Math 417 Group Theory Second Exam

Things we (will) have talked about since the first exam

(but don't forget the things covered before the first exam!)

Normal subgroups. The integers mod n can be viewed either as having elements $\{0, 1, \ldots, n-1\}$, or the elements are equivalence classes of integers, where $a \sim b$ if $n|b-a$. In the latter case, we add elements by adding representatives of equivalence classes (and then need to show that the resulting 'element' is independent of the choices made). This notion can be generalized:

For G a group and $H \leq G$ a subgroup, defining a multiplication on (left) cosets by $(aH)(bH) = (ab)H$ requires, to be well-defined, that $a_1H = a_2H$ and $b_1H = b_2H$ implies $(a_1b_1)H = (a_2b_2)H$. That is, we need $a_1^{-1}a_2, b_1^{-1}b_2 \in H$ implies $(a_1b_1)^{-1}(a_2b_2) = b_1^{-1}(a_1^{-1}a^2)b_1(b_1^{-1}b_2)$ is in H. This then requires $b_1^{-1}(a_1^{-1}a^2)b_1 = b_1^{-1}hb_1 \in H$ for every $b_1 \in G$ and $h \in H$. So we define:

$H \leq G$ is a *normal* subgroup of G if $g^{-1}Hg = \{g^{-1}hg \ : \ h \in H\} = H$ for every $g \in G$.

Then the multiplication above makes the set of (left) cosets $G/H = \{gH \ : \ g \in G\}$ a group. $H = e_GH$ is the identity element, and $(gH)^{-1} = g^{-1}H$. The order of G/H is the number of cosets of H in G, i.e., the index $[G : H]$ of H in G. We use $H \triangleleft G$ to denote "H is normal in G". We call G/H the quotient of G by H.

Alternate view: $g^{-1}Hg = H$ means $Hg = gH$, i.e., the left and right cosets of H in G coincide.

Examples: $A_n \triangleleft S_n$; a conjugate of an even permutation is even.

$Z(G) \triangleleft G$, for any group G; $h \in Z(G)$ implies $g^{-1}hg = h \in Z(G)$.

In a dihedral group D_n = symmetries of a regular n-gon, the set of rotations forms a normal subgroup; a conjugate of a rotation is a rotation.

$SL(n, \mathbb{Z}) \triangleleft GL(n, \mathbb{Z})$, $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$, and $SL(n, \mathbb{Z}_m) \triangleleft GL(n, \mathbb{Z}_m)$.

In an abelian group, every subgroup is normal.

Inverse images: If $\varphi : G \to H$ is a homomorphism, and $K \leq H$, then $\varphi^{-1}(K) = \{g \in G \ : \varphi(g) \in H\}$ is a subgroup of G, the *inverse image* of K under φ. If, in addition, $K \triangleleft H$, then $\varphi^{-1}(K) \triangleleft G$.

In particular, $\{e_H\} \triangleleft H$, so $\varphi^{-1}(\{e_H\}) = \ker(\varphi) =$ the *kernel* of φ is a normal subgroup of G. If $H \triangleleft G$, then $\varphi : G \to G/H$ given by $g \mapsto gH$ is a (surjective) homomorphism. Then $\varphi^{-1}(\{e_{G/H}\}) = H$. So every normal subgroup occcurs as the kernel of a homomorphism.

On the other hand, the image of a normal subgroup need not be normal! But it is, if the homomorphism is surjective.

First Isomorphism Theorem. If $\varphi : G \to H$ is a surjective homomorphism, then, setting $K = \ker(\varphi)$, we find that $aK = bK$ implies $\varphi(a) = \varphi(b)$, and so there is a well-defined ('induced') function $\overline{\varphi} : G/K \to H$, which is a bijective homomorphism, i.e., an isomorphism. In general, replacing H wwith $\varphi(G)$ to make it surjective, we find that $\overline{\varphi} : G/\ker(\varphi) \to \varphi(G)$ is an isomorphism. So the image of φ is isomorphic to a quotient of G.

An abelian-ness criterion: if $G/Z(G)$ is cyclic, then G is abelian (and then $G/Z(G) = 1$ (!)).

The homomorphism $G \to \mathrm{Aut}(G)$ given by $g \mapsto \varphi_g$, where $\varphi_g(x) = gxg^{-1}$ has image $\mathrm{Inn}(G)$ = the *inner* automorphisms of G, and kernel $Z(G)$, and so $G/Z(G) \cong \mathrm{Inn}(G)$.

