MATH 436 Notes: Cyclic groups and Invariant Subgroups.

Jonathan Pakianathan

September 30, 2003

1 Cyclic Groups

Now that we have enough basic tools, let us go back and study the structure of cyclic groups. Recall, these are exactly the groups G which can be generated by a single element $x \in G$.

Before we begin we record an important example:

Example 1.1. *Given a group G and an element $x \in G$ we may define a homomorphism $\phi_x : \mathbb{Z} \to G$ via $\phi_x(n) = x^n$. It is easy to see that $Im(\phi_x) = < x >$ is the cyclic subgroup generated by x.*

If one considers $ker(\phi_x)$, we have seen that it must be of the form $d\mathbb{Z}$ for some unique integer $d \geq 0$. We define the order of x, denote $o(x)$ by:

$$o(x) = \begin{cases} d \text{ if } d \geq 1 \\ \infty \text{ if } d = 0 \end{cases}$$

Thus if x has infinite order then the elements in the set $\{x^k | k \in \mathbb{Z}\}$ are all distinct while if x has order $o(x) \geq 1$ then $x^k = e$ exactly when k is a multiple of $o(x)$. Thus $x^m = x^n$ whenever $m \equiv n$ modulo $o(x)$.

By the First Isomorphism Theorem, $< x > \cong \mathbb{Z}/o(x)\mathbb{Z}$. Hence when x has finite order, $| < x > | = o(x)$ and so in the case of a finite group, this order must divide the order of the group G by Lagrange's Theorem.

The homomorphisms above also give an important cautionary example!

Example 1.2 (Image subgroups are not necessarily normal). *Let* $G = \Sigma_3$ *and* $a = (12) \in G$. *Then* $\phi_a : \mathbb{Z} \to G$ *defined by* $\phi_a(n) = a^n$ *has image* $Im(\phi_a) =< a >$ *which is not normal in* G.

Before we study cyclic groups, we make a useful reformulation of the concept:

Lemma 1.3. *A group* G *is cyclic if and only if there is an epimorphism* $\phi : \mathbb{Z} \twoheadrightarrow G$.

Proof. $\Longrightarrow$**:** If $G =< x >$ is a cyclic group then the homomorphism defined in Example 1.1 is an epimorphism $\mathbb{Z} \twoheadrightarrow G$.
$\Longleftarrow$**:** On the other hand if $\phi : \mathbb{Z} \twoheadrightarrow G$ is an epimorphism then $x = \phi(1)$ is easily seen to generate G. □

Definition 1.4. *We say* H *is a quotient group of* G *if there is an epimorphism* $G \twoheadrightarrow H$.

Now we are ready to prove the core facts about cyclic groups:

Proposition 1.5. *The following are facts about cyclic groups:*
(1) A quotient group of a cyclic group is cyclic.
(2) Subgroups of cyclic groups are cyclic.
(3) If G *is a cyclic group then* G *is isomorphic to* $\mathbb{Z}/d\mathbb{Z}$ *for a unique integer* $d \geq 0$. *(Note that when* $d = 0$, $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$*). Thus a cyclic group is determined up to isomorphism by its order.*

Proof. **(3):** By Lemma 1.3, there is an epimorphism $\phi : \mathbb{Z} \twoheadrightarrow G$. Then the First Isomorphism Theorem shows that $G \cong \mathbb{Z}/d\mathbb{Z}$ where $d\mathbb{Z} = ker(\phi)$, $d \geq 0$.
(1): Let $G \xrightarrow{\lambda} H$ and suppose G cyclic generated by x. It is easy to see that since λ is an epimorphism, $\lambda(x)$ generates H and so H is cyclic also.
(2): Now suppose G is cyclic and $H \leq G$. Then by Lemma 1.3, we have an epimorphism $\mathbb{Z} \xrightarrow{\phi} G$. Let $S = \phi^{-1}(H)$ then $S \leq \mathbb{Z}$ and so is cyclic generated by some integer $d \geq 0$. Then ϕ restricts to an epimorphism $S \twoheadrightarrow H$ and so H is cyclic as it is a quotient of a cyclic group.

