

# 1 September 19

Recall from last time:  $D_n = \{\text{rotations/reflections of } n\text{-gon}\}$ , where the  $n$  rotation by  $\frac{2\pi a}{n}$ ,  $0 \leq a \leq n-1$ , and the  $n$  reflections in axes of symmetry.

Claim: these are all distinct,  $2n$  in total. Obviously: reflections are distinct and rotations are distinct between each other. But can we have rotation = reflection?

The answer is no: linear algebra.

- The rotation of  $\mathbb{R}^2$ : matrix  $\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ . Has  $\det = 1$ .
- Reflection in  $\mathbb{R}^2$  has eigenvalues  $\pm 1$ , and  $\det = -1$ .

Then he draws a picture idk ff.

## Abstract version of $D_n$

Let  $\sigma =$  rotation through  $2\pi/n$ , so  $\sigma^a =$  rotation through  $2\pi a/n$ . Rotations are  $\sigma, \sigma^2, \dots, \sigma^n = I$  and  $I = \{1, \sigma, \dots, \sigma^{n-1}\}$ .

Now let  $\tau =$  reflection in x-axis. Claim: Reflections  $= \{\tau, \tau\sigma, \tau\sigma^2, \dots, \tau\sigma^{n-1}\}$ .

*Proof.*  $D_n = \text{group} \Rightarrow \tau\sigma^j =$  either a rotation or a reflection.

Case 1:  $\tau\sigma^j$  is a reflection

Case 2:  $\tau\sigma^j$  is a rotation, or  $\sigma^k$  for some  $k$ . But then  $\tau\sigma^j = \sigma^k \Rightarrow \tau(\sigma^j)(\sigma^j)^{j-1} = \sigma^k(\sigma^j)^{-1} \Rightarrow \tau = \sigma^k\sigma^{n-j} = \sigma^{k+n-j}$ . And this is impossible because LHS  $= \tau =$  nontrivial reflection, but RHS  $=$  rotation, which we know can't be equal.

Thus, it has to be case 1, so  $\tau\sigma^j = \text{reflection } \forall j$ . But  $\tau\sigma^j = \tau\sigma^{j'} \Rightarrow j = j'$ ,  $0 \leq j, j' \leq n-1$ . Same argument:  $\tau\sigma^j = \tau\sigma^{j'} \Rightarrow \tau^{-1}\tau\sigma^j = \tau^{-1}\tau\sigma^{j'} = \sigma^j = \sigma^{j'} \Rightarrow j = j'$ . Thus,  $\tau, \tau\sigma, \dots, \tau\sigma^{n-1}$  are all different, and all reflections, so we get them all.  $\square$

Thus, we get some idea of what  $D_n$  looks like.  $D_n = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}\}$  where  $\sigma$  is a rotation through  $\frac{2\pi}{n}$  and  $\tau$  is a reflection ff

ff end of page 3 and start of page 4 by closure, but what are  $i, j$ ? What is the algebra rule that does this? Answer:  $\tau\sigma^j = \sigma^{n-j}\tau = \sigma^{-1}\tau$ . Supposedly a homework question, nominally due today, but didn't release. Anyway,

we know how  $\tau$  and  $\sigma$  interact through linear algebra, so  $\tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  when it is a reflection in the  $y$  axis, and

the rotation  $\sigma = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$ . Then

$$\begin{aligned} \tau\sigma &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \\ &= \begin{pmatrix} -\cos \theta & -\sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \\ &= \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= f f \end{aligned}$$

So to simplify  $\sigma^2\tau\sigma^3 = (\sigma^2\tau)\sigma^3 = \tau(\sigma^2)^{-1}\sigma^3 = \tau\sigma^{n-2+3} = \tau\sigma^{n+1} = \tau\sigma \in D_n$ .

The third way to write  $D_n$  is  $\{1, \sigma, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1}\}$  with the rules  $\tau^2 = 1$  (reflection),  $\tau\sigma = \sigma^{-1}\tau$ , and  $\sigma^n = 1$ .

*Remark 1.* These rules imply all the others

Let's see with  $(\tau\sigma^i)^2 = \tau\sigma^i\tau\sigma^i = \sigma^{-i}\tau\tau\sigma^i = 1$  (where we have used  $\tau\sigma^i = \sigma^{-i}\tau$ , which can be found with induction and the given rules). This is an *algebraic* way of describing  $D_n$ .