If $H \leq G$, then G acts (by left multiplication) on the (left) cosets of H in G; if $[G : H] = n$, we can think of this as permutations of n elements, i.e., S_n, so this gives a homomorphism $G \to S_n$. The kernel N is then normal in G, and $g \in N \Leftrightarrow gaH = aH$ for all a, so $gH = H$

i.e, $g \in H$, so $N \leq H$. Moreover, $G/N \cong$ subgroup of S_n, so $[G:N] = |G/N|$ divides $|S_n| = n!$. So every subgroup of index n contains a normal subgroup of index dividing $n!$.

In particular, if $[G:H] = 2$, then $H \triangleleft G$. In general, $N = \cap_{g \in G} g^{-1}Hg =$ the intersection of all of the conjugates of H in G.

Direct products/direct sums. We can 'glue' groups together as, essentially Cartesian products: If G, H are groups, then $G \times H$, with multiplication $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ is a group. When we use this multiplication, we denote the group by $G \oplus H =$ the *direct sum* of the groups G and H.

Examples: vector spaces! We use coordinate-wise addition.

$|G \oplus H| = |G| \cdot |H|$; If G and H are abelian then $G \oplus H$ is abelian.

If $A \leq G$ and $B \leq H$, then $A \oplus B \leq G \oplus H$. But not all subgroups arise this way!

$Z(G \oplus H) = Z(G) \oplus Z(H)$

If $\varphi : G \to H_1$ and $\psi : G \to H_2$ are homomorphisms, then we can build a homomorphism $\varphi \oplus \psi : G \to H_1 \oplus H_2$ by $(\varphi \oplus \psi)(g) = (\varphi(g), \psi(g))$. The kernel of this is $\ker(\varphi) \cap \ker(\psi)$.

So, e.g, the homomorphism $\mathbb{Z}_{21} \to \mathbb{Z}_3 \oplus \mathbb{Z}_7$ given by (x mod $21 \mapsto$ (x mod $3, x$ mod 7) is injective, hence bijective (by the pigeonhole principle), hence an isomorphism! [All that was really required was that 3 and 7 are relatively prime; the generalization to more factors is, essentially, the Chinese Remainder Theorem.]

The same map gives a homomorphism $\mathbb{Z}_{21}^* \to \mathbb{Z}_3^* \oplus \mathbb{Z}_7^*$, which is still a bijection, giving an isomorphism!

In general, if you have a collection $\varphi_i : G \to H_i$ of homomorphisms that can 'separate elements', i.e. if $x \neq y$ then there is an i so that $\varphi_i(x) \neq \varphi_i(y)$, then $\oplus_i \varphi_i : G \to \oplus_i H_i$ is injective, so G is isomorphic to a subgroup of $\oplus_i H_i$.

An application of this: if $|G| = p^2$ for some prime p, then G is abelian. In fact, either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Group-based (public key) cryptography.

Sending secret messages: The basic idea is that we assume that your enemy (= 'Eve' = 'evesdropper') can see anything you transmit. So a message must be encoded by you ('Alice') (think: as a sequence of 0's and 1's) in such a way that only the intended recipient ('Bob') can decode it. Typically, this is done by converting the message in a standard way into 0's and 1's, and then add (in $\oplus_i \mathbb{Z}_2$!) a fixed sequence that both Alice and Bob know to the message. Adding the string (= a 'key') the first time encrypts the message; adding it to the encrypted message decrypts the message (since $(x + y) + y = x$ in $\mathbb{Z}_2$).

The difficult part: how do Alice and Bob go about agreeing on a key? Back in the day this was done by physically sending a list of daily keys; modern cryptography does this by exchanging in public information that allows Alice and Bob to construct a secret key.

Diffie-Hellman: The first (1970's) public key key-exchange system used $\mathbb{Z}_p^*$ for p a (large) prime. The idea is that, as we have seen, $\mathbb{Z}_p^*$ is a cyclic group, and so has a generator some $P \in \mathbb{Z}_p^*$. Alice and Bob agree on a p and P, and then each chooses a (secret) exponent n_A, n_B and transmit to one another $\alpha_A = P^{n_A}$ mod p (to Bob) and $\alpha_B = P^{n_B}$ mod p (to Alice). Both then have the information to compute $P^{n_A n_B} = [P^{n_A}]^{n_B} = \alpha_A^{n_B} = [P^{n_B}]^{n_A} = \alpha_B^{n_A}$ (Bob can compute the first version, Alice can compute the second). They then use this as the basis (takes its representation mod 2 ?) for an encryption string.

