Section 14: Finite Abelian Groups

On the third exam, you were asked to prove the following:

Prop and Def: Let G be a group and H, K be subgroups of G. Then the function $H \times K \to G : (h, k) \mapsto hk$ is an isomorphism iff

(a) for all h in H and k in K, $hk = kh$,

(b) $HK = G$, and

(c) $H \cap K = \{e\}$.

In this case, G is the *internal direct product* of H and K.

It follows by induction that, for any finite abelian group G, $G \cong G(p_1) \times G(p_2) \times \cdots \times G(p_r)$, where the p_i's are the primes that divide $|G|$ and $G(p)$ denotes the set of elements g of G for which $o(g)$ is a power of p. Our present goal is to show that G is a(n internal) direct product of cyclic groups of orders powers of primes, and by what we have just seen, it is enough to prove that, if every element of G is a power of the same prime p, then G is a direct product of cyclic groups of orders powers of p.

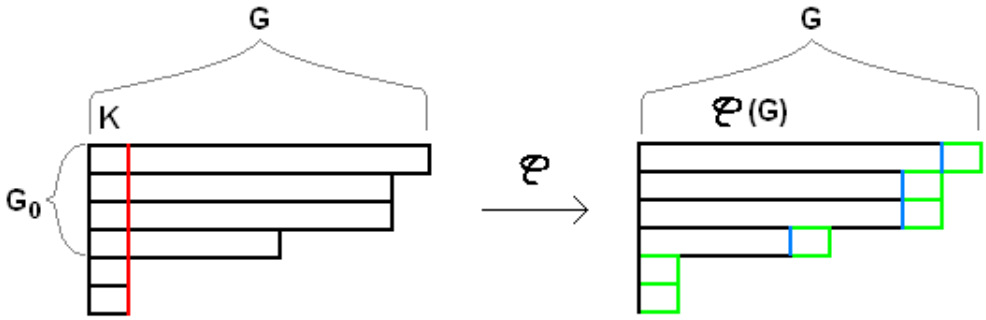
Lemma: Let G be a finite abelian group in which every element has order the prime p or 1. Then for each x in G and any subgroup H for which $H \cap \langle x \rangle = \{e\}$, there is a subgroup M of G containing H for which G is the internal direct product of $\langle x \rangle$ and M.

Pf: If $x = e$, set $M = G$. Otherwise, among the subgroups of G containing H that intersect $\langle x \rangle$ in $\{e\}$, pick one, M, that is as large as possible, i.e., if $M \subset M'$, then $M' \cap \langle x \rangle \neq \{e\}$ (and hence $= \langle x \rangle$, because $\langle x \rangle$ has no other subgroups). If $\langle x \rangle M = G$, then we are done, so assume by way of contradiction that $\langle x \rangle M \neq G$. Then there is an element y of $G - \langle x \rangle M$. But then, because $M \subset \langle y \rangle M$, by the choice of M we have $\langle x \rangle \cap \langle y \rangle M = \langle x \rangle$. Thus, $x = y^k m$ for some m in M and k in $\mathbb{Z}$. In fact, because $M \cap \langle x \rangle = \{e\}$, k can't be a multiple of p, so y^k is a generator of $\langle y \rangle$, say $y = (y^k)^r$, and we can write $y = (xm^{-1})^r = x^r m^{-r} \in \langle x \rangle M$, the desired contradiction. //

Now let G be a finite abelian group in which every element has order a power of the prime p. We proceed by induction on the highest order p^r of an element of G. If $r = 1$, we are done by repeated use of the lemma. So assume it is true for all orders less than p^r. Consider the homomorphism $\varphi : G \to G : x \to x^p$. Then $\varphi(G)$ consists of the p-th powers of elements of G, so all its elements have order a power of p less than the r-th, so by the induction hypothesis, $\varphi(G)$ is an internal direct product

$$\varphi(G) = \langle h_1 \rangle \times \cdots \times \langle h_n \rangle$$

where $o(h_i)$ is a power of p less than p^r. Note that, in the kernel K of φ, and in the factor group $G/\varphi(G)$, every element has order p or 1. Pick g_i in G for which $g_i^p = h_i$, and set $G_0 = \langle g_1 \rangle \ldots \langle g_n \rangle$, so that $\varphi(G) \subseteq G_0$. Then we can check that $G_0 \cong \langle g_1 \rangle \times \cdots \times \langle g_n \rangle$.