In a crude form, a group is set of elements with some rules how they interact. This wraps up our beginning bit of groups, but keep in mind  $S_n$  and  $D_n$ : they're the simplest nonabelian groups, and we can actually write down all the elements.

## Ch. 1.3 Isomorphism, Homomorphism

These are going to be our version of linear transformations from linear algebra, but for groups.

**Definition 1** (Homomorphism). Let  $G_1, G_2$  be groups. A *homomorphism* from  $G_1 \rightarrow G_2$  is a function  $\phi: G_1 \rightarrow G_2$  such that  $\forall g_1, g_2 \in G_1$ ,  $\underbrace{\phi(g_1 g_2)}_{\text{multiplication in } G_1} = \underbrace{\phi(g_1)\phi(g_2)}_{\text{multiplication in } G_2}$ .

We must have  $\phi(1_{G_1}) = 1_{G_2}$ .

*Isomorphism*  $\phi$  is a bijection, so it matches both sets and the multiplication, while *Homomorphism* only matches multiplication (need not be injective or surjective).

Some examples

- $\exp: x \mapsto e^x$ , which matches  $(\mathbb{R}, +) \rightarrow \mathbb{R}_+^*$  (positive reals, with multiplication). This is an isomorphism.
- $\phi: \mathbb{R} \rightarrow \mathbb{C}^*$  such that  $x \mapsto e^{2\pi i x}$ , which sends  $\mathbb{R}$  to the complex numbers of modulus 1. This is surjective, but it is not injective, since  $e^{2\pi i x} = 1, \forall x \in \mathbb{Z}$ . So this is only a homomorphism.
- Let  $G = n \times n$  invertible real matrices, and  $\phi(g) = \det(g) \in \mathbb{R}^*$ . This is only a homomorphism, since  $G \rightarrow \mathbb{R}^*$  (multiplication) since  $\det(AB) = \det(A)\det(B)$ , but it is not injective. Also have the identity map (maps to itself).
- Let  $G$  be any group, and  $\phi(G) = 1 \in G_2, \forall g \in G_1$  and any  $G_2$ . This is a homomorphism from  $G_1 \rightarrow G_2$ , called the “trivial” homomorphism.

**Definition 2** (Subgroups).  $G$  = group, a subset of it is ff (bottom of page 7)

**Theorem 1** (Cayley’s Theorem). Let  $G$  be any finite group. Then  $G$  is isomorphic to a subgroup of  $S_n$  (permutation on  $n$  letters) for some  $n$ .

Concretely, this means  $\exists n \geq 1$  and a homomorphism  $\phi: G \rightarrow S_n$  that is injective.

*Proof.* Let  $n = \#G$  = number of elements in  $G$ . So the set of  $n$  objects = elements of  $G$ . (How do objects in  $G$  move around? When you multiply two by each other, you get another element in  $G$ .) So for all  $g \in G$ , consider the function  $L_g, R_g$ , where  $L_g, R_g: G \rightarrow G$ , where  $L_g(x) = gx$  (fixed  $g, \forall x \in G$ ) and  $R_g(x) = xg$  (fixed  $g, \forall x \in G$ ).

Claim:  $L_g, R_g$  are permutations of  $G$ .

Check: we need to show they are bijections (could show that they are injective and surjective, or that they have an inverse, the second is easier). So  $(Lg^{-1}) \circ L_g(x) = g^{-1}(gx) = x \Rightarrow L_{g^{-1}} = (L_g)^{-1}$  is a function. Similarly,  $R_{g^{-1}} = (R_g)^{-1}$ . Thus  $g \mapsto L_g$  and  $g \mapsto R_g$  so  $G \rightarrow S_n$  something something.