□

2 Invariant Subgroups

We begin this section with yet another important example of a homomorphism:

Theorem 2.1. *Let G be a group and $g \in G$. We define $\gamma_g : G \to G$ by $\gamma_g(h) = ghg^{-1}$ for all $h \in G$. γ_g is refered to as the conjugation map given by conjugation by g.*

Then $\gamma_g \in Aut(G)$ for all $g \in G$. We refer to the set $\{\gamma_g | g \in G\}$ as the set of inner automorphisms of G and denote it $Inn(G)$.

Proof. The only thing we need to prove it that γ_g is a bijective homomorphism of G to itself.

We calculate

$$\gamma_g(hw) = ghwg^{-1} = ghg^{-1}gwg^{-1} = \gamma_g(h)\gamma_g(w)$$

and hence γ_g is an endomorphism of G. On the other hand

$$\gamma_{g^{-1}}(\gamma_g(h)) = \gamma_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}(g^{-1})^{-1} = h$$

for all $h \in G$. Thus $\gamma_{g^{-1}} \circ \gamma_g = 1_G$ for all $g \in G$, and also $\gamma_g \circ \gamma_{g^{-1}} = 1_G$ by interchanging the roles of g and g^{-1}. Thus each γ_g is bijective and hence gives an automorphism of G. □

We next show that the correspondence $g \to \gamma_g$ itself is a homomorphism!

Theorem 2.2 (Conjugation Action Homomorphism). *Let G be a group, then the function $\Theta : G \to Aut(G)$ given by $\Theta(g) = \gamma_g$ is a homomorphism with image $Inn(G)$ and kernel $Z(G) = \{g \in G | gh = hg \text{ for all } h \in G\}$. $Z(G)$ is called the center of G, it consists of the elements of G which commute with everything in G.*

Thus $Inn(G) \leq Aut(G)$, $Z(G) \trianglelefteq G$ and $G/Z(G) \cong Inn(G)$.

Proof. We calculate:

$$\gamma_{gg'}(h) = (gg')h(gg')^{-1} = g(g'hg'^{-1})g^{-1} = g\gamma_{g'}(h)g^{-1} = \gamma_g(\gamma_{g'}(h))$$

for all $g, g', h \in G$. Thus we conclude $\gamma_{gg'} = \gamma_g \circ \gamma_{g'}$ for all $g, g' \in G$ and hence Θ is a homomorphism.

It is clear that $Im(\Theta) = Inn(G)$ by definition. On the other hand

$$\begin{aligned} g \in ker(\Theta) &\leftrightarrow \gamma_g = 1_G \\ &\leftrightarrow ghg^{-1} = h \text{ for all } h \in G \\ &\leftrightarrow gh = hg \text{ for all } h \in G \\ &\leftrightarrow g \in Z(G). \end{aligned}$$

The final line of the theorem then follows from the First Isomorphism Theorem and the general facts on images and kernels of homomorphisms. □

Definition 2.3. *In the homework, you will in fact show that* $Inn(G) \trianglelefteq Aut(G)$*. Thus we may define the quotient group* $Out(G) = Aut(G)/Inn(G)$*, of outer automorphisms of* G*. Thus* $Out(G)$ *measures in some sense the automorphisms of* G *which are not given by conjugation.*

Notice that if G *is Abelian, all non-identity automorphisms of* G *have to be outer automorphisms.*

We look at some examples next, but first a basic lemma:

Lemma 2.4 (Orders under homomorphisms). *If* $f : G \to H$ *is a homomorphism and* $x \in G$ *has finite order then* $f(x)$ *also has finite order and* $o(f(x))|o(x)$*.*

If $f : G \to H$ *is an isomorphism then* $o(x) = o(f(x))$ *for all* $x \in G$*.*

Proof. Let $x \in G$ have finite order $o(x) = m \geq 1$. Then $x^m = e$ so applying f to both sides of this equation we fine $f(x)^m = f(x^m) = f(e) = e$. Thus $f(x)$ has finite order and $o(f(x))|m$ as we desired to show.