The point to this is that Eve has 'only' seen p, P, α_A, and α_B. She knows that $\alpha_A = P^{n_A}$ mod p (and there is only one n_A between 0 and $p - 1$ that works), but does not know n_A.

The point is that the function $n \mapsto P^n \bmod p$ is (we think!) what is known as a *one-way function*: it is very efficient to compute (using, in this case, successive squaring [compute $P^{2^i} \bmod p$] and the base 2 representation of n_A), but it is very diffiicult to invert: knowing $P^{n_A} \bmod p$, find n_A (in this case, this is called the *discrete logarithm problem*). And (we think!) there is no way to compute $P^{n_A n_B} \bmod p$, from the public information, without first recovering either n_A or n_B. This is considered secure enough (for p large enough!) that it is routinely used to protect banking information, your cellphone conversations, and internet commerce generally.

Ko-Lee-Cha-Han-Cheon: Recently (since 2000), key exchange systems have been devised that rely on the non-abelian-ness of groups. The first of these begins with a group G containing two subgroups $A, B \leq G$ so that for any $a \in A$ and $b \in B$, we have $ab = ba$. Then starting with an agreed upon $g \in G$, Alice picks an $a \in A$ and sends Bob $\alpha = aga^{-1}$, and Bob picks a $b \in B$ and sends Alice $\beta = bgb^{-1}$ then $\gamma = (ab)g(ab)^{-1} = a(bgb^{-1})a^{-1} = a\beta a^{-1}$ is something that Alice can compute; but $\gamma = (ab)g(ab)^{-1} = (ba)g(ba)^{-1} = b(aga^{-1})b^{-1} = b\alpha b^{-1}$ can also be computed by Bob. This is their shared secret key.

Example: $G = GL(n+m, \mathbb{Z}_p)$, $A =$ the block diagonal matrices with an $m \times m$ identity matrix in the lower-right corner, and $B =$ the block diagonal matrices with an $n \times n$ identity matrix in the upper-left corner. Matrices chosen one from each always commute!. If you want to 'hide' this block diagonal structure, pick a matrix x at random and use the conjugate subgroups xAx^{-1} and xBx^{-1}, instead; xax^{-1} and xbx^{-1} will still commute!

In this system, the enemy/evesdropper Eve knows G, g, α, and β. To build the key, (we think!) Eve must, from g and $\alpha = aga^{-1}$, recover $a \in A$ (this is not quite true; see below). This is called the *conjugacy search problem*: knowing $g \in G$ and that $h = xgx^{-1}$ for some x, find x ! Unlike the discrete log, which has been (relatively) well-studied, not much is known about how difficult we should expect conjugacy search to be. In some groups (abelian groups!) it is utterly trivial; in others, like $GL(n, \mathbb{Z}_k)$ it can be quite quick; $B = XAX^{-1}$ means (*) $BX = XA$ for some known matrices A, B and an unknown matrix X. But (*) is really a system of n^2 linear equations in the entries of X, which we can solve using ('just') linear algebra....

It turns out, you do not really need to solve conjugacy search to 'break' Ko-Lee. It is enough, given g and $x = aga^{-1}$, to find $a_1, a_2 \in A$ so that $x = a_1 g a_2$ (we don't need $a_2 = a_1^{-1}$). [Some people call this the *decomposition search problem.*] This is because if you know $aga^{-1} = a_1 g a_2$ and $bgb^{-1} = b_1 g b_2$ then you can compute $(ab)g(ab)^{-1} = a_1 b_1 g a_2 b_2$, since elements of A and B commute. Whether or not decomposition is 'easier' than conjugacy isn't clear...

