GU4041: Intro to Modern Algebra I

Professor Michael Harris
Solutions by Iris Rosenblum-Sellers

Homework 9

1) List the isomorphism classes of abelian groups of the following orders: 27, 200, 605, 720

Generally, the isomorphism classes of finite abelian groups of a given order are determined by the prime factorizations of the order; for a maximal prime power n such that p^n is a factor of $|G|$, and p^{n+1} is not, there are the partition function of n ways to permute the p–group components whose orders are powers of p. In practice, we permute each prime factor component individually, and mix-and-match.

27: $\mathbb{Z}_{27}, \mathbb{Z}_3 \times \mathbb{Z}_9$, and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. This one is easy, since it's a prime power; we have only one prime component to permute, so there are $p(3) = 3$ options.

200: $200 = 2^3 \times 5^2$, so we do each seperately; we should end up getting $p(3) \times p(2) = 6$ options;

$$\mathbb{Z}_{200} = \mathbb{Z}_8 \times \mathbb{Z}_{25}, \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}, \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5, \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

605: $605 = 5 \times 11^2$. There are $p(1) \times p(2)$ options, so just $\mathbb{Z}_5 \times \mathbb{Z}_{121}$, and $\mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$.

720: $720 = 5 \times 12^2$. Same deal with this one; $\mathbb{Z}_5 \times \mathbb{Z}_{144}, \mathbb{Z}_5 \times \mathbb{Z}_{12} \times \mathbb{Z}_{12}$.

2) Judson 13.3: 6,8

6: Let G be an abelian group of order m. If n divides m, prove that G has a subgroup of order n.

Proof. We first reduce to the case where $m = p^\alpha$, p prime. To do this, suppose we had shown this statement for primes. Then if we let $m = \prod p_i^{\alpha_i}$, the prime factorization of m. $n = \prod p_i^{\beta_i}$, where each $\beta_i \le \alpha_i$, because $n|m$. Then we view m as the product of n p_i-groups, which follows from the chinese remainder theorem. We call these P_i. By our assumption that the statement holds for p-groups, for each p_i-group P_i, we can pick a subgroup of P_i of order $p_i^{\beta_i}$, which we call Q_i. Then each of these Q_i's are subgroups of G, and they're *normal*, since G is abelian. Then their product, $Q_1Q_2 \dots Q_n$ is a subgroup of G. Also, since these groups have trivial overlap, and G is abelian, we have $|Q_1Q_2 \dots Q_n| = n$. This amounts to saying that for any $g_1, g_2 \in Q_i, h_1, h_2 \in Q_j . g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2, h_1 = h_2$; i.e. every tuple of elements of the Q_i's is distinct. However, we know that they have trivial overlap, since they're subgroups of trivially overlapping P_i's so $g_1g_2^{-1} = h_1h_2^{-1}$ implies that they're both the identity. So from the statement for prime powers, we have the general statement; it remains to show the statement for prime powers. We now reduce to the cyclic case similarly. Let $m = p^\alpha, n = p^\beta, \beta \le \alpha$. An abelian group of order p^α is of the form $\prod_{i=1}^n \mathbb{Z}_{p^{k_i}}$, where $\sum k_i = \alpha$. If the proposition is true for cyclic groups, we pick $j_i \le k_i : \sum j_i = \beta$, and let Q_i be subgroups of the $\mathbb{Z}_{p^{k_i}}$ of order p^{j_i}. We have the same situation as before where $Q_1Q_2 \dots Q_n$ is a subgroup of order $p^\beta = n$. It now remains to show for cyclic p-groups. Then let $G = \mathbb{Z}_{p^\alpha}$ for some α, and let $n = p^\beta$ for some $\beta \le \alpha$. Let $H := \langle [p^{\alpha-\beta}] \rangle$. We note that $[p^{\alpha-\beta}]^{p^\beta} = [p^\beta p^{\alpha-\beta}] = [p^\alpha] = [0]$, so $|H| \le p^\beta$. However, $[p^{\alpha-\beta}]^k = [0] \Rightarrow kp^{\alpha-\beta} = qp^\alpha \Rightarrow k = qp^\beta$, for some $q \in \mathbb{Z}$, so $k > 0 \Rightarrow k \ge p^\beta \Rightarrow |H| \ge p^\beta \Rightarrow |H| = p^\beta$. $\square$

8) Show that if G, H, K are finitely generated abelian groups, and $G \times H \cong G \times K$, then $H \cong K$. Give a counterexample to show that this is not true in general.

