Department of Mathematics
University of Maryland
Written Graduate Qualifying Exam Solutions
Algebra (M.A. Version)
August, 2001

1. Let G be a group of order $165 = 11 \cdot 5 \cdot 3$.
   (a) Show that G has a normal subgroup N of order 11.
   (b) Show that with N as in (a), G/N is abelian, and thus that G is solvable.
   (c) Classify all groups of order 165 up to isomorphism.

Solution. (a) By the Sylow theorems, G has a subgroup N of order 11, and the number of conjugates of this subgroup divides 15 and is congruent to 1 mod 11. Hence N is normal, and G/N is a group of order 15. (b) Then G/N contains a Sylow 5-subgroup of order 5, and the number of conjugates of this subgroup divides 3 and is congruent to 1 mod 5. So the Sylow 5-subgroup of N is normal, and also central since 3 does not divide $5 - 1$. So G/N is abelian, and is necessarily isomorphic to $(\mathbb{Z}/5) \times (\mathbb{Z}/3)$ (since the Sylow subgroups are both cyclic and central). Since G is an extension of an abelian group by an abelian group, it is solvable. (c) Furthermore, the extension

$$1 \to N \to G \to G/N \to 1$$

splits. To see this, first note that a Sylow 3-subgroup of G/N lifts to a Sylow 3-subgroup of G commuting with N, since 3 does not divide $11 - 1$. So G has an abelian normal subgroup H of order 33, the inverse image in G of the Sylow 3-subgroup of G/N. Then $G/H \cong \mathbb{Z}/5$ and a Sylow 5-subgroup of G gives a semidirect product decomposition of G as $H \rtimes (\mathbb{Z}/5)$. Furthermore, since the subgroup of order 3 in H is characteristic and 5 does not divide $3 - 1$, a Sylow 5-subgroup of G centralizes the Sylow 3-subgroup of H. Hence G splits as a product $(\mathbb{Z}/3) \times (\mathbb{Z}/11 \rtimes \mathbb{Z}/5)$, for some action of a cyclic 5-group on a cyclic 11-group. It remains to understand the possible actions. Since the automorphism group of a cyclic group of prime order p is cyclic, of order $p - 1$, there is (up to changes of generators) exactly one non-trivial homomorphism from $\mathbb{Z}/5$ to the automorphism group of $\mathbb{Z}/11$. Hence there are exactly two possibilities for G up to isomorphism: $(\mathbb{Z}/11) \times (\mathbb{Z}/5) \times (\mathbb{Z}/3)$, and $(\mathbb{Z}/11 \rtimes \mathbb{Z}/5) \times (\mathbb{Z}/3)$ (non-trivial semidirect product). Since $4^5 \equiv 1 \pmod{11}$, the second of these groups has generators a, b, c, with $a^{11} = 1$, $b^5 = 1$, $c^3 = 1$, c central, and $bab^{-1} = a^4$.

2. Suppose A is a 3×3 matrix with entries in a field F of characteristic 0, and assume $\operatorname{Tr} A = 6$, $\operatorname{Tr} A^2 = 14$, and $\det A = 6$. (Tr denotes the trace.) Prove that A is similar over F to the diagonal matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Solution. Let x_1, x_2, x_3 be the roots of the characteristic polynomial of A (in some splitting field). Then the given data tells us that $x_1 + x_2 + x_3 = 6$, that $x_1^2 + x_2^2 + x_3^2 = 14$, and that $x_1 x_2 x_3 = 6$. But

$$(x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1 x_2 + x_1 x_3 + x_2 x_3),$$

so $x_1 x_2 + x_1 x_3 + x_2 x_3 = (6^2 - 14)/2 = 22/2 = 11$. (Note that we've used the assumption that F does not have characteristic 2.) So the characteristic polynomial of A is $x^3 - 6x^2 + 11x - 6$, the same as for

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

and factors as $(x-1)(x-2)(x-3)$. Since this has distinct roots (again we're using the fact that the characteristic is $\neq 2$) and the roots lie in the prime field, A is diagonalizable over F and similar to the indicated matrix.

3. You may assume the fact that the ring $R = \mathbb{Z}[\omega]$, where ω is a primitive cube root of unity, is a PID — in fact, a Euclidean ring with respect to the norm N defined by

$$N(a+b\omega) = (a+b\omega)(a+b\omega^2) = a^2 - ab + b^2.$$

Let $p \in \mathbb{Z}$ be an ordinary prime number. Show that:

(a) An element $y \in R$ is a unit in R if and only if $N(y) = 1$.

(b) p can be written in the form $a^2 - ab + b^2$, a, $b \in \mathbb{Z}$, if and only if the ideal (p) is not prime in R.

(c) The ideal (p) is not prime in R if and only if the polynomial $x^2 + x + 1$ is reducible in $\mathbb{F}_p[x]$.

Deduce that:

(d) (3) and (7) are not prime in R, but that (2) and (5) are prime in R.

Solution. (a) is a general fact about Euclidean rings: If $N(y) = 1$, then since also $N(1) = N(1^2) = N(1)N(1)$ and thus $N(1) = 1$, the division algorithm yields $1 = yz + r$ for some z, $r \in R$ with $N(r) < 1$, so $r = 0$ and y is a unit. The other direction is even easier: if y is a unit, then $1 = N(1) = N(y)N(y^{-1})$, so $N(y) = 1$.

