M7210 Lecture 19 Friday October 5, 2012

Today, we'll begin by proving the criterion for recognizing products that we didn't get to last time. Then, we'll define and study semidirect products.

Direct Products.

If K and L are groups, then $K \times L$, with operation $(k_1, \ell_1)(k_2, \ell_2) = (k_1k_2, \ell_1\ell_2)$ is a group. $K \times L$ has projection homomorphisms $\pi_K : (k, \ell) \mapsto k$ and $\pi_L : (k, \ell) \mapsto \ell$ that satisfy the following universal mapping property:

(UMP) given any group T and homomorphisms $\gamma : T \to K$ and $\delta : T \to L$, there is a unique homomorphism $\gamma \times \delta : T \to K \times L$ such that $\pi_K(\gamma \times \delta) = \gamma$ and $\pi_L(\gamma \times \delta) = \delta$.

Notice that $K \times \{e_L\}$ and $\{e_K\} \times L$ are both normal in $K \times L$; indeed, these are the kernels of the projection homomorphisms. Also note that in $K \times L$ every element of the former commutes with every element of the latter, and their intersection is $e_{K\times L}$.

The following theorem is useful in recognizing when a group is isomorphic to a product.

Proposition 1. *Suppose G is a group with subgroups K and L such that:*

i) $K \cap L = \{e_G\}$;

ii) *for all $k \in K$ and $\ell \in L$, $k\ell = \ell k$;*

iii) $KL = G$.

Then G is isomorphic to the product $K \times L$.

Proof. By *iii)*, every element $g \in G$ can be written in the form $k\ell$ with $k \in K$ and $\ell \in L$. If $k_1\ell_1 = k_2\ell_2$, then $k_2^{-1}k_1 = \ell_2\ell_1^{-1} \in K \cap L$, so by *i)* $k_1 = k_2$ and $\ell_1 = \ell_2$. Thus, the representation is unique. Thus, we can define "projection maps" $\phi_K := G \to K$ by $\phi_K(k\ell) = k$ and $\phi_L := G \to L$ by $\phi_L(k\ell) = \ell$. We prove that G, with these projections has the UMP that defines $K \times L$. Suppose T is any group, and let $\gamma : T \to K$ and $\delta : T \to L$ be given. Define $(\gamma \times \delta)(t) := \gamma(t)\delta(t)$. This map is obviously the unique function that composes with the projections as required, but is it a homomorphism? If $s, t \in T$, then (Ta'Daa):

$$(\gamma \times \delta)(st) = \gamma(st)\delta(st) = \gamma(s)\gamma(t)\delta(s)\delta(t) \overset{\text{by } ii)}{=} \gamma(s)\delta(s)\gamma(t)\delta(t) = \Big((\gamma \times \delta)(s)\Big)\Big((\gamma \times \delta)(t)\Big). \quad /////$$

Exercise 1. Suppose that p and q are distinct primes. Show that any abelian group of order pq is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Exercise 2. Give an alternate proof of the proposition that produces an isomorphism between $K \times L$ and G directly.

Remark. The proposition does not assume that the subgroups K and L are normal, but this of course follows from the isomorphism of G with $K \times L$.

Exercise 3. Prove the normality of K and L directly from the hypotheses. Are all three assumptions about K and L needed for this conclusion?

Exercise 3 has a converse. Assumption *ii)* is a consequence of *i)* and: *ii′)* the two subgroups K and L are normal in G. To see this, assume *i)*, *ii′)*. Let $k \in K$ and $\ell \in L$. Then $\ell k\ell^{-1} \in K$, so $\ell k\ell^{-1}k^{-1} \in K$. Also, since $\ell^{-1} \in L$, $k\ell^{-1}k^{-1} \in L$, so $\ell k\ell^{-1}k^{-1} \in L$. By *i)*, $\ell k\ell^{-1}k^{-1} = e$. It follows that $\ell k = k\ell$. Thus,

Proposition 2. *Suppose G is a group with subgroups K and L such that:*

i) $K \cap L = \{e_G\}$;

ii′) *K and L are both normal;*

iii) $KL = G$.

Then G is isomorphic to the product $K \times L$.