Check: we need to show that the homomorphism respects the multiplication. Let  $\phi(g) = L_g$  and  $\phi(g) = R_g$ . We want  $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$  and  $\psi(g_1 g_2) = \psi(g_1)\psi(g_2)$ . Looking at the first, we have LHS =  $L_{g_1 g_2} = x \mapsto (g_1 g_2)x$  and RHS =  $L_{g_1} \circ L_{g_2}(x) = g_1(g_2 x) = (g_1 g_2)x$ . Thus  $\phi$  is a homomorphism. Now looking at the second, note that  $\psi$  is not a homomorphism in general. We see LHS =  $R_{g_1 g_2} = x \mapsto x g_1 g_2$  and RHS =  $R_{g_1} \circ R_{g_2}(x) = (x g_2) g_1 = x g_2 g_1 \neq x g_1 g_2$ . Just so happens that left multiplication is the homomorphism. So we get the homomorphism  $\phi: G \rightarrow S_n$  where  $g \mapsto L_g$ .

Finally, to show that this is an isomorphism, need to check that  $\phi$  is injective.

ff (page 10 and 11)

Conclusion  $\phi: G \rightarrow S_n$  where  $g \mapsto L_g$  is an injective homomorphism  $G \rightarrow S_n$ . □

Going to sort out homework, probably compressed deadline but has given some answers already.

## 2 September 21

Last time, we started proving (proved?) Cayley’s theorem. That is, for a finite group  $G$ , there exists  $\phi: G \rightarrow S_n$  that is an injective homomorphism ( $n = \#G$ ).

**Remark 2.**  $\#S_n = n! > n = \#G$ .  $G$  is a very small subgroup of  $S_n$ .

Something we will see again later:  $\exists m \neq n$  with  $G \rightarrow S_m$  injectively (usually  $m$  could be much smaller).

## 2.1 1.4 Commutativity, general associativity

The usual associative law is  $(ab)c = a(bc)$ : can put brackets anywhere to simplify (don't rearrange terms). Usual law of commutativity is  $ab = ba$ . Not going to spend much time on this, kinda boring, can figure it out for yourself.

## 2.2 1.5 ff

We'll be looking at cyclic groups, and subgroups generated by a subset.

Let  $G$  be a group, and  $S \subseteq G$  any subset.

*Definition 3* (Subgroup Generated by  $\langle S \rangle$ ).  $\langle S \rangle$  = smallest subgroup of  $G$  containing  $S$ .  $\langle S \rangle$  is a subgroup containing  $S$ , and if  $H$  is any subgroup which contains  $S$ . Then  $\langle S \rangle \subseteq H$ . We call  $\langle S \rangle$  the subgroup generated by  $S$ .

Existence of  $\langle S \rangle$ :  $X$  = set of subgroups of  $G$  containing  $S$ . Then  $G \in X$ ,  $X \neq \emptyset$ .  $\langle S \rangle$  is a minimal element of  $X$ . Arbitrary intersections of subgroups are subgroups (exercise), thus take the intersection of all elements of  $X$  to get  $\langle S \rangle$ . Concretely,  $\langle S \rangle$  is the arbitrary finite products of elements of  $S$  and their inverses.

$$\langle S \rangle = \left\{ \prod_{i=1}^r S_i^{\varepsilon_i} \mid S_i \in S, \varepsilon_i = \pm 1, r = \text{any positive integer} \right\}$$

You can think of this as the "span" of  $S$  (but not commutative).

*Remark 3.*  $\langle S \rangle$  is very hard to describe in terms of  $S$  (expressions as products are usually not unique).

For example, if  $G = S_n$  and  $S = \{\sigma, \tau\}$  from  $D_n$ , so  $\sigma = 1 \rightarrow 2, 2 \rightarrow 1$  (fixes all others) and  $\tau = 1 \rightarrow 2 \rightarrow \dots \rightarrow n \rightarrow 1$ . Actually,  $\langle S \rangle = S_n$ . This means that we can get any permutation

Special case:  $S = \{g\}$  = single element. Then  $\langle S \rangle = \{g^i \mid i \in \mathbb{Z}\}$ . We have  $1 = g^0$  (convention from law of exponents) and  $g^i g^j = g^{i+j}$ . Our subgroup generated by  $S$  is  $\langle S \rangle = \text{group, } g \in S \subseteq \langle S \rangle \iff g^i \in \langle S \rangle \forall i$ .

There exists a homomorphism  $\phi: (\mathbb{Z}, +) \rightarrow \langle S \rangle \subseteq G$  defined by  $i \mapsto g^i$ . 2 cases:  $\phi$  is injective or  $\phi$  is not injective.

