Department of Mathematics
University of Maryland
Written Graduate Qualifying Exam Solutions
Algebra (Ph.D. 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

$$(x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3),$$

so $x_1x_2 + x_1x_3 + x_2x_3 = (6^2 - 14)/2 = 22/2 = 11$. (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 R be a commutative ring. An R-module M if called *flat* if, for all short exact sequences

$$0 \to A \to B \to C \to 0 \tag{1}$$

of R-modules, the sequence

$$0 \to M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0 \tag{2}$$

is exact. An R-module M is called *faithfully flat* if M is flat, and if in addition, exactness of sequence (2) implies (1) is exact.

(a) Show that a free R-module is faithfully flat.

(b) Take $R = \mathbb{Z}$. Show that the R-module $\mathbb{Z}/(2)$ is not flat, and that the R-module $\mathbb{Q}$ is flat but not faithfully flat.

Solution. (a) If M is free, say on a set X, then tensoring with M is the same as taking a direct sum of copies indexed by X. So given $A \xrightarrow{\alpha} B$, $M \otimes_R A \xrightarrow{1\otimes\alpha} M \otimes_R B$ is the same as $\bigoplus_X (A \xrightarrow{\alpha} B)$. Thus one of these is injective if and only if the other one is, and M is faithfully flat.

(b) $\mathbb{Z}/(2)$ is not flat since

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/(2) \to 0$$

is exact, but when we tensor with $\mathbb{Z}/(2)$, this becomes

$$0 \to \mathbb{Z}/(2) \xrightarrow{0} \mathbb{Z}/(2) \xrightarrow{\cong} \mathbb{Z}/(2) \to 0,$$

which is not exact on the left.

To show $\mathbb{Q}$ is flat as a $\mathbb{Z}$-module, one can observe that given $x_1, \ldots, x_n \in \mathbb{Q}$, they have a "common denominator" d, and then we can write $x_i = \frac{y_i}{d}$ with $y_i \in \mathbb{Z}$, i.e., all the x_i lie in the cyclic subgroup generated by $\frac{1}{d}$. Since tensor product with anything is right exact, we only need to check exactness on the left. Suppose $a_1, \ldots, a_n \in A$ and $\alpha : A \to B$ is injective. Then

$$(1 \otimes \alpha)\big(\sum_i x_i \otimes a_i\big) = \frac{1}{d} \sum_i y_i \otimes \alpha(a_i) = \frac{1}{d} \otimes \alpha\big(\sum_i y_i a_i\big).$$

If this is 0 in the $\mathbb{Q}$-vector space $\mathbb{Q} \otimes_{\mathbb{Z}} B$, then $\alpha\big(\sum y_i a_i\big)$ is a torsion element of B, so $m \cdot \alpha\big(\sum y_i a_i\big) = 0$ for some m, i.e., $\alpha\big(\sum m y_i a_i\big) = 0$, so $\sum m y_i a_i = 0$ by injectivity of α. Then $0 = \frac{m}{d} \sum y_i a_i = m \cdot \big(\sum x_i \otimes a_i\big)$. So $\sum x_i \otimes a_i$ is a torsion element of the $\mathbb{Q}$-vector space $\mathbb{Q} \otimes_{\mathbb{Z}} A$ and so is 0. So $(1 \otimes \alpha)$ is injective.

Finally, to see that $\mathbb{Q}$ is not faithfully flat, observe that if $A = B = \mathbb{Z}/2$, the 0-map $A \to B$ is not injective, whereas $\mathbb{Q} \otimes_{\mathbb{Z}} A = \mathbb{Q} \otimes_{\mathbb{Z}} B = 0$, so $\mathbb{Q} \otimes_{\mathbb{Z}} A \xrightarrow{1 \otimes 0} \mathbb{Q} \otimes_{\mathbb{Z}} B$ is injective. Thus $\mathbb{Q}$ is not faithfully flat.

5. Let $f(x) = x^5 - 6x + 2$.
   (a) Show that f is irreducible in $\mathbb{Q}[x]$, and that in $\mathbb{C}$, it has exactly three real roots. (For the last assertion you need freshman calculus.)
   (b) Deduce that if L is the splitting field of f over $\mathbb{Q}$, $G = \operatorname{Gal}(L/\mathbb{Q})$, when identified with a subgroup of S_5, contains a 5-cycle and a 2-cycle. (Remark: This then implies that $G = S_5$, but you don't need to prove this.)

Solution. (a) Irreducibility follows by Eisenstein with $p = 2$. Now $f'(x) = 5x^4 - 6$, which is negative for $|x| < \sqrt[4]{6/5}$ and positive for $|x| > \sqrt[4]{6/5}$. So f is monotone on three intervals covering the real line, and so can have at most 3 real roots. On the other hand, it does have at least 3 real roots by the intermediate value theorem, since $f(x)$ is continuous and $f(-2) = -32 + 12 + 2 < 0$, $f(0) = 2 > 0$, $f(1) = 1 - 6 + 2 < 0$, and $f(2) = 32 - 12 + 2 > 0$. So f has exactly 3 real roots.

(b) Irreducibility implies G acts transitively on the 5 roots of f in $\mathbb{C}$. That means the order of G must be divisible by 5, so G contains an element of order 5. But every element of order 5 in S_5 is a 5-cycle. Since f has exactly two non-real roots in $\mathbb{C}$, and f has real coefficients, there is one pair of complex conjugate non-real roots, and complex conjugation gives an element of G interchanging two roots and fixing the other three, in other words, a 2-cycle.

6. Let G be a finite group and let $g \in G$.
   (a) Let $\pi : G \to M_n(\mathbb{C})$ be a representation of G and let χ_π be its character. Show that $\chi_\pi(g^{-1}) = \overline{\chi_\pi(g)}$.
   (b) Prove that g is conjugate in G to g^{-1} if and only if the following condition is satisfied: for every irreducible complex representation π of G, the character χ_π of π is real-valued on g.
   (c) Show that the condition of (b) is satisfied for all elements of S_n, and thus that all characters of S_n are real-valued.

Solution. (a) After "averaging" an inner product on $\mathbb{C}^n$ with respect to the action of G, we may assume that the action of G is unitary. Thus for each $g \in G$, $\pi(g^{-1}) = \pi(g)^{-1} = \overline{\pi(g)}^t$. Taking traces, we obtain $\chi_\pi(g^{-1}) = \overline{\chi_\pi(g)}$.

(b) If g is conjugate to g^{-1}, then for each irreducible representation π of G, we have $\chi_\pi(g) = \chi_\pi(g^{-1}) = \overline{\chi_\pi(g)}$, and thus $\chi_\pi(g)$ is real. Conversely, if $\chi_\pi(g)$ is real for all $g \in G$, then $\chi_\pi(g) = \chi_\pi(g^{-1})$ for every irreducible representation π of G. Since the irreducible representations separate conjugacy classes (by the Schur orthogonality relations), it follows that g is conjugate to g^{-1} for all $g \in G$.

(c) 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 $n_1, n_2, \ldots$, i.e.,

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

Then

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

is an element of order 2 conjugating g to g^{-1}. By (b), it follows that all characters of S_n are real-valued.