VIGRE Algebra QR Review, September 23, 2002

Summary of Session

There was discussion of the fact that subgroups of free (in the non-abelian sense) groups are free. Solutions to some problems were presented, as follows (in some cases these were only partial solutions). The last problem, concerning polycyclic groups, is not from either of the lists: it was given on the QR exam this fall.

(9/16) 4. Find all finite groups G with at most 3 conjugacy classes.

Solution. Some related but easier problems were discussed first. The identity is always in a conjugacy class by itself: this is true precisely for the elements of the center. In particular, the number of conjugacy classes in an abelian group is equal to the number of elements in the group. Thus if a group has only one conjugacy class, it must be trivial. Second, the elements of a conjugacy class all have the same order, since conjugation by a given element is a group automorphism. Third, if a finite group has only two conjugacy classes its order can only be divisible by one prime. (There will be elements of order p for each p that divides $|G|$: if there are two distinct such primes, there will be at least three conjugacy classes). Thus, it will be a p-group with, say, p^k elements, and the two conjugacy classes must be $\{e\}$, and $G - \{e\}$ (which must consist of all elements of order p). The latter has $p^k - 1$ elements. But a conjugacy class is an orbit: its cardinality divides the order of the group, and so we must have that $(p^k - 1)|p^k$. Since $\mathrm{GCD}(p^k,\, p^k - 1) = 1$ (they differ by 1), we must have $p^k - 1 = 1$, i.e., $p^k = 2$. Thus, $|G| = 2$, and $G \cong \mathbb{Z}_2$.

We now come back to the original problem and assume that G has exactly three conjugacy classes. If G is abelian, we must have $|G| = 3$, and therefore $G \cong \mathbb{Z}_3$. We know that $|G|$ has at most two prime factors. We first consider the case where G is a p-group. Since the size of any conjugacy class divides $|G| = p^k$, the three conjugacy classes must have sizes 1, p^a, and p^b, where a and b are integers ≥ 0. Then $p^k = 1 + p^a + p^b$. If a and b are both positive we get a contradiction, since p does not divide 1, and so we may assume that $a = 0$. But then $p^k = 2 + p^b$. If $b = 0$ we get that the group is abelian (all conjugacy classes have one element) and $p^k = 3$: the group must be $\mathbb{Z}_3$, a possibility that we already discussed. If $b \neq 0$ we must have that $2|p$ and so $p = 2$. But $2^k = 2 + 2^b$ with $b < k$ forces $k = 2$, and then G has four elements and must be abelian. This not a possibility.

Finally, we consider the case where $|G| = p^r q^s$ has exactly two distinct prime factors, p and q. One of the conjugacy classes other than $\{e\}$ must contain all elements of order p; the other all elements of order q. An element of order p cannot commute with an element of order q, or their product will have order pq (one can make the same statement for any two commuting elements of relatively prime order). Consider the centralizer C of an element x of order p. We have that $C = \{g \in G : gxg^{-1} = x\}$, i.e., C is the stabilizer of x under conjugation. (Note that $gxg^{-1} = x$ if and only if $gx = xg$.) Thus, C contains only elements of order dividing p, and is a p-group. This means that the cardinality of the conjugacy class of x has the form $p^a q^s$. Similarly, the other conjugacy class must have cardinality of the form $p^r q^b$. We then have the equation $p^r q^s = 1 + p^a q^s + p^r q^b$. Since $p^a q^b$ divides all terms except 1, we must have that $a = b = 0$. This gives $p^r q^s = 1 + q^s + p^r$ or $(p^r - 1)(q^s - 1) = 2$. Thus $p^r - 1$ and $q^s - 1$ must be 1 and 2 in some order (the only factorization of 2 into two positive integers), and if follows that p^r and q^s are 2 and 3 in some order. Thus, G must be a non-abelian group of order 6, and the only such group is S_3. S_3 does have 3 conjugate elements of order 2 and 2 conjugate elements of order 3.