*Remark 4.*  $\phi: \mathbb{Z} \rightarrow \langle S \rangle$  is always onto. If  $\phi$  is injective, then  $\phi: \mathbb{Z} \rightarrow \langle S \rangle$  is an isomorphism,  $\langle S \rangle$  and  $\mathbb{Z}$  are the same.

Some notation: we would say  $\mathbb{Z} \cong \langle S \rangle$  (isomorphic) (isomorphic)

Some more notation (additive notation):  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ . In this case  $\langle S \rangle$  is called an *infinite* cyclic group (cyclic because it is generated by one element). We have  $n = \underbrace{1 + 1 + \dots + 1}_{n \text{ times}}$ ,  $-n = \underbrace{(-1) + (-1) + \dots + (-1)}_{n \text{ times}} = -(\underbrace{1 + 1 + \dots + 1}_{n \text{ times}})$ .

Some more notation: if  $S = \{g\}$ , then  $\langle S \rangle = \langle g \rangle$  = cyclic group generated by  $g$ . Can see that different elements  $g$  can generate the same group.

Something with matrices ff (page 5).

$\phi \rightarrow \langle g \rangle$  is not injective. This means there are repeats  $g^i = g^j$   $i \neq j$ . WLOG  $i > j \Rightarrow g^{i-j} = 1$  and  $i - j > 0$ . Define  $d$  to be the smallest positive integer with  $g^d = 1$ . We call  $d$  the order of  $g$ . Claim:  $\langle S \rangle = \{1, g, g^2, \dots, g^{d-1}\}$

*Proof.* Fix any  $n \in \mathbb{Z}$ .  $fn = qd + r$  where  $0 \leq r \leq d - 1$ . We have

$$\begin{aligned} g^n &= g^{qd+r} = (g^{qd})g^r \\ &= (g^d)^q = g^r \\ &= (1)^q g^r \\ &= ff(\text{page 6}) \end{aligned}$$

If  $0 \leq r_1, r_2 \leq d - 1$ , let  $r_2 \geq r_1$  (WLOG) and  $g^{r_1} \neq g^{r_2}$  since  $g^{r_1} = g^{r_2} \iff g^{r_2-r_1} = 1$ , if  $r_1 \neq r_2$ . But  $d$  is the smallest positive integer with  $g^d = 1$ . So  $\{1, g, g^2, \dots, g^{d-1}\}$  represent all powers of  $g$ , with no repeats.  $\square$

Multiplication rule:  $g^i g^j = g^{i+j}$ . Read exponents mod  $d$  (replace by remainder). Algebra rule  $g^d = 1, g^{-1} = g^{d-1}$ . On this case  $\langle g \rangle = \{0, 1, 2, \dots, d-1\}$  and all additions are taken mod  $d$ . All such groups with the same  $d$  are isomorphic.

In summary, if  $G$  is a group and  $g \in S$ , the cyclic subgroup generated by  $g$  is  $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\} \subseteq G$ . There are 2 cases:  $\langle g \rangle$  is infinite,  $\cong \mathbb{Z}$ , or  $\langle g \rangle$  is finite,  $\# \langle g \rangle = d$ , and is equal to  $\{1, g, g^2, \dots, g^{d-1}\}$ ,  $\cong$  integers mod  $d$ . This is commutative.

This was the simplest case, when only generated by 1 element. But what about when we generate from more than one element. Two generators can make something that is much more complex. For example,  $\sigma, \tau$  for  $D_n$ , and no longer commutative and no longer can just be represented as powers of a single element (doesn't have to be cyclic?).

*Remark 5.*  $\langle S \rangle = \langle g \rangle$  is described above. But if  $S = \{g_1, g_2\}$  it is not easy to relate to  $\langle g_1 \rangle$  and  $\langle g_2 \rangle$  to the subgroup generated by both elements.

## 2.3 Structure of Cyclic Groups

- Describe all possible generators: when is  $\langle g \rangle = \langle h \rangle$ ?
- Find all possible subgroups of  $\langle g \rangle$

Consider the infinite cyclic group  $\langle g \rangle \cong (\mathbb{Z}, +)$ . Suppose  $t \in \mathbb{Z}$  is a generator. Then any positive integer  $n$  is of the form

$$n = t + t + \dots + t$$

so  $t$  is a multiple of  $n$ . This is supposed to hold for all  $n \Rightarrow t = \pm 1$ . Thus,  $\pm 1$  are the only possible generator.