It remains to show that $G \cong \langle x_1\rangle \times \cdots \times \langle x_k\rangle \times G_0$ where $x_i \in K$: If $K \subseteq G_0$, then $G_0 = \varphi^{-1}(\varphi(G_0)) = \varphi^{-1}(\varphi(G)) = G$ and we are done. Otherwise, take x_1 from $K - G_0$; then in $G/\varphi(G)$, we have $\langle x_1\varphi(G)\rangle \cap G_0/\varphi(G) = \{e\varphi(G)\}$. By the lemma, there is a subgroup $\overline{G_1}$ of $G/\varphi(G)$ containing $G_0/\varphi(G)$ such that $G/\varphi(G) \cong \langle x_1\varphi(G)\rangle \times \overline{G_1}$; set $G_1 = \varphi^{-1}(\overline{G_1})$, so that $\varphi(G) \subseteq G_1$. Because $x_1\varphi(G) \notin \overline{G_1}$ and $\langle x_1\rangle$ has only two subgroups, $\langle x_1\rangle \cap G_1 = \{e\}$, so $G \cong \langle x_1\rangle \times G_1$. We have $\varphi(G_1) = \varphi(G)$ and the kernel of the restriction of φ to G_1 is $K \cap G_1$. The argument above shows that if we choose x_2 from $(K \cap G_1) - G_0$, we can find a subgroup G_2 of G_1 for which $G_1 \cong \langle x_2\rangle \times G_2$. We continue until $K \cap G_k \subseteq G_0$. This completes the proof.

Structure Theorem for Finite Abelian Groups: A finite abelian group of order n is, up to isomorphism, a product of cyclic groups. The cyclic groups may have prime power orders, or they may have orders $d_1, d_2, \ldots, d_{k-1}, d_k$ where $d_k | d_{k-1} | \ldots | d_2 | d_1$; these are called the *invariants* of the group. The list of prime powers or the invariants uniquely determine the group up to isomorphism.

The uniqueness up to isomorphism can be inferred by counting numbers of elements of various orders. For example, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 8 elements of order 4 (anything with 1 or 3 as the first coordinate), while $\mathbb{Z}_4 \times \mathbb{Z}_4$ has 12 (anything with 1 or 3 as either coordinate).

The decomposition into groups of prime power orders comes right out of the proof: Write G as the product of its $G(p)$'s, and then write each $G(p)$ as a product of cyclics of prime power orders. We show by an example how to get the decomposition into factors whose orders are the invariants (having the divisibility property). Suppose

$$\begin{array}{rcccccccccc} G & \cong & & \mathbb{Z}_8 & \times & \mathbb{Z}_8 & \times & \mathbb{Z}_4 & \times & \mathbb{Z}_2 & \times & \mathbb{Z}_2 \\ & & \times & \mathbb{Z}_{27} & \times & \mathbb{Z}_3 & \times & \mathbb{Z}_3 & & & & \\ & & \times & \mathbb{Z}_5 & \times & \mathbb{Z}_5 & . & & & & & \end{array}$$

Group together into a single product the first terms in each row, and the second terms into a product, and so on. Because the orders in different rows are relatively prime, each of these subproducts is cyclic:

$$\begin{array}{rcl} \mathbb{Z}_8 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 & \cong & \mathbb{Z}_{1080} \\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 & \cong & \mathbb{Z}_{120} \\ \mathbb{Z}_4 \times \mathbb{Z}_3 & \cong & \mathbb{Z}_{12} \\ \mathbb{Z}_2 & \cong & \mathbb{Z}_2 \\ \mathbb{Z}_2 & \cong & \mathbb{Z}_2 \\ \mathbb{Z}_{1080} \times \mathbb{Z}_{120} \times \mathbb{Z}_{12} \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \cong & G \end{array}$$

and $2|2|12|120|1080$.