The bottom line is that a finite group with exactly 3 conjugacy classes must be isomorphic with $\mathbb{Z}_3$ or with S_3.

5. (9/16) Let G be a group with $|G| = 30$.

(i) Prove that either G has a normal Sylow 3-subgroup or a normal Sylow 5-subgroup.

(ii) Prove that G is isomorphic with a semidirect product of $\mathbb{Z}_{15}$ by $\mathbb{Z}_2$. (This is equivalent to showing that G has a normal subgroup that is cyclic of order 15 and a subgroup that is cyclic of order 2 meeting it only in the identity element.)

Discussion of solution. There are elements of order 2, since $2|30$, and so there is a subgroup isomorphic with $\mathbb{Z}_2$. A subgroup of order 15, if it exists, is automatically normal (any subgroup N of index 2 in a group G is normal, since the left cosets must be N and $G - N$, and this is also true of the right cosets). Any group of order 15 is abelian, and, therefore, cyclic, since it is the semi-direct product of $\mathbb{Z}_5$ by $\mathbb{Z}_3$, and $\mathbb{Z}_5$ has no non-trivial automorphism of order dividing 3. Thus, it suffices to show that there is a subgroup of order 15. (Possible suggestions: one approach is to consider the normalizer of a 5-Sylow subgroup. Recall that the normalizer of a subgroup is its stabilizer under conjugation. Thus, the index of the normalizer of a p-Sylow subgroup is the same as the number of p-Sylow subgroups. Alternatively, prove that there is either a normal subgroup N of order 3 or one of order 5, and then that G/N has a subgroup of index 2.)

(9/16) 7. Prove: a finite simple group of even order is generated by elements of order 2.

Solution. Since the order of the group is even, there are elements of order 2. Thus, the subgroup generated will not be just $\{e\}$. Since G is simple, it suffices to prove that this subgroup is normal. It consists of the identity and finite products of elements of order two (each element of order two is its own inverse). But conjugating such a product produces another such product, because conjugation is an automorphism. Q.E.D. [More generally, a subgroup is normal if and only if it is generated by a union of conjugacy classes (to prove "if," note that if we apply conjugation by g to a finite product involving elements from those classes and inverses of elements from those classes, we get another such product).]

(9/16) 9. Let I and J be ideals of a commutative ring with identity R such that $I + J = R$. Prove that for any two positive integers m, n, $I^m + J^n = R$. (The ideal I^m is generated by all products of m elements of I.)

Solution. An ideal is all of R if and only if it contains 1. Thus, we can choose $x \in I$ and $y \in J$ such that $x + y = 1$. Raise both sides to the $m + n - 1$ power (any larger integer also works). We get a sum of terms of the form $\binom{m+n-1}{i}x^i y^j$ where i, j are nonnegative integers and $i + j = m + n - 1$. We cannot have both $i \le m - 1$ and $j \le n - 1$: the sum will only be at most $m + n - 2$ in that case. Thus, in each term, either $i \ge m$ or $j \ge n$. But then all terms are either in I^m or in J^m, and so $1 \in I^m + J^n$ which implies $I^m + J^n = R$.

(9/23) 1. Determine the group with generators v_1, v_2 subject to the relations $v_1^2 = v_2^2 = 1$ and $(v_1 v_2)^3 = 1$.

Solution. We can map such a group to S_3 by sending v_1 and v_2 to any two elements of order 2: their product has order three. We shall show that the group must, in fact, be S_3.