Subgroups: let  $H$  be any subgroup of  $(\mathbb{Z}, +)$ . Pick  $t \in H$  which is the smallest positive element. ( $t \in H \iff -t \in H$ , so positive elements exist.) Then  $t\mathbb{Z} \subseteq H$  ( $t\mathbb{Z} = \{t, t+t, \dots, -t, -t-t, \dots\}$ ). Our claim is that  $H = t\mathbb{Z}$ .

*Proof.* Suppose  $s \in H$ , then  $s = qt + r, 0 \leq r < t$ . Then  $qt \in H$  (as above). Then  $s - qt = r \in H$ , which is impossible, since  $t$  is the smallest positive element. Then  $H = t\mathbb{Z}$ .  $\square$

Thus, subgroups of  $\mathbb{Z}$  are the set  $t\mathbb{Z}, t \in \mathbb{Z}$  (positive  $t$ ).

Now we consider the finite case  $\langle g \rangle = \{1, g, g^2, \dots, g^{d-1}\} \cong \{0, 1, 2, \dots, d-1\}$  with addition mod  $d$ . Fix  $t, 0 \leq t \leq d-1$  that generates, which means  $\{0, t, 2t, \dots, (d-1)t\} \equiv_{\text{mod } d} \{0, 1, 2, \dots, d-1\}$ .

For example,  $d = 5$ . Now let  $t = 2$ . We have  $\langle 2 \rangle = \{0, 2, 4, 6, 8\} = \{0, 1, 2, 3, 4\}$  so  $\langle 2 \rangle = \langle 1 \rangle$  in integers mod 5. (The fact that 5 is prime is what makes this work, makes it cyclic; can't have a cycle sit within a group.) But if  $d = 6$ ,  $\langle 2 \rangle = \{0, 2, 4, 6\} = \text{ff}(\text{page 12})$ .

Answer???:  $\langle t \rangle$  generates  $\iff (t, d) = 1$ .

*Proof.* Suppose  $(t, d) = s > 1$ . Then  $c = \frac{d}{s}$  is an integer,  $0 < c < d$ . Then  $ct = t + t + \dots + t$   $c$  times.  $\frac{d}{s}t = d \frac{t}{s} = d$ , integer is divided by  $d$ . Thus  $[ct] = [0]$  ( $ct$  is a multiple of  $d$ .  $0, t, 2t, \dots, dt$  is not distinct mod  $d$ ,  $[ct] = [0], c < d$ . Thus, if there's a common factor, can't generate.

It remains to show that if  $(t, d) = 1$ , then  $t$  generates. Assume  $(t, d) = 1$ . Find the smallest integer  $s$  such that  $[st] = [0]$ . This is obviously  $s = d$ , because  $st$  is divisible by  $d$ , so  $d \mid s$  since  $(t, d) = 1$ . Thus,  $0, t, 2t, \dots, (d-1)t$  are distinct (can't have overlaps, the multiples of  $t$  are smaller than  $d$ , same argument as before).

Conclusion: possible generators in this case are the integers  $t, 0 \leq t \leq d-1$  with  $(t, d) = 1$ . Multiplicative rotation  $g^t$  is a generator of  $\langle g \rangle \iff (t, d) = 1$ . Lots of choices for generators.  $\square$

Something something this is used in a cryptography scheme.

Still don't know how many open groups??? Strongly recommend reading this section before next class.

## 3 September 26

Last time, we were talking about cyclic groups/subgroups.  $G$  is a group,  $g \in G$ , then there are two cases for the subgroup generated by  $g$   $\langle g \rangle = \{g^t \mid t \in \mathbb{Z}\}$ .

- $\langle g \rangle$  is infinite

(b).  $\langle g \rangle$  finite,  $\# \langle g \rangle = d$

Terminology  $\# \langle g \rangle$  = the order of  $g$  (can be infinite or  $d$ ). This defines the order of  $g, g \in G$ .

*Remark 6.*  $\#G$  = order of  $G$ , but  $\# \langle g \rangle$  = order of  $g$  (as an element). Usually context will distinguish which one we're talking about. These only coincide when  $G = \langle g \rangle$  (group generated by  $g$ ).