Cor: If G is a finite abelian group and d is a factor of $|G|$, then G has a subgroup of order d.

Section 15: Sylow Theorems

For nonabelian groups, we don't get such a nice description of all the groups of a given order. But the three theorems proved by the Norwegian mathematician Sylow are often helpful.

Def: Let p be a prime integer. A (sub)group (of a group) is a *p-(sub)group* iff every element has order a power of p. If G is any finite group and p^n divides $|G|$ but p^{n+1} doesn't, then a subgroup of G of order p^n is a *Sylow p-subgroup* of G.

Sylow's First Theorem: Let G be a finite group and p a prime that divides $|G|$.

(i) If p^k divides $|G|$, then G has a subgroup of order p^k. In particular, G has a Sylow p-subgroup.

(ii) If K is a p-subgroup of G and H is a Sylow p-subgroup, then K is contained in a conjugate of H (which is also a Sylow p-subgroup of G).

Sylow's Second Theorem: All Sylow p-subgroups of a finite group are conjugate. Thus, a Sylow p-subgroup is normal iff it is the only Sylow p-subgroup.

Sylow's Third Theorem: Suppose G is a finite group and p^n is the highest power of the prime P that divides $|G|$. Then the number of Sylow p-subgroups in G divides $|G|/p^n$ (and hence also $|G|$) and is congruent to 1 mod p.

Proof of Sylow's First Theorem (i): First we prove that every finite group with order divisible by p has a Sylow p-subgroup: Induction on $|G|$. Assume that every finite group with fewer than $|G|$ elements has a Sylow p-subgroup. If some proper subgroup H of G has order divisible by the same power of p, say p^n, as G, then by the induction hypothesis, H has a subgroup of order p^n, which is a Sylow p-subgroup of G. If no proper subgroup has order divisible by p^n, then the index in G of every proper subgroup is divisible by p, so every term in the class equation except $|Z(G)|$ is divisible by p; so $|Z(G)|$ is also divisible by p. Now by the Structure Theorem for Finite Abelian Groups, $Z(G)$ has a subgroup A of order p, and $A \triangleleft G$. By the induction hypothesis, G/A has a Sylow p-subgroup $\overline{K}$, which has order p^{n-1}. The preimage K in G of $\overline{K}$ in G/A has order p^n.

Now to find p-subgroups of G with p^k elements where $k < n$, by looking inside any Sylow p-subgroup of G, we may assume that G has order a power of p, and use induction again: We saw using the class equation that $Z(G) \neq \{e\}$, so we can find x of order p in $Z(G)$. By the induction hypothesis $G/\langle x \rangle$ has a subgroup of order p^{k-1}, and its preimage in G has order p^k. //

Basic setup for the rest of the proofs: Let G be a finite group, let p^n be the highest power of p that divides $|G|$, and let $\mathcal{X}$ be the set of Sylow p-subgroups of G, i.e., the set of subgroups with p^n elements. Then we get an equivalence relation on $\mathcal{X}$, given by:

$$H_1 \mathcal{R} H_2 \text{ iff there is an element } g \text{ of } G \text{ for which } H_2 = gH_1g^{-1}.$$

The $\mathcal{R}$-equivalence classes are called the *G-orbits* in $\mathcal{X}$. By reasoning similar to the one used on conjugation of elements in the proof of the class equation, the number of elements in the G-orbit of a Sylow p-subgroup H is $[G : N(H)]$, where $N(H) = \{g \in G : gHg^{-1} = H\}$, the *normalizer* of H. Because $H \subseteq N(H)$, the number of elements in the G-orbit of H divides $|G|/p^n$, relatively prime to p, but a factor of $|G|$. Moreover, for any subgroup K of G, there is a corresponding equivalence relation: Two Sylow p-subgroups of G (not K) are equivalent iff they are conjugate by an element of K. This gives a "finer" partition of $\mathcal{X}$: Each G-orbit is a union of some K-orbits. And the number of elements in the K-orbit of H is $[K : K \cap N(H)]$, which divides $|K|$.

