2014 Algebra SEP $\sim$ Groups Day 2 Solutions, by E. Dummit

1. (Aug-13.1): Let p be prime and V a 3-dimensional vector space over $\mathbb{Z}/p$.

   (a) Construct an explicit bijection between ordered bases of V and elements of $GL_3(\mathbb{Z}/p)$, and find the order of $GL_3(\mathbb{Z}/p)$.

   (b) Show that the kernel of the natural homomorphism from $GL_3(\mathbb{Z}/p^2)$ to $GL_3(\mathbb{Z}/p)$ is abelian of exponent p, and find the order of $GL_3(\mathbb{Z}/p^2)$.

   Solution:

   a) A bijection is: choose a fixed basis B for V, and then associate the ordered triple (v_1, v_2, v_3) to the matrix whose ijth entry is the coefficient of b_i appearing in v_j. This is a bijection because a matrix is in $GL_3(\mathbb{Z}/p)$ iff its determinant is nonzero iff its rows are linearly independent iff its rows are a basis. There are $p^3 - 1$ choices for v_1 (anything nonzero), $p^3 - p$ choices for v_2 (anything not in $\langle v_1 \rangle$), and $p^3 - p^2$ choices for v_3 (anything not in $\langle v_1, v_2 \rangle$), so the order is $(p^3 - 1)(p^3 - p)(p^3 - p^2)$.

   b) The homomorphism is simply "reduce entries modulo p", and therefore the kernel is the set of matrices of the form $I + pA$ where A is an arbitrary matrix in $M_{3\times 3}(\mathbb{Z}/p)$. Since $(I+pA)(I+pB) = I + p(A+B)$ modulo p^2, we see that the kernel's group structure is simply that of the additive group $M_{3\times 3}(\mathbb{Z}/p)$. Since this group's order is p^9, by the first isomorphism theorem we see that $\left|GL_3(\mathbb{Z}/p^2)\right| = p^9(p^3-1)(p^3-p)(p^3-p^2)$.

   Remark It is an easy exercise to extend this result to show that $|GL_k(\mathbb{Z}/p^n)| = p^{k^2(n-1)} \cdot \prod_{j=0}^{k-1}(p^k - p^j)$.

---

2. (Jan-97.3) Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree 5 that is not solvable by radicals and let S be its splitting field over $\mathbb{Q}$.

   (a) Show that there exists at most one subfield E of S such that $[E : \mathbb{Q}] = 2$.

   (b) If $\alpha, \beta \in S$ are irrational and satisfy $\alpha^2 \in \mathbb{Q}$ and $\beta^2 \in \mathbb{Q}$, show that $\alpha\beta \in \mathbb{Q}$.

   Solution:

   a) By the Galois correspondence and Abel's theorem, the Galois group of f is a non-solvable subgroup of the symmetric group S_5, whose order is $120 = 2^3 \cdot 3 \cdot 5$. Since groups of order $p^a q^b$ are solvable for primes p and q, the order of G must be divisible by at least 3 distinct primes, hence is a multiple of 30. Furthermore, a group of order pqr is solvable: if $p < q < r$ then there must be at least pq r-Sylows, at least r q-Sylows, and at least q p-Sylows, but together these contain at least $pq(r-1) + r(q-1) + q(p-1) > pqr$ distinct elements. So the only possibilities for the order are 60 and 120. Since the only subgroup of S_5 of order 60 is A_5 (else its intersection with A_5 would be have index 2 in A_5, contradicting the simplicity of A_5), we see that G is either A_5 or S_5. If $G = A_5$ then there is no quadratic subfield of E (since it would correspond to an index-2 normal subgroup of A_5), and if $G = S_5$ then there is exactly one quadratic subfield (namely, the fixed field of A_5).