Observation:  $g^m = g^l \iff g^{ml} = g^0 = 1$ . Any repeat  $g^m = g^l$  can be assumed to have  $l = 0$ . ???

Back to last class: we were trying to find all subgroups of  $\langle g \rangle$  when  $\# \langle g \rangle = d < \infty$ . Let  $G = \langle g \rangle$  and let  $H \subseteq G$  be any subgroup. Let  $t$  be the smallest positive integer with  $g^t \in H$ . We have  $0 \leq t \leq d - 1$ . Our claim is that  $H = \langle g^t \rangle$ .

*Proof.* The proof is the same as the infinite order case. If  $h \in H$  then  $h = g^s$  for some  $0 \leq s \leq d - 1$ . We have  $s = qt + r$ ,  $0 \leq r < t$ . Then  $h = g^s = g^{qt+r} = (g^t)^q g^r$ . But  $h \in H$  and  $g^t \in H$ , so  $g^r \in H$ . But this contradicts the minimality of  $t$  unless  $r = 0$  ( $r < t$ ). Thus  $s = qt \implies h = g^s = (g^t)^q \in \langle g^t \rangle$ .  $\square$

**Corollary 1.** Any subgroup  $H \subseteq G = \langle g \rangle$  is cyclic,  $H = \langle g^t \rangle$ .

We might ask what the order of  $H = \langle g^t \rangle$  is. The answer is

$$\frac{\#G}{\gcd(\#G, t)} = \frac{d}{(d, t)}$$

Last time, we computed the order of  $g^t = \frac{d}{(d, t)}$ . Recap: the order of  $g^t$  is the smallest positive integer  $s$  such that  $(g^t)^s = 1 \implies g^{ts} = 1 \implies d \mid ts$  ( $d$  is the order of  $g$ ). But then  $s$  is the smallest number such that  $d$  divides  $ts$ , and then  $s = \frac{d}{(d, t)}$ .

After a while, people just take these kind of operations for granted, because it is quite tedious to go through details. Need to be able to prove yourself or hold in your head.

**Corollary 2.**  $\text{order}(H) = \#H = \frac{d}{(d, t)}$  is a divisor of  $d = \#G$ . Then  $H \subseteq G \implies \#H \mid \#G$ .

This is a nice property of all finite groups (not just cyclic), but we will prove this later.

**Corollary 3.**  $G$  is cyclic,  $s \mid d \implies$  there exists a unique  $H \subseteq G$  of order  $S$ .

*Proof.* Existence: take  $H = \langle g^t \rangle, t = \frac{d}{s}$ . For uniqueness, do similar to what we showed before: given  $H \subseteq G, H = \{1, g^t, g^{2t}, \dots, g^{(r-1)t}\}$ , we have  $r$  is the order of  $h = g^t$ . We can read off elements of  $G$  from  $t$ . The order of  $H$  determines  $t$ , since  $rt = d$  ( $t = \frac{d}{r}, r = \#H$ ). Thus  $H$  is determined by  $\#H$ .  $\square$

*Remark 7.* This fails for most groups:  $G$  does not have subgroups of order  $r$  when  $r \nmid \#G$ . This is a unique property of cyclic groups: when we pick some divisor of the order of  $G$ , we are going to get a subgroup of order of that divisor.

You have to remember these basic facts about cyclic groups. We'll be using it a lot: we often try to understand the behaviour of a larger group by understanding cyclic subgroups of it, like with the dihedral group  $D_n$ , where we have a cyclic subgroup of order 2, and of order  $n$ .

### 3.1 Using our cyclic group properties for finite groups

Some terminology: the *exponent* of a group is the smallest positive integer  $n$  such that  $g^n = 1, \forall g \in G$  (not typically the order).

**Theorem 2.** Suppose  $G$  is commutative. Then  $G$  is cyclic  $\iff \text{exponent}(G) = \text{order}(G)$ .

This is good for a lot of stuff that we won't actually get to in this class, but the proof is a good test of understanding. Proof requires two lemmas.

**Lemma 1.** Suppose  $g, h$  are elements of a commutative group and let  $m = \text{order}(g)$  and  $n = \text{order}(h)$ . Then  $(m, n) = 1 \implies \text{order}(gh) = mn$ .