(b) If p is irreducible in R, then (p) is prime. Otherwise p has a nontrivial factorization $p = yz$ with $N(y)$ and $N(z)$ proper divisors of $N(p)$. But $N(p) = p^2$, so this implies there is some $y = a + b\omega \in R$ with $N(y) = a^2 - ab + b^2 = p$.

(c) Note that $R = \mathbb{Z}[x]/(x^2 + x + 1)$ (since $x^2 + x + 1$ is the minimal polynomial of ω over $\mathbb{Q}$), so that $R/(p) = \mathbb{F}_p[x]/(x^2 + x + 1)$. If $x^2 + x + 1$ is irreducible in $\mathbb{F}_p[x]$, then it generates a maximal ideal, so $R/(p)$ is a field, and (p) is a prime ideal in R. But if $x^2 + x + 1$ is reducible in $\mathbb{F}_p[x]$, then $R/(p)$ is not an integral domain, and so (p) is not a prime ideal.

(d) The polynomial $f(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_p[x]$ for $p = 2$ or 5, since $f(0) = 1$, $f(1) = 3$, $f(2) = 7$, $f(3) = 13$, $f(4) = 21$, and none of these values is divisible by 2 or 5. But $f(1) \equiv 0 \pmod 3$ and $f(2) \equiv 0 \pmod 7$, so $f(x) = x^2 + x + 1$ is reducible in $\mathbb{F}_p[x]$ for $p = 3$ or 7. Now apply (c).

4. Let M be a finitely generated module over a PID, R, and suppose that for some distinct nonzero prime ideals P and Q of R, $(P^2Q^2) \cdot M = 0$. Prove that there are unique integers $p_1, p_2, q_1, q_2 \geq 0$ such that M is isomorphic to

$$(R/P)^{p_1} \oplus (R/P^2)^{p_2} \oplus (R/Q)^{q_1} \oplus (R/Q^2)^{q_2}.$$

Solution. By the structure theorem for finitely generated modules over a PID, M is a direct sum of finitely many cyclic primary modules of the form R/I^k, $k \geq 1$, with I prime. Since our M is annihilated by P^2Q^2, which is non-zero (since P and Q are non-zero), and since P and Q are relatively prime, we claim first of all that the only I's that can occur here are P and Q, and that the only k's that can occur are 1 and 2. Indeed, $I = 0$ is ruled out (since $R/(0) = R$ is not annihilated by P^2Q^2), as is any prime I different from P and Q (since then P^2Q^2 and I^k have no prime factors in common, hence are relatively prime, hence $P^2Q^2 + I^k = R$ and $(P^2Q^2) \cdot (R/I^k) = R \cdot (R/I^k) = R/I^k \neq 0$. Furthermore, any $k > 1$ is ruled out, since $(P^2Q^2) \cdot (R/P^k) = Q^2 \cdot (P^2/P^k) = P^2/P^k$ (again because $Q^2 + P^k = R$), which is non-zero if $k > 2$, and similarly with P and Q interchanged. Thus

$$M \cong (R/P)^{p_1} \oplus (R/P^2)^{p_2} \oplus (R/Q)^{q_1} \oplus (R/Q^2)^{q_2}$$

for some $p_1, p_2, q_1, q_2 \geq 0$. To show these are unique, observe that $(PQ^2) \cdot M \cong (P/P^2)^{p_2}$, a vector space of dimension p_2 over R/P, and similarly $(P^2Q) \cdot M$ is a vector space of dimension q_2 over R/Q. That shows (by invariance of dimension for a vector space) that p_2 and q_2 are uniquely determined, while we can recover $p_1 + p_2$ and $q_1 + q_2$ as the minimal number of generators of $Q^2 \cdot M$ and $P^2 \cdot M$, respectively.

5. (a) Prove that for every element g of $G = S_n$, g is conjugate in G to g^{-1}.

(b) Show that there is an element of A_4 which is **not** conjugate to its inverse.

Solution. (a) Each element of S_n has a unique representation as a product of disjoint cycles. (The uniqueness is up to the order of the factors, since they commute with one another.) Say g is a product of disjoint cycles of orders n_1, n_2, ..., i.e.,

$$g = (i_1 i_2 \dots i_{n_1})(j_1 j_2 \dots j_{n_2}) \dots .$$

Then

$$(i_1 i_{n_1})(i_2 i_{n_1-1}) \dots (j_1 j_{n_2})(j_2 j_{n_2-1}) \dots$$

is an element of order 2 conjugating g to g^{-1}.

(b) The group A_4 has a normal subgroup $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ and A_4/V_4 is cyclic of order 3. A 3-cycle in A_4, say (123), projects to a generator of A_4/V_4. Since A_4/V_4 is abelian, any conjugate of (123) projects to the **same** generator of A_4/V_4. Hence (123) is not conjugate in A_4 to its inverse (132).

6. Show that if M is an $n \times n$ matrix over $\mathbb{C}$ and if $M^2(M+1)^2 = 0$, then M is similar to a direct sum of blocks of the forms

$$(0), \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, (-1), \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Solution. Apply the argument of #4 with $R = \mathbb{C}[x]$, $P = (x)$, $Q = (x+1)$, or else use Jordan canonical form.