Anshel-Anshel-Goldfeld: A different cryptosystem which relies on non-ablelian-ness uses *commutators* $xyx^{-1}y^{-1}$ instead. In this system, we start with a group G and (finite) subsets $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ of G. Alice chooses a secret word (i.e., product) $\alpha = a_{i_1} \cdots a_{i_k}$ of elements of A and sends to Bob the group elements $\alpha_1 = \alpha b_1 \alpha^{-1}$, $\ldots$, $\alpha_m = \alpha b_m \alpha^{-1}$. Bob chooses a secret word $\beta = b_{j_1} \cdots b_{j_\ell}$ built fro B, and sends the elements $\beta_1 = \beta a_1 \beta^{-1}, \ldots, \beta_n = \beta a_n \beta^{-1}$. Their shared secret is the commutator $\alpha\beta\alpha^{-1}\beta^{-1}$. Bob can compute this as $\alpha(b_{j_1} \cdots b_{j_\ell} \alpha^{-1}\beta^{-1} = (\alpha b_{j_1} \alpha^{-1}) \cdots (\alpha b_{j_\ell} \alpha^{-1})\beta^{-1} = \alpha_{j_1} \cdots \alpha_{j_\ell} \beta^{-1}$, using information he has and Alice sent, since he knows <u>how</u> he built β. Alice can compute this as $\alpha\beta(a_{i_k}^{-1} \cdots a_{i_1}^{-1})\beta^{-1} = \alpha\beta_{i_k}^{-1} \cdots \beta_{i_1}^{-1}$ from information she has and Bob sent. (They both need to know how to invert elements in G....)

This system allows for more groups G to be used; we don't need to know how to find commuting subgroups. The security of the system rests on the *simultaneous conjugacy search problem*

(SCSP): given a list $(a_1, xa_1x^{-1}), \dots, (a_n, xa_nx^{-1})$ of pairs of elements of G and the knowledge that one element conjugates the first entries to the second, find x ! Again, we think that recovering the commutator $\alpha\beta\alpha^{-1}\beta^{-1}$ generally requires you to solve SCSP for one of the two lists; and (we think!) there are groups in which SCSP is 'hard'.

For both of these systems, much of the security rests on choosing the right group G. Such groups are called *platform groups*, and the study of which groups are good or bad for this purpose is the subject of ongoing research. Most such groups are finite (as an aid to computation). Which makes the next subject of interest!

Sylow Theory. Work carried out in the 1870's highlighted how knowledge of certain subgroups of a (finite) group G can help us understand questions like "what are all of the groups of a given order n?". This has come to be known as *Sylow theory* (after its discoverer). It starts with

Proposition: If G is a finite abelian group and p is a prime which divides $|G|$, then there is an element $x \in G$ with order p. [The proof consists of picking an element $y \in G$; if p divides $|y|$ then a power of y will work; otherwise we build an inductive argument and use the (inductive) hypothesis that $G/\langle y \rangle$ has an element of order p to find an $x \in G$ with $x\langle y \rangle$ of order p and show that a power of this x has order p.]

A key ingredient to understanding finite groups is the *class equation*, which come from studying conjugation in a group, as an action of G on itself. Specifically, the homomorphism $G \to \mathrm{Aut}(G)$ given by $g \mapsto \varphi_g$, where $\varphi_g(x) = gxg^{-1}$ [so $\varphi_{gh} = \varphi_g \circ \varphi_h$] gives an action, and the orbit of $x \in G$, $\mathrm{orb}_G(x) = \{gxg^{-1} \ : \ g \in G\}$ is the *conjugacy class* $\mathrm{cl}(x)$ of x in G. The stabilizer of x, $\mathrm{stab}_G(x) = \{g \in G \ : \ gxg^{-1} = x\} = \{g \in G \ : \ gx = xg\} = C_G(x)$ is the centralizer of x in G. The orbit-stabilizer theorem then tells us that $|G| = |\mathrm{cl}(x)| \cdot |\mathrm{stab}_G(x)|$, and so $|\mathrm{cl}(x)| = [G : C_G(x)]$ (which then divides $|G|$). $|\mathrm{cl}(x)| = 1$ precisely when $x \in Z(G)$. If we choose one representative for each conjugacy class of size > 1, then noting then G is partitioned into disjoint conjugacy classes, we find that

$|G| = |Z(G)| + \Sigma[G : C_G(x)]$, where the sum is taken over the $\mathrm{cl}(x)$ of size > 1 (and so each $[G : C_G(x)] > 1$).

This is the *class equation*. It is a fundamental result for counting things in a group. For example:

Proposition: If $|G| = p^k$ for some prime p, then $|Z(G)| > 1$; every group of prime-power order has non-trivial center. [This is because in the class equation every $[G : C_G(x)] > 1$ divides p^k and so is a multiple of p. Therefore $|Z(G)|$ is a multiple of p.]