We split $G = \prod G_i$ into a unique ordered decomposition form, where G_i are cyclic, $H = \prod H_i, K = \prod K_i$ likewise. Then we have $\prod G_i \times \prod H_i \cong \prod G_i \times \prod K_i$. By uniqueness of the decompositions, we have that each component of the left is isomorphic to the same-numbered component on the right, so each H_i is isomorphic to each K_i, so the product of the H_i's, H is isomorphic to the product of the K_i's, K. Then to show the converse in general, let $G = \prod_{k=1}^{\infty} \mathbb{Z}, H = \mathbb{Z}$, and let K be trivial. $G \times H \cong G \cong G \times K$, just by the principle "$\infty + 1 = \infty$"; i.e., let $\Phi : G \times H \to G$ be defined by, if $(h, g_1, g_2, \cdots) \in H \times G, \Phi(h, g_1, g_2, \cdots) = (h, g_1, g_2, \cdots)$. This is an isomorphism. Of course, $H \ncong K$.

3) Find the smallest $n > 42$ such that there is exactly one isomorphism class of abelian groups of order n and exactly one isomorphism class of abelian groups of order $n+1$. Justify your answer, including why there is no smaller n.

We note that it is exactly equivalent for there to be exactly one isomorphism class of abelian groups of order n and for the prime factorization of n to have no multiplicities greater than 1 for a given prime, by the statement we expressed in 1 about the partition function. Then we just proceed in order from $n = 43$. 43 is prime, but $44 = 2^2 \times 7$, so that rules our both 43 and 44. $45 = 5 \times 3^2$, which rules out 45. 46, however, is 23×2, which are both multiplicity 1, and $46 + 1 = 47$ which is prime, so 46 works.

4) Let $n > 1$ and $m > 1$ be integers. In the next question, we recall that if $a \in \mathbb{Z}$ and $x \in \mathbb{Z}_n$, we can define $ax \in \mathbb{Z}_n$ by letting $\tilde{x}$ be any element of $\mathbb{Z}$ with residue class x modulo n and letting ax denote the residue class of $a\tilde{x}$ modulo n.

a) Show that if a and d are integers such that $(a, n) = (d, m) = 1$, then there is an automorphism $\alpha_{a,d} : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_n \times \mathbb{Z}_m$, such that for all $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m$, we have $\alpha_{a,d}(x, y) = (ax, dy)$.

Proof. We have the definition of α already; it suffices to show that it's an isomorphism. It is a homomorphism; we note that $\alpha_{a,d}((x_1, y_1) + (x_2, y_2)) = \alpha_{a,d}(x_1 + x_2, y_1 + y_2) = (a(x_1 + x_2), d(y_1 + y_2)) = (ax_1, dy_1) + (ax_2, dy_2) = \alpha_{a,d}(x_1, y_1) + \alpha_{a,d}(x_2, y_2)$. Then it suffices to show that it's invertible. We consider $[a] \in \mathbb{Z}_n^\times, [d] \in \mathbb{Z}_m^\times$. This is valid because they're relatively prime to n and m respectively by assumption. Then let $[b] : b \in [1, n-1] \cap \mathbb{Z}, [b] := [a]^{-1}, [c] := [d]^{-1}$ in this group. Then consider $\alpha_{b,c}$. It clearly commutes with $\alpha_{a,d}$ because multiplication does, and $\alpha_{b,c}(\alpha_{a,d})(x, y) = (abx, cdy)$. By assumption, $ab = kn + 1, cd = jm + 1$ for $k, j \in \mathbb{Z}$, so we have RHS$=(knx + x, jmy + y) \cong (x, y)$, so this is a proper inverse. Therefore, α is an automorphism. □

b) Suppose $(n, m) = 1$. Show that the group $\mathbb{Z}_{nm}$ has a unique subgroup A_n of order n and a unique subgroup A_m of order m. Write down an isomorphism $A_n \times A_m \xrightarrow{\sim} \mathbb{Z}_{nm}$

