example of T such that $V \neq \ker(T) \oplus \mathrm{im}(T)$ is as follows: for $T \in L(\mathbb{C}^2)$ given by $T(a,b) = (b,0)$, we have $\ker(T) = \mathrm{im}(T) = \mathbb{C} \oplus 0 \subset \mathbb{C}^2$.