If $H \leq G$, then G acts (by conjugation) on the conjugates $\mathscr{H} = \{gHg^{-1} \ : \ g \in G\}$ of H in G, and the orbit-stabilizer theorem again tells us that, noting that $\mathrm{stab}_G(H) = \{g \in G \ : \ gHg^{-1} = H\} = N_G(H) =$ the <u>normalizer</u> of H in G, we have $|\mathscr{H}| = [G : N_G(H)|$ divides $[G : H]$ (and hence divides $|G|$).

Sylow theory focuses on subgroups (and elements) of G whose orders are a power of a given prime p. [Such (sub)groups are call *p-groups*.]

(First) Theorem: If G is a finite group, p is prime, and p^k divides $|G|$, then G contains a subgroup H with $|H| = p^k$. [The proof is again an induction on $|G|$; either p^k divides one of the $C_G(x)$ (which are proper subgroups, when $|\mathrm{cl}(x)| > 1$), letting us find H in $C_G(H)$, or p divides $|Z(G)|$. Then we can find an $x \in Z(G)$ of order p and use induction on $G/\langle x \rangle$, to find a subgroup H of order p^{k-1}. Then $\varphi^{-1}(H)$, where $\varphi : G \to G/\langle x \rangle$, has order p^k.

Corollary: If p is prime and p divides $|G|$, then there is an element of G of order p.

A *p-Sylow subgroup* of G is a subgroup H with $|H| = p^k$ and $|G|/p^k$ is relatively prime to p. The first theorem tells us that, for every prime p, G has a p-Sylow subgroup. The remaining theorems tell us about these subgroups.

(Second) Theorem: Every subgroup K of G of order p^k is contained in a p-Sylow subgroup. [In fact, given a p-Sylow subgroup H, K acts in the conjugates $\mathscr{H}$ of H, and an orbit-stabilizer argument, using that $|\mathscr{H}|$ is relatively prime to p, shows that K fixes one of the elements H_i of $\mathscr{H}$, which in turn implies that $K \leq H_i$.]

An immediate consequence of (the proof of) the second theorem is that the p-Sylow subgroups of G are all conjugate (one is contained in, hence equal to, a conjugate of the other).

(Third) Theorem: The number $|\mathscr{H}|$ of p-Sylow subgroups of G is congruent to 1 mod p, and divides $[G:H]$. [This comes from a more careful count of the orbits of H under conjugation, when $|H| = p^k$ and $[G:H]$ is relatively prime to p.]

Taken together, these results provide a powerful tool for understanding the structure of a group, based (almost) solely on its order. For example:

A group of order $35 = 5 \cdot 7$ has (cyclic) Sylow subgroups of order 5 and 7, and $|\mathscr{H}_5| = |\mathscr{H}_7| = 1$, i.e, both are normal (their normalizers are both G). Then G/H_5 and G/H_7 are both (cyclic) groups, and the 'natural' homomorphism $G \to G/H_5 \oplus G/H_7$ is injective (the kernel is $H_5 \cap H_7 = \{e_G\}$), and therefore, since both groups have order 35, is surjective. So G is isomorphic to a direct sum of groups of order 7 and 5, i.e., to $\mathbb{Z}_7 \oplus \mathbb{Z}_5$ (which is turn is $\cong \mathbb{Z}_{35}$). So every group of order 35 is cyclic.

A group of order $225 = 3^2 \cdot 5^2$ has Sylow subgroups of order 9 and 25. $|\mathscr{H}_3|$ divides 25 and is 1 mod 3, and so is either 1 (and so H_3 is normal) or 25. $|\mathscr{H}_5|$ divides 9 and is 1 mod 5, and so is equal to 1 (and so H_5 is normal). If $H_3 \lhd G$, then as above we can build an isomorphism $G \to G/H_3 \oplus G/H_5$. But $|G/H_3| = 25 = 5^2$, and $|G/H_5| = 9 = 3^2$, and so both quotients are abelian and so G is abelian, and is isomorphic to a direct sum of one of $\mathbb{Z}_{25}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ with one of $\mathbb{Z}_9$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_3$. On the other hand, if $|\mathscr{H}_3| = 25$, then since $H_5 \lhd G$ we have that H_3 acts in H_5 by conjugation, yielding a homomorphism $H_3 \to \mathrm{Aut}(H_5)$. But $textrmAut(H_5)$ is either $\mathbb{Z}_{25}^*$ (if $H_5 = \mathbb{Z}_{25}$), which has order 20, or $GL(2, \mathbb{Z}_5)$ (if $H_5 = \mathbb{Z}_5 \oplus \mathbb{Z}_5$), which has order 480. But the only homomorphism $H_3 \to \mathbb{Z}_{25}^*$ is trivial, so in this case elements of H_3 commute with elements of H_5, and so G is abelian. In the other case, there are homomorphisms $H_3 \to GL(2, \mathbb{Z}_5)$; by Sylow theory (!), there are elements of order 3 in $GL(2, \mathbb{Z}_5)$ to map to. In this case conjugation will be non-trivial, and so G will be non-abelian.