   a-alt) It is a bit overkill, but another method is to prove that any non-solvable group of order 60 is isomorphic to A_5. (For this we may assume G is actually simple, because any group of smaller order is solvable.) Here is a beautiful proof of this, due to Philip Hall: G has six Sylow-5 subgroups, so the permutation action of G on them yields an injective homomorphism from G into A_6 (since G is simple). Then the permutation action of A_6 on the $|A_6| / |G| = 6$ cosets of G yields another homomorphism from G into S_6. But G stabilizes a point under this action (namely, the coset corresponding to itself), so we actually obtain a homomorphism from G into S_5, hence into A_5 since G is simple. But since $|A_5| = |G|$, this map must be an isomorphism.

   b) By part (a), α and β must lie in the same quadratic extension of $\mathbb{Q}$, say $\mathbb{Q}(\sqrt{D})$. Since their squares lie in $\mathbb{Q}$ but they do not, it must be the case that $\alpha = r\sqrt{D}$ and $\beta = s\sqrt{D}$ for some rational numbers r and s: then $\alpha\beta = rsD \in \mathbb{Q}$.

---

3. (Jan-13.1): A finite group is said to have property C if, whenever $g \in G$ and n is relatively prime to the order of g, g and g^n are conjugate in G.

   (a) Give infinitely many nonisomorphic finite groups which have property C.

   (b) Give infinitely many nonisomorphic finite groups which do not have property C.

   (c) Show that if G has property C and $\rho : G \to GL_m(\mathbb{C})$ is a homomorphism, then the trace of $\rho(g)$ lies in $\mathbb{Q}$ for every $g \in G$.

Solution:

a) The symmetric group S_k has property C: to see this recall that two permutations are conjugate in S_k if and only if they have the same cycle decomposition, and that the order of any permutation is the lcm of the lengths of its cycles. We thus observe that if n is relatively prime to the order of the permutation σ, then n is relatively prime to each of the cycle lengths in σ, and since the nth power of a k-cycle is again a k-cycle if n is relatively prime to k, we see that the cycles in σ^n have the same lengths as in σ – hence σ and σ^n are conjugate.

a-alt) The groups of the form $(\mathbb{Z}/2\mathbb{Z})^n$ have property C: every element has order 2, and so the only possible relatively prime powers of an element are itself (to which it is certainly conjugate).

b) Any abelian group that is not an elementary abelian 2-group does not have property C, since no two distinct elements are conjugate in an abelian group and every element has a power relatively prime to and strictly less than its order, unless its order is 1 or 2.

c) If g has order k, then since ρ is a representation, $\rho(g)^k = 1$, so all the eigenvalues of $\rho(g)$ are kth roots of unity. Suppose that the eigenvalue ζ, which we assume to be a primitive mth root of unity for $m|k$, occurs a_j times. Then by standard facts about cyclotomic polynomials, the Galois conjugates of ζ are ζ^j where j runs through the integers in $\{1, \cdots, m\}$ relatively prime to m. Since g and g^j are conjugate by hypothesis, we see that ζ and ζ^j occur as eigenvalues of $\rho(g)$ with equal multiplicities. Since then, again by standard properties of cyclotomic polynomials, the sum of all the primitive mth roots of unity for any m is in $\mathbb{Q}$, we see that the sum of all the eigenvalues of $\rho(g)$ is rational, since each collection of primitive mth roots of unity has rational sum.

Remark In fact, the trace of $\rho(g)$ is a sum of roots of unity, which are algebraic integers, so we see that the trace is an algebraic integer and in $\mathbb{Q}$, hence actually in $\mathbb{Z}$.

c-alt) As above, if $|g| = k$, observe that all the eigenvalues of $\rho(g)$ are kth roots of unity. If ζ_k is a primitive kth root of unity, let $\varphi_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$ be the map sending $\zeta_k \mapsto \zeta_k^a$, for a relatively prime to k. Now observe that $\varphi_a \mathrm{tr}\,\rho(g) = \mathrm{tr}\rho(g^a)$: this follows simply because the trace is additive and the eigenvalues of $\rho(g^a) = \rho(g)^a$ are the ath powers of the eigenvalues of $\rho(g)$. Then since G has property C, g and g^a are conjugate for all a relatively prime to k, so $\mathrm{tr}\,\rho(g) = \mathrm{tr}\rho(g^a)$ for such a. But this means $\mathrm{tr}\,\rho(g) \in \mathbb{Q}(\zeta_k)$ is fixed by every element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q})$, so it actually lies in $\mathbb{Q}$.