Proof of Sylow's First Theorem (ii): For K as in (ii), note that the number of elements in each K-orbit is a power of p, but the K-orbits whose union is the G-orbit containing H add up to a factor of $|G|/p^n$, which is not divisible by p; so at least one of these K-orbits has only $p^0 = 1$ element. Thus, $K \subseteq N(H')$ for an H' in the G-orbit containing H. But $H' \triangleleft N(H')$, and $|N(H')/H'| = [N(H') : H']$ divides $[G : H'] = |G|/p^n$, so $|N(H')/H'|$ is not divisible by p. For k in K, the element $H'k$ of $N(H')/H'$ has order both a power of p (because k does) and not divisible by p (because it divides $|N(H')/H'|$), so the order is 1, i.e., $k \in H'$. Thus $K \subseteq H'$, and H' is a (G-)conjugate of H. //

Proof of Sylow's Second Theorem: The assertion that any two Sylow p-subgroups are conjugate follows from (ii) of the First Theorem. (So in fact there is only one G-orbit in $\mathcal{X}$, namely, the whole set $\mathcal{X}$.) The second assertion is then clear. //

Proof of Sylow's Third Theorem: We have already seen that the number of elements in the G-orbit $\mathcal{X}$ divides $|G|/p^n$. To see that it is congruent to 1 mod p, let H be one of the Sylow p-subgroups of G. Then the H-orbits in $\mathcal{X}$ all have cardinalities that are powers of p, and the H-orbit containing H has only one element — conjugating H by elements of itself just gives itself. If H' is a Sylow p-subgroup different from H, then $H \not\subseteq N(H')$ (for otherwise, as we saw in the proof of part (ii) of the First Theorem, $H \subseteq H'$ and hence $H = H'$). So H' has more than one H-conjugate, and hence its H-orbit has cardinality a power of p greater than 1. Thus, the cardinality of the G-orbit $\mathcal{X}$ is the sum of 1 and powers of p greater than 1, so it is congruent to 1 mod p. //

The rest of Section 15 in the text includes a wonderful list of results showing how the Sylow theorems can put limits on the non-isomorphic groups of a given order. We present below a construction that allows us to build certain groups of given orders, so that, if a certain group is not ruled out as possible by the Sylow theorems, we can sometimes actually build one. For example, one result in the text is:

Cor: If the order of a finite group is the product of two primes $p < q$, and p does not divide $q - 1$, then the group is cyclic.

Pf: The group G must have a Sylow p-subgroup H and a Sylow q-subgroup K, both cyclic because they are of prime order. Now the number of Sylow q-subgroups divides p and is congruent to 1 mod q; because $p < q$, K must be the only Sylow q-subgroup. Let x be a generator of H. Then conjugation by x is an element of $\mathrm{Aut}(K)$ whose order divides both $o(x) = p$ and $|\mathrm{Aut}(K)| = |U(\mathbb{Z}_q)| = q - 1$; and by hypothesis, the only possible order of this conjugation is 1, i.e., it is the identity. So $xkx^{-1} = k$ for all k in K. It follows that all the elements of H commute with all the elements of K, and hence that G is the internal direct product of its cyclic subgroups H, K, which have relatively prime orders; so G is cyclic. //

But suppose that p does divide $q - 1$; must there be a non-cyclic group of that order? If $p = 2$, then we know that the group D_q is a non-cyclic, in fact non-abelian, example. But in general, if p divides $q - 1$, can we always find a non-cyclic — in fact, preferably a non-abelian — group of order pq? It turns out that the answer is yes. The first step is to show that $U(\mathbb{Z}_q)$ is cyclic when q is prime; and this fact requires a bit more proof that I want to put here. But it follows that we can find a homomorphism from $\mathbb{Z}_p$ into $U(\mathbb{Z}_q) \cong \mathrm{Aut}(\mathbb{Z}_q)$, by sending 1 to an automorphism of $\mathbb{Z}_q$ of order p. We can then complete the proof by using the following construction.