If $f : G \to H$ is an isomorphism, it restricts to an isomorphism of $< x >$ and $< f(x) >$ and so $o(x) = o(f(x))$ in this case. □

We can now work out some examples:

Example 2.5 (Automorphisms of Σ_3). *As* $|\Sigma_3| = 3! = 6$*, there are* $6! = 720$ *bijections of* Σ_3 *to itself. We would like to decide which of these are automorphisms! We can compute the orders of elements of* Σ_3*:*
$Order 1 : e$
$Order 2 : (12), (13), (23)$
$Order 3 : (123), (132)$
We have seen that $\{(12), (13)\}$ *generate* Σ_3 *and that automorphisms* τ *are uniquely determined by what they do on a generating set. Thus it suffices to*

consider the possibilities for $\tau((12))$ and $\tau((13))$. Since (12) has order 2, we see that $\tau((12))$ would have to have order 2 by Lemma 2.4. Thus there are 3 possibilities for $\tau((12))$. Once we have chosen one of these, as $\tau((13))$ must also have order 2, and τ is injective we have two possibilities left for $\tau((13))$. Thus there are at most $3 \times 2 = 6$ automorphisms of Σ_3.

On the other hand it is simple to check that $Z(\Sigma_3) = \{e\}$ and so $Inn(\Sigma_3) \cong \Sigma_3/Z(\Sigma_3)$ has order 6. Thus we conclude that $Aut(\Sigma_3) = Inn(\Sigma_3) \cong \Sigma_3$ and that $Out(\Sigma_3) = 1$. Thus all automorphisms of Σ_3 are inner automorphisms.

Notice also that only 6 out of the 720 bijections of Σ_3 to itself preserve the algebraic structure!

We next consider subgroups invariant under various classes of endomorphisms of G:

Definition 2.6. *Let $H \leq G$. We say that:*
(1) H is normal in G if $\gamma_g(H) \subseteq H$ for all inner automorphisms γ_g of G. We write $H \trianglelefteq G$ in this case.
(2) H is characteristic in G if $\tau(H) \subseteq H$ for all automorphisms τ of G. We write $H \leq_{char} G$ in this case.
(3) H is fully invariant in G if $\lambda(H) \subseteq H$ for all endomorphisms λ of G. We write $H \leq_{f.i.} G$ in this case.

It is immediate that

$$H \leq_{f.i.} G \implies H \leq_{char} G \implies H \trianglelefteq G.$$

This is because $Inn(G) \subseteq Aut(G) \subseteq End(G)$ and because if a subgroup is invariant under a bigger set of endomorphisms, it is also invariant for a subset.

One thing we should check is that the definition of normal subgroup given in Definition 2.6 is the same as the one we previously gave!

Note $\gamma_g(H) \subset H$ for all $g \in G$ is equivalent to $gHg^{-1} \subset H$ for all $g \in G$. This is in turn equivalent to $gHg^{-1} = H$ for all $g \in G$. (This can be seen by replacing g with g^{-1}.) Finally this is equivalent to $gH = Hg$ for all $g \in G$ which was our original definition of normality. Thus the two definitions coincide.

The following is a basic proposition:

Proposition 2.7. *Let G be a group then:*
(1) $K \leq_{char} H, H \leq_{char} G \implies K \leq_{char} G$.

(2) $K \leq_{f.i.} H, H \leq_{f.i.} G \implies K \leq_{f.i.} G$.
(3) $K \trianglelefteq H, H \trianglelefteq G$ *does not imply* $K \trianglelefteq G$. *Thus "being a normal subgroup" is not a transitive relation!*

Proof. We only prove (1). The proof of (2) is similar and is left to the reader. So suppose $K \leq_{char} H, H \leq_{char} G$ and let $\tau \in Aut(G)$. Then τ restricts to an automorphism $\tau|_H$ of H as H is characteristic in G. (τ^{-1} will restrict to give the inverse automorphism.) Since K is characteristic in H, $\tau|_H(K) = \tau(K) \subseteq K$. Thus we see that $\tau(K) \subseteq K$ for all $\tau \in Aut(G)$ and so $K \leq_{char} G$.