Example of failing with no commutativity: take  $D_n$ , and  $\sigma$  is a rotation and  $\tau$  is a reflection. Then  $\sigma\tau$  is also a reflection, but this has order 2 (regardless of order of  $\sigma$ ).

*Proof.* Suppose  $(gh)^r = 1 \implies g^r h^r = 1$  (commutativity). So  $g^r = h^{-r} = (h^{-1})^r$ . Note that  $\text{order}(g^r)$  divides  $\text{order}(g) = m$  and  $\text{order}(h^{-r})$  divides  $\text{order}(h) = n$ . (Using property of cyclic groups!) But since  $m, n$  were coprime,  $\text{order}(g^r) = \text{order}(h^{-r}) = 1$ . And  $\frac{m}{(m,r)} = 1$  so  $m \mid r$  and  $n \mid r$ , thus  $mn \mid r$  (coprimeness).

So  $(gh)^r = 1 \implies r$  is divided by  $mn$ . It is clear that  $(gh)^{mn} = (g^{mn})(h^{mn}) = 1$ . Thus  $n = \text{order}(h), m = \text{order}(g)$ , therefore  $(gh)^r = 1 \iff mn \mid r \implies gh$  has order  $mn$ .  $\square$

(proof also on page 47)

**Lemma 2.**  $G$  is commutative and finite. Suppose  $g \in G$  has maximal order. Then  $\text{exponent}(G) = \text{order}(g)$ .

*Remark 8.* Suppose  $g_2$  is any element of  $G$ . Our assumption is that  $\text{order}(g_2) \leq \text{order}(g)$ . Have to show  $g_2^{\text{order}(g)} = 1$ . ( $\text{order}(g)$  is killing off every element. This is not automatic: just because order is smaller, it does not follow that being raised to the power of a larger order means it will go to 1.

*Proof.* Let  $n = \text{order}(g)$  and  $m = \text{order}(g_2)$  (random element). We have  $n = \prod p_i^{e_i}$  (prime factorization) and  $m = \prod p_i^{f_i}$  (using same  $p_i, e_i, f_i \geq 0$ ). It is enough to show that  $f_i \leq e_i \forall i$  (then  $m \mid n$ ). (Will show this with commutativity.)

Suppose that it is not that case, by renumbering,  $f_1 > e_1$ . Now  $g$  has order  $n = \prod p_i^{e_i} = p_1^{e_1} \left( \prod_{i \geq 2} p_i^{e_i} \right) = p_1^{e_1} r$  and  $g_2$  has order  $m = \prod p_i^{f_i} = p_1^{f_1} \left( \prod_{i \geq 2} p_i^{f_i} \right) = p_1^{f_1} s$ . Let  $g_3 = g^{p_1^{e_1}}$  and  $g_4 = g_2^s$ . Note  $\text{order}(g_3) = r = \frac{\text{order}(g)}{(g, p_1^{e_1})} = \frac{n}{p_1^{e_1}}$ . and  $\text{order}(g_4) = p_1^{f_1}$  (for the same reason). But then by Lemma 1,  $\text{order}(g_3 g_4) = p_1^{f_1} r > \text{order}(g)$  (coprime because primes are different), which is a contradiction.  $\square$

Clever, but a typical argument in group theory... reread until you get the argument. No standard proof technique in group theory, but will use a bunch of properties of specific groups, and combine the facts to get the theorem that we wanted.

Additional property of finite cyclic groups: suppose  $g = \langle g \rangle$ ,  $\#G = d$ . Pick  $s \mid d$ ,  $\exists H \subseteq G$ ,  $\#H = s$ . Fact:  $H = \{x \in G \mid x^s = 1\}$ .

*Proof.* We can easily see that  $H$  is a subgroup (as defined). So it suffices (by uniqueness) to show it has order  $S$ . The elements of  $G = \langle g \rangle$  are  $1, g, g^2, \dots, g^{d-1}$ . The order of  $g^t$  is  $\frac{d}{(d,t)}$ .

$$(g^t)^s = 1 \implies d \mid ts$$

$t = 0, \frac{d}{s}, \frac{2d}{s}, \dots$  is a list of elements satisfyin  $x^s = 1$ , we have  $S$  of them.  $\square$

## 4 September 28

ff

## 5 October 3

"Point-set topology has got to be one of the most boring subjects ever. After about two weeks, you get the point."