Remark The converse to part (c) is also true: if the trace of $\rho(g)$ is in $\mathbb{Q}$ for every representation ρ and $g \in G$, then G has property C. (We note that the first statement is equivalent to saying that G has a rational character table.) Since the irreducible characters form a basis for the set of class functions on G (i.e., the functions which are conjugation-invariant), we see that the function which is 1 on a given conjugacy class and 0 on the others is a linear combination of irreducible characters, so $\chi(g) = \chi(h)$ for all (irreducible) characters iff g and h are conjugate in G. The alternate solution to (c) shows that $\varphi_a\chi(g) = \chi(g^a)$, so for any $g \in G$ and a relatively prime to $|G|$, since $\chi(g) \in \mathbb{Q}$, we have $\chi(g^a) = \varphi_a\chi(g) = \chi(g)$ for all (irreducible) characters χ, whence g and g^a are conjugate.

4. (Aug-92.5): Let G be the group of 2×2 integer matrices with determinant 1, and let G act by right multiplication on the set Ω of all 1-dimensional subspaces of $\mathbb{Q}^2$.

   (a) Find all elements of G which fix every element of Ω.

   (b) Prove that G acts transitively on Ω.

Solution:

a) The answer is $\{\pm I\}$. Let $A \in G$ and let $\langle v \rangle \in \Omega$. Saying A fixes $\langle v \rangle$ is the same as saying that $Av \in \langle v \rangle$ – i.e., that v is an eigenvector of A. So if A fixes every element of Ω, then every vector in $\mathbb{Q}^2$ is an eigenvector for A, meaning that A is a scalar multiple of the identity. (Reason: if v, w are linearly independent and $Av = \lambda v$, $Aw = \delta w$, and $A(v + w) = \gamma(v + w)$ we see $(\gamma - \lambda)v + (\gamma - \delta)w = 0$, so $\gamma = \lambda = \delta$.) The only scalar multiples of the identity in G are $\pm I$.

b) We only need to show that we can map $V_0 = \{[t, 0]\}$ onto an arbitrary V_1, since if $gV_0 = V_1$ and $hV_0 = V_2$ then $hg^{-1}V_1 = V_2$. So let $v = [a, b]$ generate V_1, and rescale v to make a and b relatively prime integers; by basic properties there then exist integers s, r with $sa - rb = 1$. Now simply observe that $[1, 0] \cdot \begin{bmatrix} a & b \\ r & s \end{bmatrix} = [a, b]$, and$\begin{vmatrix} a & b \\ r & s \end{vmatrix} = sa - rb = 1$, so $A = \begin{bmatrix} a & b \\ r & s \end{bmatrix}$ sends V_0 to V_1.

---

5. (Aug-05.5): Let $G = GL_n(\mathbb{Z})$, fix a prime p, and let S be the subset of G of matrices of the form $I + pX$.

   (a) Prove that S is a subgroup of G.

   (b) Suppose $M \in S$ has prime order q. Show that $q = p$.

   (c) If $p > 2$, show that no element of S has order p. Conclude S has no nonidentity element of finite order.