Note that v_1 conjugates v_1v_2 to $v_1v_1v_2v_1 = v_2v_1$ (since $v_1 = v_1^{-1}$), and $(v_1v_2)(v_2v_1) = 1$, so that $v_2v_1 = (v_1v_2)^{-1}$ $(= (v_1v_2)^2)$. Thus, v_1 conjugates the subgroup H generated by v_1v_2 to itself. But v_2 does the same thing, similarly, so that the normalizer of H contains both v_1 and v_2 and therefore the entire group. Thus, it suffices to show that when we kill the normal subgroup H, which has order at most 3, we get a group of order at most 2. But once we kill H we have that $v_1v_2 = e$, so that $v_2 = v_1^{-1} = v_1$, and thus the quotient is generated by one element, v_1, which has order at most 2.

(9/23) 2. Let $x_1, \ldots, x_n$ be variables over the complex numbers $\mathbb{C}$. Let θ be a primitive nth root of unity in $\mathbb{C}$, and let G be the cyclic group of order n that it generates. Let G act on the field $F = \mathbb{C}(x_1, \ldots, x_n)$ in such a way that θ maps x_i to $\theta^i x_i$, $1 \leq i \leq n$. Determine a finite set of generators for the fixed field F^G.

Solution. We can write an element of F^G as P/Q, where P, $Q \neq 0$ are polynomials with GCD $(P, Q) = 1$. Let's call $\sum_{i=1}^n ia_i$ the *weighted degree* of the monomial $x_1^{a_1} \cdots x_n^{a_n}$. When we let θ act on P (or Q) we get a linear combination of precisely the same monomials with new coefficients. The degrees don't change. Call the new numerator P^* and the new denominator Q^*. Since $P/Q = P^*/Q^*$, $PQ^* = P^*Q$. Since $Q|PQ^*$ and GCD $(P, Q) = 1$, $Q|Q^*$. Since the degrees are the same, $Q^* = \lambda Q$ for some scalar $\lambda \neq 0$; likewise, $P^* = \mu P$ for some scalar $\mu \neq 0$, and for P/Q to be invariant we must have $\mu = \lambda$. This means that the weighted degree D of every monomial in P must be the same mod n, for each monomial is multiplied by θ^D. It also follows that every monomial in the denominator must have the same weighted degree mod n, and these must be the same mod n as for the numerator. Let d be an an integer representing this weighted degree mod n. We can divide both numerator and denominator by x_1^d. The new numerator is a $\mathbb{C}$-linear combination of terms M/x_1^d, where M is a monomial of weighted degree $\equiv d$ mod n, and the same is true for the denominator. Each of the terms M/x_1^d is itself an invariant. Thus, the field of invariants is generated by all the monomials of the form M/x_1^d, where d is congruent to the weighted degree of the numerator mod n. It was left as an exercise to complete this by showing $x_1^n, x_2/x_1^2, \ldots, x_{n-1}/x_1^{n-1}, x_n$ generate F^G.

(9/23) 3. Let G be a group and suppose that G acts (on the left) transitively on a set Ω. For each $\alpha \in \Omega$ let G_α be the stabilizer of α in G.

(a) Prove that a subgroup $H \subseteq G$ acts transitively on Ω if and only if $H \cap xG_\alpha \neq \emptyset$ for all $x \in G$.

(b) Assume that G is finite, that $|\Omega| = p^a$, where p is a positive prime integer and $a \geq 1$, and let P be a Sylow p-subgroup of G. Prove that:

(1) P acts transitively on Ω;

(2) $G = G_\alpha P = PG_\alpha$; and

(3) $G_\alpha \cap P$ is a Sylow p-subgroup of G_α.

