Math 417 – Twelfth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 21, 2020

There is a lot of material in section 9 of the book on cycles and permutations, and section 10 on cosets, and I think we've covered most of it already.

One topic I'm going to mention but not have on homework or exams is the idea of even and odd permutations. This is based on counting transpositions, and the "real" proof of it requires matrices. Since linear algebra isn't a prerequisite, I can't give the full proof, but I'd like to sketch it anyway.

A *transposition* is a permutation $\pi \in S_n$ with the property that $\pi(k) = k$ for $n-2$ of the elements in $\{1, \ldots, n\}$, and for $i \neq j$, $\pi(i) = j$ and $\pi(j) = i$. Examples include the μ_j's in S_3. The cycle representation for π consists of the cycle (ij), and everything else a singleton. For example, with $n = 5$,

$$\pi_5 = \begin{pmatrix} 12345 \\ 15342 \end{pmatrix} = (25) = (25)(1)(3)(4),$$

Two comments on notation. Since (i) doesn't do anything, we often don't write it. Also, Fraleigh puts commas in his cycles. I don't.

I mentioned in passing a few days ago that any cycle can be written as a product of transpositions: if the x_i's are all different, then

$$(x_1 x_n)(x_1 x_{n-1}) \cdots (x_1 x_3)(x_1 x_2) = (x_1 x_2 x_3 \cdots x_{n-1} x_n)$$

But there are many ways to write permutations as products. For example,

$$(12)(13)(14)(13) = (12)(34).$$

We call a permutation an *even* permutation if it is a product of an even number of transpositions and an *odd* permutation if it is a product of an odd number of transpositions.

The obvious and crucial question would be: is this well-defined? Could you write the same permutation as a product of an even number of transpositions and as a product of an odd number of transpositions? The answer is no, and there are two proofs in the book. What I'll give you is the most fundamental proof; this is "culture".

The *permutation matrix* M_π associated to $\pi \in S_n$ is an $n \times n$ matrix $[a_{ij}]$ so that $a_{ij} = 1$ if $j = \pi(i)$ and $a_{ij} = 0$ otherwise. For example, for the D_4 element $\mu_1 = (12)(34)$,

$$M_{\mu_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

I won't go into details, but if you define $G = \{M_\pi, \pi \in S_n\}$ with the operation of matrix multiplication, you get a group, and $\Phi(\pi) = M_\pi$ defines an isomorphism. Big deal, right?

But here's the thing. If you know row reduction, you can very easily persuade yourself that the determinant $\det(M_\pi)$ is always equal to ± 1.

If you know matrices, $\det(M_1 M_2) = \det(M_1)\det(M_2)$ is basic. It is not hard to show that if τ is a transposition, then $\det(M_\tau) = -1$. Thus if π is a product of k transpositions, then $\det(M_\pi) = (-1)^k$.

So an alternative definition of an even permutation π is one for which $\det(M_\pi) = 1$, and an odd permutation π is one for which $\det(M_\pi) = -1$.

There is an important subgroup of S_n, for $n \geq 2$, called the *alternating subgroup* A_n and consisting of the even permutations in S_n: $|A_n| = n!/2$.

As noted in the book, A_4 is a group of order 12, and even though $6 \mid 12$, A_4 does not have a subgroup of order 6. Thus, Lagrange's Theorem can't be an iff statement.

I'd like to move onto a new topic which we've seen instances of. Suppose $(G, *_G)$ and $(H, *_H)$ are both groups. They might even be the same, it doesn't matter. They can be finite or infinite, abelian or not abelian. We define the *direct product* as follows: the elements come from a Cartesian product

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

and we define the operation $*_{G\times H}$ in the simplest way possible: if $g_i \in G$ and $h_i \in H$, then

$$(g_1, h_1) *_{G\times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

THEOREM Using the definitions given above, $G \times H$ is a group.

PROOF What do we have to prove? First that the operation is a binary operation. But if $(g_1, h_1), (g_2, h_2) \in G \times H$, then
$g_1, g_2 \in G \implies g_1 *_G g_2 \in G$, because G is a group, and
$h_1, h_2 \in H \implies h_1 *_H h_2 \in H$, so the product is in $G \times H$.