Proof. Existence is clear; let $A_n = \langle [m] \rangle, A_m = \langle [n] \rangle$. For uniqueness, we recall that any subgroup of a cyclic group is cyclic, so it suffices to show that if $|[x]| = n, x = km$ for some k, and likewise for A_m; by symmetry, it suffices to show just for n. If $|[x]| = n$, then $nx = jnm$ for some j, which implies $x = jm$. Then let $\Phi : A_n \times A_m \xrightarrow{\sim} \mathbb{Z}_{nm}$ map $([1], [0])$ to $[m]$, and $([0], [1])$ to $[n]$. We require it to be a homomorphism from here; we note that this works because $|([1], [0])| = |[m]| = n$, and likwise for m. We note that the orders of the groups agree, so it suffices to show surjectivity, for which it suffices to write an inverse of a generator of $\mathbb{Z}_{nm}$, since it's cyclic. To do this, we simply use the greatest common divisor fact $\exists x, y : xn + ym = (n, m) = 1$; then $\Phi([x], [y]) = [1]$. □

c)

Proof. Let Φ be an automorphism of $\mathbb{Z}_n \times \mathbb{Z}_m$. We recall that homomorphisms are completely determined by where they send generators, and that isomorphisms preserve orders. We note that $\Phi([1], [0]) = ([a], [0])$ for some a; to see this, we realize that if the latter component were nonzero, it would mean that $|([a],[x])| = n$, which means that $[x]^n = 0$, which means that $nx = mk$ for some k, which means that $x = m$, since $(n,m) = 1$. Likewise, $\Phi([0],[1]) = ([0],[d])$ for some d. This means that $\Phi([x],[y]) = ([ax],[dy])$. Finally, in order for Φ to preserve orders, we have to have $|[a]| = n, |[d]| = m$, which is equivalent to $(a,n) = (d,m) = 1$, so we have that $\Phi = \alpha_{a,d}$. $\square$

d)

Proof. Let $\Phi : \mathbb{Z}_3 \times \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_9$ be given by $\Phi([x],[y]) = ([x],[3x]+[y])$. This is well-defined; the only concern is in $[3x]$, since $[x]$ is defined up to equivalence mod 3. However, if $x_1 = x_2 + 3k$ for some k, we have that $[3x_1] = [3x_2 + 9k] = [3x_2]$ since we're now in mod 9. It's also a homomorphism; $\Phi(([x_1],[y_1]) + ([x_2],[y_2])) = ([x_1+x_2],[3(x_1+x_2)+y_1+y_1]) = ([x_1],[3x_1+y_1])+([x_2],[3x_2+y_2]) = \Phi([x_1],[y_1])+\Phi([x_2],[y_2])$. It's also a map from the same space to itself, so it suffices to show surjectivity. Let $([x],[y])$ in $\mathbb{Z}_3 \times \mathbb{Z}_9$. Then $\Phi([x],[y]-[3x])$, which is a well-defined element for the same reason $[3x]$ was well-defined before, is equal to $([x],[3x]+[y]-[3x]) = ([x],[y])$. $\square$

e)

Proof. The somewhat surprising answer is that it is iff (a,b) and (c,d) are linearly independent when considered as vectors over $\mathbb{Z}_3^2$, which is in fact a vector space. To see this, we note that it's always a homomorphism; $M((x_1,y_1)+(x_2,y_2)) = (a(x_1+x_2)+b(y_1+y_2), c(x_1+x_2)+d(y_1+y_2)) = (ax_1+by_1, cx_1+dy_1)+(ax_2+by_2, cx_2+dy_2) = M(x_1,y_1)+M(x_2,y_2)$. Then we can express any linear map from a vector space to itself by a square matrix; in this case, it's the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This is bijective iff it's invertible; we know from linear algebra that it's invertible iff the rows are linearly independent, so that's the correct condition. $\square$