In this last case, we can say still more. Since $H_5 \lhd G$, the product set $H_5H_3 = \{hk : h \in H_5, k \in H_3\}$ is a subgroup of G, and multiplication in this subgroup looks like $(h_1k_1)(h_2k_2) = (h_1[k_1h_2k_1^{-1}])(k_1k_2)$, where $k_1h_2k_1^{-1} \in H_5$ since H_5 is normal. Furthermore, $H_5H_3 = G$, since the map $H_5 \times H_3 \to H_5H_3$ is injective ($h_1k_1 = h_2k_2$ means $h_2^{-1}h_1 = k_2k_1^{-1} \in H_5 \cap H_3 = \{e_G\}$), and hence maps onto G. So the group multiplication is 'determined' by how H_3 conjugates elements of H_5, i.e., by the homomorphism $H_3 \to \mathrm{Aut}(H_5)$.

This last situation occurs often enough that this construction is given a name. If G and H are groups, and $\varphi : H \to \mathrm{Aut}(G)$ is a homomorphism, then $M = G \times H$, with multiplication $(g_1, h_1)(g_2, h_2) = (g_1 \cdot [\varphi(h_1)](g_2), h_2h_2)$ is a group, and $G \times \{e_H\}$ is (check!) a normal subgroup of M. Such a group is called a *semidirect product* of G and H, and is denoted $G \rtimes H$. So what we were finding above is that in the last case(s), G is isomorphic to $H_5 \rtimes H_3$.

A final example: if $|G| = 3 \cdot 17 \cdot 23 = 1173$, then $|\mathscr{H}_3|$ is 1 or $17 \cdot 23 = 391$, $|\mathscr{H}_{17}|$ is 1 or 69, and $|\mathscr{H}_23|$ is 1. But if $|\mathscr{H}_3| = 391$, then there are 391 distinct subgroups of order 3, and so (since pairs intersect only in e_G) G has 782 elements of order 3. And if $|\mathscr{H}_{17}| = 69$, then G

has $69 \cdot 16 = 1051$ elements of order 17. But a group of order 1173 can't do that (there are then at least $782 + 1051 = 1833$ elements...). So at least one of H_3 and H_{17} (in addition to H_23) must be normal. In fact, applying arugments like the first example to G/H_3 or G/H_{17} and G/H_23 implies that two of these are abelian, which forces G to be abelian, so both H_3 and H_{17} are normal!

These kind of techniques can, with work, typically enable us to identify all of the groups with a given (small...) order.

The Fundamental Theorem of Finite Abelian Groups. Our work with Sylow theory tells us that if G is abelian and $|G| = p_1^{k_1} \cdots p_n^{k_n}$ is the prime factorization of $|G|$, then G has (Sylow) subgroups H_i of orders $p_i^{k_i}$. Since G is abelian, these subgroups are normal, and, in fact, the map $H_1 \oplus \cdots \oplus H_n \to G$ sending $(h_1, \dots h_n) \mapsto h_1 \cdots h_n$ is a homomorphism (since G is abelian) and injective, and so is an isomorphism. To completely classify the finite ablelian groups, it is then enough to do so for groups of prime-power order. This we can do:

Theorem: If G is an abelian group and $|G| = p^k$ for some prime p, then $G \cong \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_m}}$ for some numbers $k_1 \geq \cdots \geq k_n$ and $k_1 + \cdots + k_n = k$.

This is proved, as with most of our other results of this type, by induction on k. We pick the element x with largest possible order p^{k_1}, and then build the quotient group $H = G/\langle x \rangle$ and (by induction) an isomorphism $\mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_m}} \to H$. When can then 'lift' this map to a map to G, and then build a homomorphism $\langle x \rangle \oplus (\mathbb{Z}_{p^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_m}}) \to G$, which we can then show is an isomorphism! To build the 'lift' thhe fact that x has largest possible order plays a key role....