Next there is the identity, but G and H are groups, so they have identity elements e_G and e_H, and so for every $(g, h) \in G \times H$,

$$(g, h) *_{G\times H} (e_G, e_H) = (g *_G e_G, h *_H e_h)$$
$$= (g, h) = (e_G, e_H) *_{G\times H} (g, h).$$

Inverses are handled the same way: suppose $g \in G, h \in H$, then there exist $g^{-1} \in G, h^{-1} \in H$ and

$$(g, h) *_{G\times H} (g^{-1}, h^{-1}) = (g *_G g^{-1}, h *_H eh^{-1})$$
$$= (e_G, e_H) = e_{G\times H}.$$

Finally, associativity is verified for each component separately, since G and H are themselves associative.

$$((g_1, h_1) *_{G\times H} (g_2, h_2)) *_{G\times H} (g_3, h_3) =$$
$$(g_1 *_G g_2, h_1 *_H h_2) *_{G\times H} (g_3, h_3) =$$
$$((g_1 *_G g_2) *_G g_3, (h_1 *_H h_2) *_H h_3)$$
$$= (g_1 *_G (g_2 *_G g_3), h_1 *_H (h_2 *_H h_3))$$
$$= (g_1, h_1) *_{G\times H} ((g_2, h_2) *_{G\times H} (g_3, h_3)).$$

So this is a group. If G and H are both finite groups, then $|G \times H| = |G| \cdot |H|$; if they are both abelian, then so is $G \times H$.

We can generalize this and consider the direct product $G_1 \times G_2 \times \cdots \times G_s$ in exactly the same way. Yes, it's associative. We won't talk about this except at the end of class today.

What about subgroups?

THEOREM If $G_1 < G$ and $H_1 < H$, then

$$\{(g, h) \ : \ g \in G_1, h \in H_1\}$$

is a subgroup of $G \times H$. (It is customarily called $G_1 \times H_1$.)

PROOF The proof is simple. We have the same operation as before, and for $g_1, g_2 \in G_1$ and $h_1, h_2 \in H_1$

$$(g_1, h_1) *_{G \times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2).$$

Since G_1 is a subgroup, $g_1 *_G g_2 \in G_1$; since H_1 is a subgroup, $h_1 *_H h_2 \in H_1$, so $G_1 \times H_1$ closed under the operation.

Also, $e_G \in G_1$ and $e_H \in H_1$ so $(e_G, e_H) = e_{G\times H} \in G_1 \times H_1$, and $(g^{-1}, h^{-1}) \in G_1 \times H_1$, so we've satisfied all the criteria, and $G_1 \times H_1$ is a subgroup. Is it the only kind of subgroup?

Time for some examples. It is not hard to show that $G \times \{e\}$ and $\{e\} \times G$ are both isomorphic to G, so they are not interesting.

The smallest nontrivial group is C_2. What happens if we take $G \times H$, when G and H are each cyclic groups of order 2? It is a group of order $2 \times 2 = 4$, so we should know it.

Let's be more specific and overly careful with notation. Look at

$$\{e_G, a\} \times \{e_H, b\}$$

where $a *_G a = e_G$ and $b *_H b = e_H$. So there are four elements

$$\{(e_G, e_H), (a, e_H), (e_G, b), (a, b)\}$$

Multiplication is by component: for example

$$(a, e_H) *_{G\times H} (a, b) = (a *_G a, e_H *_H b) = (e_G, b).$$

We can finish the multiplication table, and I think you'll recognize it.

$G \times H$	(e_G, e_H)	(a, e_H)	(e_G, b)	(a, b)
(e_G, e_H)	(e_G, e_H)	(a, e_H)	(e_G, b)	(a, b)
(a, e_H)	(a, e_H)	(e_G, e_H)	(a, b)	(e_G, b)
(e_G, b)	(e_G, b)	(a, b)	(e_G, e_H)	(a, e_H)
(a, b)	(a, b)	(e_G, b)	(a, e_H)	(e_G, e_H)

Yes, this is V, in its true colors as $C_2 \times C_2$. Let's look at the subgroups. Since G and H are cyclic groups of order 2, they have no proper subgroups, so the subgroups of G are $\{e_G\}$ and $\{e_G, a\}$ and the subgroups of H are $\{e_H\}$ and $\{e_H, a\}$.

This gives four subgroups of $G \times H$

$$\{(e_G, e_H)\}, \{(e_G, e_H), (a, e_H)\}, \{(e_G, e_H), (e_G, b)\}, G \times H.$$

To make this more familiar, let's apply the isomorphism to V which takes

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto X, (e_G, b) \mapsto Y, (a, b) \mapsto Z.$$

Then the four subgroups are $\{I\}$, $\{I, X\}$,$\{I, Y\}$. $\{I, X, Y, Z\}$.

One subgroup is missing: $\{I, Z\}$ or $\{(e_G, e_H), (a, b)\}$. This is a subgroup which does not come from a product of subgroups of G and H.

We've seen other instances of this: $(\mathbb{Z}/m\mathbb{Z}, \oplus) \times (\mathbb{Z}/n\mathbb{Z}, \oplus)$, when $m = 2$ and $n = 3, 4$. You looked at some subgroups of these too.