Semidirect Products

Some groups do not satisfy the hypotheses of this proposition, but *nearly* do. Consider the group D_{2n}, which as we have seen is generated by two elements ρ and σ such that $\rho^n = e$, $\sigma^2 = e$ and $\sigma\rho\sigma\rho = e$:

$$D_{2n} = \{\, \rho^k\sigma^\ell \mid 0 \le k \le n-1,\, 0 \le \ell \le 1 \,\}.$$

The subgroups $K = \langle\rho\rangle$ and $L = \langle\sigma\rangle$ satisfy all the hypotheses of Proposition 2, except that only K is normal, but L is not. There is a bijection of D_{2n} with the set $K \times L$, but the multiplication is not the canonical product operation. Indeed, if we write (k, ℓ) as an abbreviation for $\rho^k\sigma^\ell$—taking $k \in \mathbb{Z}/n\mathbb{Z}$ and $\ell \in \mathbb{Z}/2\mathbb{Z}$—then the rule for multiplication is:

$$(k_1, \ell_1)(k_2, \ell_2) = \rho^{k_1}\sigma^{\ell_1}\rho^{k_2}\sigma^{\ell_2} = \rho^{k_1}\rho^{(-1)^{\ell_1}k_2}\sigma^{\ell_1}\sigma^{\ell_2} = (k_1 + (-1)^{\ell_1}k_2, \ell_1 + \ell_2).$$

Can we generalize this construction? We need to make sense of the meaning of $(-1)^\ell k$. The map $k \mapsto -k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/nZ$ is an bijection of $\mathbb{Z}/n\mathbb{Z}$ with itself and is also a homomorphism.

Definition. Let K be a group. An *automorphism* of K is an isomorphism of K with itself. The group of all automorphisms of K is denoted $\mathrm{Aut}(K)$

The map $\ell \mapsto (-1)^\ell : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is a homomorphism.

Suppose K and L are any groups whatsoever, and $\ell \mapsto \alpha_\ell : L \to \mathrm{Aut}(K)$ is any homomorphism. Define an operation $\cdot_\alpha$ on $k \times \ell$ by:

$$(k_1, \ell_1) \cdot_\alpha (k_2, \ell_2) = (k_1\alpha_{\ell_1}(k_2), \ell_1\ell_2).$$

Exercise 4. Show that $\cdot_\alpha$ is an associative operation on $K \times L$ with identity (e_K, e_L) and inversion $(k, \ell) \mapsto (\alpha_\ell^{-1}(k^{-1}), \ell^{-1})$.

Exercise 5. Call the group obtained in the previous exercise $K \times_\alpha L$. Show that $K \times \{e_L\}$ and $\{e_K\} \times L$ are subgroups of $K \times_\alpha L$ that are isomorphic to K and L respectively. Identifying these subgroups with K and L, show that if $k \in K \subseteq K \times_\alpha L$ and $\ell \in L \subseteq K \times_\alpha L$, then $\ell k \ell^{-1} = \alpha_\ell(k)$.

Exercise 6. Study the text, pages 167 and 168. Restate 4.43 and 4.44 in the notation of this lecture.

In order to construct concrete examples, we will need to be able to name concrete homomorphisms $L \to \mathrm{Aut}(K)$. The simplest situation arises when both L and K are cyclic. Any homomorphism with a cyclic group as domain is completely determined by the image of a generator. So, in particular, any automorphism of a cyclic group is determined by the image of a generator, and the generators of $\mathbb{Z}/n\mathbb{Z}$ are the classes $m + n\mathbb{Z}$ such that $(m, n) = 1$.

Example. Here, we will give an example that parallels the dihedral group. The purpose is to illustrate the semidirect product construction. Let's let $K = \mathbb{Z}/100\mathbb{Z}$. There is an automorphism α of K that sends $\overline{1}$ to $\overline{71}$. (I just selected this number randomly.) Note that α is "multiplication by 71 mod 100". Thus, $\alpha^n(1) = \overline{71}^n$. Using a calculator, we find the following (where we understand the integers that are not in exponents to refer to elements of $K = \mathbb{Z}/100\mathbb{Z}$):

$$\alpha(1) = 71,\ \alpha^2(1) = 41,\ \alpha^3(1) = 11,\ \alpha^4(1) = 81,\ \alpha^5(1) = 51,$$

$$\alpha^6(1) = 21,\ \alpha^7(1) = 91,\ \alpha^8(1) = 61,\ \alpha^9(1) = 31,\ \alpha^{10}(1) = 1.$$

This shows that there is a homomorphism from $\mathbb{Z}/10\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/100\mathbb{Z})$ that sends $1 + 10\mathbb{Z}$ to α. Thus, on $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, we have a group operation defined by:

$$(k_1, \ell_1)(k_2, \ell_2) = (k_1 + (71)^{\ell_1}k_2, \ell_1 + \ell_2),$$

where we read the k_is modulo 100 and the ℓ_js modulo 10.

Remark. Let p be a positive prime. As you know, $\mathbb{Z}/p\mathbb{Z}$ is a field, and therefore the non-zero elements form an abelian group under multiplication. This $(p-1)$-element abelian group is denoted $(\mathbb{Z}/p\mathbb{Z})^\times$. It is straightforward to show that $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Amazingly, $(\mathbb{Z}/p\mathbb{Z})^\times$ is always cyclic. This takes some effort to prove. The usual approach today is to use some facts about polynomials—see Knapp, page 152. The first proofs of this were given by Gauss in the *Disquisitiones Arithmeticae* (1801) in Articles 54 and 55.