A counterexample for (3) will be done in the Homework. The proof for (1) and (2) does not carry over to (3) as the restriction of an inner automorphism of G to a subgroup H can yield an automorphism of H which is not inner. For example, in Σ_3, let $H =< (123) >$ and let $g = (12) \in \Sigma_3 - H$. Then conjugation by g, gives an inner automorphism γ_g of Σ_3 which restricts to a nontrivial automorphism of H as $H \trianglelefteq \Sigma_3$. Moreover since H is Abelian, we see that $\gamma_g|H$ is an outer automorphism of H. So restrictions of inner automorphisms need not be inner!

□

We will give an example of a fully invariant subgroup but first a definition:

Definition 2.8 (Commutators). *Given a group* G *and* $x, y \in G$ *we define the commutator* $[x, y]$ *by* $[x, y] = xyx^{-1}y^{-1}$. *It is simple to check that*

$$xy = [x, y]yx$$

and so the commutator $[x, y]$ *measures the failure of* x *and* y *to commute.*

Note:

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x].$$

So the inverse of a commutator $[x, y]$ *is the commutator* $[y, x]$.

Example 2.9 (Commutator subgroup). *Given a group* G, *we define the commutator subgroup* G' *(sometimes denoted also by* $[G, G]$*) by*

$$G' =< [x, y] | x, y \in G > .$$

Thus G' is generated by all the commutators in G. The typical element in G' is a finite product of commutators $[x_1, y_1][x_1, y_2] \dots [x_k, y_k]$. (we don't have to use inverses as the inverse of a commutator is itself a commutator).

Note it is easy to see that $G' = \{e\}$ if and only if G is Abelian.

Proposition 2.10 (Commutator Subgroups are Fully Invariant). *Let G be a group, then $G' \leq_{f.i.} G$ and so in particular $G' \trianglelefteq G$. The quotient group G/G' is Abelian.*

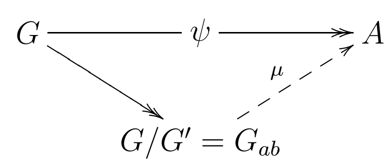
Proof. Let $f : G \to G$ be an endomorphism of G. Then we compute:

$$f([x, y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = [f(x), f(y)].$$

Thus f takes commutators to commutators and hence takes a finite product of commutators to a finite product of commutators. Hence $f(G') \subseteq G'$. Since this holds for any endomorphism f, we see that $G' \leq_{f.i} G$.

Now we show G/G' is Abelian. Let $x, y \in G$ then it is simple to compute that $[xG', yG'] = [x, y]G' = G'$ as $[x, y] \in G'$. Thus xG', yG' commute in G/G'. Since xG', yG' were arbitrary in G/G' we conclude that G/G' is Abelian. □

Theorem 2.11 (Abelianizations). *Given a group G we define G_{ab}, the Abelianization of G via $G_{ab} = G/G'$. We have seen previously that G_{ab} is Abelian. In fact, it is the largest Abelian quotient of G. In other words, given an epimorphism $G \overset{\psi}{\twoheadrightarrow} A$ where A is Abelian, we may always find a homomorphism μ making the following diagram commute:*



In particular, A will be a quotient of G_{ab}.

Proof. This will follow from our fundamental factorization lemma once we can show G' is contained in $ker(\psi)$. Now $\psi([x, y]) = [\psi(x), \psi(y)] = e$ as this final commutator lives in an Abelian group A. Thus all commutators of G lie in $ker(\psi)$ and so it follows that $G' \subseteq ker(\psi)$. The existance of a homomorphism μ making the diagram commute then follows from our fundamental factorization theorem.

□