Solution:

a) Clearly $(I + pX)(I + pY) = I + p(X + Y + XY)$ so S is closed under multiplication. Furthermore, if $(I + pX)(A + pY) = I$, then reducing mod p gives $A \equiv I \bmod p$, so by adjusting Y we can take $A = I$ – hence the inverse of an element of S is also in S. Since S is nonempty, we conclude it is a subgroup.

a-alt) Let $H = SL_n(\mathbb{Z}) \subset G$. Observe that reduction modulo p is a well-defined homomorphism from H to $SL_n(\mathbb{Z}/p\mathbb{Z})$. Since the kernel of this homomorphism is S, S is a subgroup of H, hence of G.

b) Suppose $(I + pX)^q = I$ with q prime. Expanding and then reducing mod p^2 yields $I + pqX \equiv I$, and this forces $q = p$.

c) Suppose $(I + p^tX)^p = I$ where X is not divisible by p and $t \geq 1$ is an integer. Expanding yields $I + p \cdot p^tX + p \cdot \frac{p-1}{2}p^{2t}X^2 + \cdots = I$, so reducing mod p^{2t+1} yields $I + p^{t+1}X \equiv I$, which is impossible since $t \geq 1$, so $p^{t+1}X$ cannot be zero mod p^{2t+1}. We conclude that S has no element of prime order for any prime, so it cannot have any nonidentity element of any finite order (since taking an appropriate power of an element of finite order will give an element of prime order).

Remark If $p = 2$, S does have an element of order p, namely $I + 2(-I) = -I$.

---

6. (Jan-91.5) Let G be a nontrivial group whose subgroups are totally ordered by inclusion: thus if H, K are subgroups, then either $H \subseteq K$ or $K \subseteq H$.

   (a) Show that G is abelian and that the orders of the elements of G are all powers of the same prime p.

   (b) If $G_n = \{g \in G : g^{p^n} = 1\}$, show that $|G_n| \le p^n$.

Solution:

a) If $x, y \in G$ then either $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle$, hence x is a power of y or y is a power of x. In particular we see that x and y commute, so G is abelian. Further, if $g \in G$ were an element of infinite order, then the subgroups generated by g^2 and g^3 would not be comparable, so every element of G has finite order. Now if $|x| = p$ and $|y| = q$ have prime order then we see that $p|q$ or $q|p$ hence $q = p$, so the only elements of prime order have order p. Finally, there cannot be elements of non-p-power order since taking an appropriate power would give an element of prime order $q \ne p$.

b) Suppose $x, y \in G$ both have order p^d for some $d \ge 1$. Then $\langle x \rangle$ and $\langle y \rangle$ have the same order and one is contained in the other, so they are equal – therefore, there is at most one cyclic subgroup of order p^d of G for any $d \ge 1$, so in particular we see G_n is finite, hence cyclic (since for any x, y we see one of $\langle x \rangle$ and $\langle y \rangle$ is contained in the other, hence $\langle x, y \rangle$ is either $\langle x \rangle$ or $\langle y \rangle$.) Then we immediately see that $|G_n| \le p^n$ since its generator has order at most p^n.

Remark In fact the analysis of part (b) shows that either $G = \mathbb{Z}/p^n\mathbb{Z}$ for some n, or $G = \mu_{p^\infty}$, the group of p-power roots of unity. If any G_n has order less than p^n, then since each G_i is cyclic we see that each G_i for $i > n$ must be equal to G_n (since each of them is cyclic and there is no element of order p^n in G) and hence $G = G_n$. If all G_n have order p^n then G is equal to the direct limit of $\mathbb{Z}/p^n\mathbb{Z}$, which is isomorphic to μ_{p^∞}.

---

7. (Aug-11.5): Let A be an additive abelian group.

   (a) If A is free abelian, show that A contains no nonzero divisible element.

   (b) Now let $A = \prod \mathbb{Z}$ be the countably infinite direct product of copies of $\mathbb{Z}$, and B be the subgroup given by the direct sum (i.e., with all but finitely many coordinates equal to 0). Prove that A/B contains a nonzero divisible element and conclude that A/B is not free abelian.