Solution to (b). (Only part (b)(1) was discussed.) The hypotheses imply that $|G| = p^k m$ where k, m are positive integers, p does not divide m, and $k \geq a$: because the whole set is an orbit of G, its cardinality must divide $|G|$. Let $\alpha \in \Omega$. The stabilizer P_α of α in P is the same as $G_\alpha \cap P$. The index of P_α in P is the same as the length of the orbit of α in Ω, while the index of G_α in G must Ω, and so $|G_\alpha| = |G|/|\Omega| = p^{k-a}m$. Since P_α is a p-group contained in G_α, its order is a divisor of p^{k-a}. If it is a proper divisor, then the length of the orbit of α under P is greater than $p^k/p^{k-a} = p^a$, which is impossible. Thus, P_α has order precisely p^{k-a}, which says that it is a p-Sylow subgroup of G_α, and the length of the orbit of α under P is precisely p^a, which shows that P acts transitively on Ω. This does parts (1) and (3). There are many ways to do (2). For any two finite subgroups H, K of a group G, the cardinality of $HK = \{hk : h \in H, k \in K\}$ is $|H||K|/|H \cap K|$, for $h_1k_1 = h_2k_2$ if and only if there exists $j \in H \cap K$ such that $h_2 = h_1j^{-1}$ and $k_2 = jk_1$ (since the condition is equivalent to $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, and we may take j to be their common value). In this problem one then sees that PG_α and $G_\alpha P$ have the same cardinality as G.

(9/23) 5. (a) Let x and y be elements of a (non-commutative) ring R such that x and y are both nilpotent and $yx = cxy$, where c is in the center of R. Is $x + y$ necessarily nilpotent? Prove your answer.

(b) Give an example of a ring R with identity and nilpotent elements x, y in R such that $x + y$ is invertible.

Solution. (a) Suppose that $x^m = 0$ and $y^n = 0$. We claim that $(x + y)^N = 0$ where $N = n + m - 1$. Expanding by the iterated use of the distributive law produces the sum of 2^N terms, each of which is a product of N factors, where every factor is either x or y. Suppose a product has i occurrences of x and j occurrences of y, with $i + j = m + n - 1$. As in the solution of problem 9. above, either $i \geq m$ or $j \geq n$ in every product. Therefore, it suffices to show by induction on the length that any such product can be rewritten as $c^Dx^iy^j$ for a suitable power c^D of c. If the product has x on the left it can be written as xL, where L is a product of shorter length, and we can rewrite this, by the induction hypothesis, as $xc^Dx^{i-1}y^j = c^Dx^iy^j$, since c is in the center. If a product has y on the left it can be rewritten as $yL = yc^Dx^iy^{j-1} = c^D(yx^i)y^{j-1}$. By an easy induction on i, $yx^i = c^ix^iy$, $i \geq 1$, and so this is $c^Dc^ix^iyy^{j-1} = c^{D+i}x^iy^j$.

For part (b), consider a 2×2 matrix A (over any field) with a 1 in the upper left corner and 0's elsewhere, and let B be the transpose of A. Then $A^2 = B^2 = 0$ while $A + B$ is the same as a 2×2 identity matrix with its rows switched, and is its own inverse.

Additional problem. A group G is called *polycyclic* if it has a finite subnormal series $\{e\} = G_0 \subseteq \cdots \subseteq G_i \subseteq \cdots \subseteq G_n = G$ in which the factor groups G_{i+1}/G_i are all cyclic, $0 \leq i < n$. Show that subgroups and homomorphic images of polycyclic groups are polycyclic, and that a free group is polycyclic if and only if it is cyclic.

Partial solution. First note that polycyclic groups are obviously solvable, and for finite groups the two notions coincide (a finite solvable group will have a composition series with simple abelian factors, each of which must be $\mathbb{Z}_p$ for some prime p). The part discussed was that subgroups of polycyclic groups are polycyclic. Let H be a subgroup. Then the $G_i \cap H$ give a subnormal series for H with cyclic factors. Main point: if the map $G_{i+1} \twoheadrightarrow G_{i+1}/G_i$ is restricted to $G_{i+1} \cap H$, the kernel is clearly $G_i \cap H$, which shows that $G_i \cap H$ is normal in $G_{i+1} \cap H$ and that the quotient $(G_{i+1} \cap H)/(G_i \cap H)$ embeds in the cyclic group G_{i+1}/G_i, and is therefore cyclic (subgroups of cyclic groups are cyclic).