Construction: Suppose we have two groups, G and H, and a homomorphism $\varphi : G \to \mathrm{Aut}(H)$

— so that, for any g in G, $\varphi(g)$ is an automorphism of H. To minimize parentheses, we will denote $\varphi(g)$ by φ_g. Then we can define a new operation $*$ on the set $G \times H$, given by

$$(a, p) * (b, q) = (ab, \varphi_b(p)q) \ .$$

With this operation, the set $G \times H$ is denoted $G \times_\varphi H$ and called the *semidirect product* of G and H by φ. You can check that $*$ is an associative operation, that (e_G, e_H) acts as an identity, that the inverse of (a, p) is $(a^{-1}, \varphi_a^{-1}(p^{-1})$, that the functions

$$G \to G \times_\varphi H : g \mapsto (g, e_H) \qquad , \qquad H \to G \times_\varphi H : h \mapsto (e_G, H)$$

are group homomorphisms, that the image of the second is a normal subgroup of $G \times_\varphi H$, and that conjugating an (e_G, h) by an (g, e_H) gives $(e_G, \varphi_g(h))$.

If φ is the trivial homomorphism $G \to \mathrm{Aut}(H)$, sending every element to the identity function on H, the semidirect product is just the ordinary direct product $G \times H$.

Applications: (1) If q is an odd prime, then $q - 1$ is an element of $U(\mathbb{Z}_q)$ (which is isomorphic to $\mathrm{Aut}(\mathbb{Z}_q)$) of (multiplicative) order 2, so there is a homomorphism $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_q)$ given by: 0 goes to the identity automorphism φ_0 on $\mathbb{Z}_q$, and 1 goes to the automorphism φ_1 given by $a \mapsto (q-1)a$. The semidirect product of $\mathbb{Z}_2$ and $\mathbb{Z}_q$ with the homomorphism $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_q)$ is (isomorphic to) D_q: $\langle f \rangle$ is cyclic of order q and normal, and conjugation by g is an automorphism of $\langle f \rangle$ of order 2.

(2) Because 7 divides $29 - 1$, we should be able to construct a non-abelian group of order $7 \cdot 29 = 203$: The group $U(\mathbb{Z}_{29})$ is cyclic of order 28, so there must be elements of order 7. By trial and error, we find that an element in $U(\mathbb{Z}_{29})$ of (multiplicative) order 7 is 16. (So is 7, but I don't want to use the same number in two contexts if I can avoid it.) Thus, a homomorphism $\varphi : \mathbb{Z}_7 \to \mathrm{Aut}(\mathbb{Z}_{29})$ determined by taking 1 to the automorphism φ_1 of $\mathbb{Z}_{29}$ given by $a \mapsto 16a$. The desired group is the semidirect product $\mathbb{Z}_7 \times_\varphi \mathbb{Z}_{29}$.

(3) I constructed the group used on Exam 3 as a semidirect product: Reversing the coordinates is an automorphism of $\mathbb{Z}_3 \times \mathbb{Z}_3$ that is its own inverse, so there is a natural homomorphism from $\mathbb{Z}_2$ into $\mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$, taking 1 to this automorphism. We get a semidirect product of $\mathbb{Z}_2$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. Then I simplified the notation: a for $(0, (1, 0))$, b for $(0, (0, 1))$ and k for $(1, (0, 0))$.)