Shuffling cards. We can use our understanding of group theory to analyse problems which appear to have little to do with groups. For example, a deck of cards (with an even number $2n$ of cards) can be 'perfectly' shuffled in two ways by splitting the deck into two stacks of n and interleaving them in one of two ways. These can be represented by two permutations of $2n$ letters:

$$\begin{pmatrix} 1 & 2 & \cdots & 25 & 26 & 27 & 28 & \cdots & 51 & 52 \\ 1 & 3 & \cdots & 49 & 51 & 2 & 4 & \cdots & 50 & 52 \end{pmatrix} \quad \text{and}$$

$$\begin{pmatrix} 1 & 2 & \cdots & 25 & 26 & 27 & 28 & \cdots & 51 & 52 \\ 2 & 4 & \cdots & 50 & 52 & 1 & 3 & \cdots & 49 & 51 \end{pmatrix}$$

The first is an *outshuffle*, and the second is an *inshuffle*. A basic question to ask (these live in the finite group S_{52} is: what is the order of these permutations? How many perfect shuffles will return the deck to its original position? By thinking of these differently, we can find the answer. For the outshuffle, dropping the first and last (fixed) numbers and shifting by 1, and then thinking modulo 51, the permutation T_0 becomes T:

$$\begin{pmatrix} 1 & 2 & \cdots & 24 & 25 & 26 & 27 & \cdots & 49 & 50 \\ 2 & 4 & \cdots & 48 & 50 & 1 & 3 & \cdots & 47 & 49 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & 24 & 25 & 26 & 27 & \cdots & 49 & 50 \\ 2 & 4 & \cdots & 48 & 50 & 52 & 54 & \cdots & 98 & 100 \end{pmatrix}$$

This is the 'permutation' "multiply by 2, and then reduce modulo 51". That is, $T(k) = 2k$ mod 51 . So $T^n(k) = 2^n \cdot k$ mod 51, and so $T^n(k) = k$ for all k precisely when $2^n \equiv 1$ mod 51. SO the order of the outshuffle is the order of 2 in $\mathbb{Z}_{51}^*$! Which happens to be 8; so 8 outshuffles will return a deck to its original position. [Note that this also tells us the orbit of every k under successive multiplication by T; most have orbits of size 8 (when k is not (one more than) a multiple of 17, while $T_0(18) = 35$ and $T_0(35) = 18$.

For the inshufffle, thinking modulo 53, it is

$$\begin{pmatrix} 1 & 2 & \cdots & 25 & 26 & 27 & 28 & \cdots & 51 & 52 \\ 2 & 4 & \cdots & 50 & 52 & 54 & 56 & \cdots & 102 & 104 \end{pmatrix}$$

and so it <u>is</u> multiplication by 2 modulo 53; $N(k) = 2k \bmod 53$. So the order of N is the order of 2 in $\mathbb{Z}^*_{53}$, which is 52. In fact, $N^m(k) = K$ for the first time when $m = 52$, for all k, so N is a 52-cycle!

This kind of analysis works the same for deck of any (even) size $2n$; the outshuffle is (ignoring the outer two cards) multiplication by 2 modulo $2n - 1$, and the inshuffle is multiplication by 2 modulo $2n + 1$, and so the order of the permutations are thhe orders of 2 in $\mathbb{Z}^*_{2n-1}$ and $\mathbb{Z}^*_{2n+1}$, respectively.

... and something we will probably run out of time before reaching....

Wallpaper groups. Our first encounter with groups was as the symmetries of some object. Returning to that theme, we can introduce 'structures' on the plane in the form of *tilings*: a tile is (essentially) a polygon or collection of polygons, and a tiling is a way to cover the plane by copies of the tiles, overlapping only along their edges. Many familiar tilings can be found all around us; squares, equilateral triangles, regular hexagons, and even <u>any</u> single quadrilateral can tile the plane. We also saw how a pentagon (with two right angles, shaped like a 'house') can tile the plane. A *wallpaper group* (or *tiling group*, or *crystallographic group*) is the group of symmetries of a tiling, that is, the group of rigid motions of the plane that carries each tile of a tiling to another tile of the <u>same</u> tiling. For the tilings described above, these groups contain translations, reflections, glide reflections, and rotations.

A fundamental result, that was observed by crystallographers, is:

Theorem: If a wallpaper group G contains a non-trivial translation, then every rotation in G has order either 2, 3, 4, or 6.

The proof uses the Law of Cosines!