I wanted to finish with two nice theorems about the direct product of cyclic groups, which show the deep connection with number theory.

THEOREM If $gcd(m, n) = 1$, then $C_m \times C_n$ is isomorphic to C_{mn}.

Two remarks: when $m = n = 2$, the condition fails ($gcd(2, 2) = 2$) and $C_2 \times C_2$ is isomorphic to V, which is *not* isomorphic to C_4.

We have seen that $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/3\mathbb{Z}, \oplus)$ has an element of order 6, and so is isomorphic to C_6, which is isomorphic to $(\mathbb{Z}/6\mathbb{Z}, \oplus)$.

We need a lemma which we might have done already, but is worth repeating:

LEMMA If $gcd(m, n) = 1$, then $lcm(m, n) = mn$: if $m \mid t$ and $n \mid t$, then $mn \mid t$.

PROOF Suppose $m \mid t$, then we can write $t = ma$ for some $a \in \mathbb{Z}$. But now we have $n \mid ma$, and since $gcd(m, n) = 1$, one of our first results was that this implies that $n \mid a$, so $a = nb$ for some $b \in \mathbb{Z}$, Putting this together,

$$t = ma = mnb$$

That is, $mn \mid t$. □

PROOF OF THEOREM Let's write

$$G = C_m = \langle a \rangle = \{e_G, a, a^2, \ldots, a^{m-1}\}, \quad a^m = e_G,$$
$$H = C_n = \langle b \rangle = \{e_H, b, b^2, \ldots, b^{n-1}\}, \quad b^n = e_H.$$

The elements of $C_m \times C_n$ are $\{(a^j, b^k)\}$, with j taken mod m and k taken mod n, and the combined operation is clear:

$$(a^j, b^k)(a^r, b^s) = (a^{j+r}, b^{k+s}).$$

It follows that the powers of (a, b) are straightforward:

$$(a, b)^t = (a^t, b^t).$$

What is the order of (a, b)?

$$(a, b)^t = e_{G\times H} \iff (a^t, b^t) = (e_G, e_H)$$
$$\iff a^t = e_G, b^t = e_H \iff m \mid t, n \mid t \iff mn \mid t.$$

This last equivalence is the lemma, because $gcd(m, n) = 1$.

It follows that

$$\{e_{G\times H}, (a,b), (a,b)^2, \ldots, (a,b)^{mn-1}\}$$

are distinct and $(a,b)^{mn} = e_{G\times H}$. That is,

$$C_m \times C_n = \langle (a,b) \rangle$$

is a cyclic group of order mn. □

This is what we found for $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/3\mathbb{Z}, \oplus)$.

What happened for $(\mathbb{Z}/2\mathbb{Z}, \oplus) \times (\mathbb{Z}/4\mathbb{Z}, \oplus)$ is different. Here, we can take the generators of the factors as $[1]_2$ and $[1]_4$, and $([1]_2, [1]_4)^4 = ([4]_2, [4]_4) = ([0]_2, [0]_4)$ is the identity. In fact, for any element of this group of order 8,

$$([i]_2, [j]_4)^4 = ([4i]_2, [4j]_4) = ([0]_2, [0]_4),$$

so there is no element of order 8, and so the group is not cyclic.

THEOREM If $gcd(m,n) = g > 1$, then $C_m \times C_n$ is not cyclic.

PROOF Write $m = gm'$ and $n = gn'$ and let $T = gm'n' = mn/g$; $T < mn$. (This is also equal to $lcm(m,n)$, but we don't need that here.) Let (a^j, b^k) be any element of the group. Then recalling the definitions of m' and n', we get

$$(a^j, b^k)^T = (a^{jgm'n'}, b^{kgm'n'}) = (a^{jmn'}, b^{knm'}) =$$
$$((a^m)^{jn'}, (b^n)^{km'}) = (e_G^{jn'}, e_H^{km'}) = e_{G\times H}.$$

Since $|C_m \times C_n| = mn > T$, this means that there is no element which generates the entire group, so it isn't cyclic. □

Final note: we won't prove it in this class, and Fraleigh doesn't prove it in the book, but one of the reasons this sort of thing is studied is the Fundamental Theorem of Abelian Groups: every finite abelian group can be written as a product of cyclic groups whose orders are each the power of a prime.

To be precise, suppose G is a finite abelian group of order

$$n = p_1^{a_1} \dots p_s^{a_s}$$

Then for each k, $1 \leq k \leq s$, there is a group

$$G_k = C_{p_k^{b_{k1}}} \times \cdots \times C_{p_k^{b_{km_k}}}, \quad \sum_{\ell} b_{k\ell} = a_k$$

and G is isomorphic to

$$G_1 \times G_2 \cdots \times G_s.$$