Solution:

a) Let d be a divisible element and write $d = \sum n_i b_i$ where the b_i are basis elements. Let n be a prime larger than all of the $|n_i|$; then by hypothesis there is another element $y = \sum a_i b_i$ with $d = ny$; then $d = \sum n a_i b_i = \sum n_i b_i$, so by uniqueness we see that $n a_i = n_i$. But this forces all n_i to be zero, since n_i is divisible by a prime larger than its absolute value. Hence $d = 0$.

b) We claim that the image of $x = (1!, 2!, 3!, 4!, \cdots)$ is divisible in A/B. To see this, set $y_n = (1!, 2!, \cdots, (n-1)!, 0, 0, \cdots) \in B$, and then observe that $x - y_n$ has all entries divisible by n (indeed, by $n!$), hence in A/B we see that $x + B$ can be divided by n for every n, so it is divisible. By part (a), we see immediately that A/B cannot be free abelian, since it contains a nonzero divisible element.

Remark This is a simplified portion of the proof that the direct product $\prod \mathbb{Z}$ is not a free $\mathbb{Z}$-module: the general proof requires more consideration of why (for any possible choice of basis) there exists a nonzero divisible element. The needed modification is to add ± signs to all the terms of x, and observe that the number of elements spanned by any potential basis is countable but the ± signs produce an uncountable number of divisible elements, at least one of which must therefore be nonzero.

---

8. (Aug-09.5): Let A be a multiplicative abelian group.

   (a) If A is divisible, show that any homomorphic image $\bar{A}$ of A is divisible.

   (b) If A is a finite divisible group, prove that $A = 1$.

   (c) Suppose A is divisible and $A \subseteq B$. If $A \cap X > 1$ for all nonidentity subgroups X of B, show that $A = B$.

Solution:

a) Let $\varphi(g) \in \bar{A}$ and $n \in \mathbb{N}$. By hypothesis, there exists $h \in A$ such that $h^n = g$, so $\varphi(h)^n = \varphi(g)$, hence $\varphi(g)$ is divisible.

b) Suppose $|A| = n$ and let $x \in A$ be arbitrary. By hypothesis, there exists $y \in A$ with $y^n = x$: but $y^n = 1$ by Lagrange's theorem, so $A = 1$.

b-alt) Suppose A is a finite divisible group of order greater than 1 and choose $g_1 \in A$ of prime order p (where necessarily p divides $|A|$). By divisibility, there exist elements $g_2, g_3, \cdots$ with $g_i^p = g_{i-1}$ for $i \geq 2$. We claim by induction that the order of g_i is p^i: to see this, observe $g_i^{p^i} = 1$ so the order of g_i divides p^i, but $g_i^{p^{i-1}} = g_1$, so the order does not divide p^{i-1}. But this is a contradiction, since p^i exceeds $|A|$ for large enough i.

c) First, let $g \in B$ be nontrivial and have prime order p. By applying the criterion to $X = \langle g \rangle$ we see $A \cap X$ is a nontrivial subgroup of X, which must therefore be all of X: hence $g \in A$.

Now we claim by induction on the exponent d that if g has prime power order p^d, then $g \in A$: the base case $d = 1$ is above so assume the induction hypothesis, and suppose now that g has order p^d. By the induction hypothesis, $g^p \in A$: now by divisibility there exists $h \in A$ with $h^p = g^p$, so $(gh^{-1})^p = 1$. Then gh^{-1} has order dividing p hence is in A by the above, hence $g = gh^{-1} \cdot h \in A$.

Next, any element of finite order $r = \prod p_i^{a_i}$ can be written as a product of elements of prime power order by the Chinese Remainder Theorem (namely, as a product of powers of the elements $g^{r/p_i^{a_i}}$ each of which has order $p_i^{a_i}$, and whose exponents in g are collectively coprime).

Finally, if g has infinite order, then by the assumption on A applied to $\langle g \rangle$, A contains some power g^k. Then by divisiblity there exists $h \in A$ with $h^k = g^k$, so that $(gh^{-1})^k = 1$. Since gh^{-1} has finite order, by the above it is in A; then $g = gh^{-1} \cdot h \in A$.