We are now hitting the core stuff in the class.

## 5.1 Section 1.7

Let  $G$  be a group and  $X$  be a set.  $S = S_X =$  group of permutations of  $X$  (saying in this way because if  $X$  is not finite, bijections, and if it is finite, just  $S_X = S_n$ ).

**Definition 4** (Group Action). Suppose  $\exists \phi: G \rightarrow S_X$  (a homomorphism). Then  $\forall g \in G, \phi(g) \in S_X$  is a permutation, so  $\forall g \in G, \forall x \in X, \phi(g)(x) = y \in X$ . So we get a function  $(g, x) \rightarrow y = \phi(g)(x) = g \cdot x$  (short-hand). We say that  $G$  acts on  $X$ ; the elements of  $G$  move the elements of  $X$  around, according to the homomorphism  $\phi$ .

For example, if  $X = G, \phi(g) = Lg, x \mapsto gx$  (Cayley's theorem).

**Definition 5** (Orbit). Fix  $x \in X$ . Define  $\text{orbit}_G(x) = \text{orb}_G(x) = \{y \in X : \exists g \text{ with } \phi(g)(x) = y\}$

In words:  $\text{orb}_G(x) \subseteq X$ , elements we can reach via permutationns from  $\phi(G) \subseteq S_X$ . For example (Cayley's theorem),  $\text{orb}_G(1) = G$ , since  $\forall g \in G, Lg(1) = g \cdot 1 = g$ .

$X$  is divided up into  $G$ -orbits, these orbits carry lots of information (about  $G$ !), pretty fundamental for understanding the structure of a group (have to choose good maps  $\phi$  and sets  $X$ ). Will look at a lot later.

Today, we are only interested in one example:

$$\phi: G \rightarrow S_G = \text{permutations of } X : g \rightarrow Lg$$

and

$$\psi: G \rightarrow S_G = \text{permutations of } X : g \rightarrow Rg^{-1}$$

(where we've put the inverse to make it a homomorphism).  $\phi, \psi$  give injective maps  $G \hookrightarrow S$  (hook is injection).

**Definition 6** (Left Coset).  $H \subseteq G$  be any subgroup, can restrict  $\phi, \psi$  to  $H$  and get  $H \hookrightarrow S = S_G$  (permutations of  $G$ ). Consider  $g \in G, \text{orb}_H(g)$  under  $\phi$ . Define  $Hg = \{L_h(g), h \in H\} = \{hg \mid h \in H\}$ . This is called a coset of  $g$  with respect to  $H$  (or a coset of  $H$  with respect to  $g$ ).

(naming depends on  $g$  wrt  $H$  or the other way ff)

**Definition 7** (Right Coset). Take  $\psi$  instead;  $gH = \text{orb}_H(g) = \{gh^{-1} \mid h \in H\} = \{gh \mid h \in H\}$ . This is the right coset of  $H$ .

Warning: sometimes left/right get swapped.

**Remark 9.**  $gH \neq Hg$  in general

**Lemma 3.** The function  $h \mapsto gh$  and  $h \mapsto hg$  give bijections  $H \rightarrow gH$  and  $H \rightarrow Hg$ .

*Proof.*  $gh = gh' \implies h = h'$  (multiplication by  $g^{-1}$  on left). Onto is obvious. (or if  $H$  is finite  $\#H = \#gH = \#Hg$   $\forall g$ ).  $\square$

**Lemma 4.**  $G = \sqcup_{g_i} g_i H = \sqcup_{g'_i} H g'_i =$  disjoint union of cosets. (what is  $g'$  ?fff)

*Proof.*  $\forall g \in G, g \in gH$  and  $g \in Hg$ . So  $G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg$ .

Observation:  $g_1, g_2 \in G$ , either  $g_1 H = g_2 H$  or  $g_1 H \cap g_2 H = \emptyset$ . If we assume this observation, we are done. This is because  $G =$  disjoint union of distinct cosets. If we prove this observation, we prove the lemma.

Suppose  $g_1 H \cap g_2 H \neq \emptyset$ .  $\exists h_1, h_2 \in H$  with  $g_1 h_1 = g_2 h_2$ . Then  $g_1 = g_2 h_2 h_1^{-1} \in g_2 H$ . Then  $\forall h \in H, g_1 h \in g_2 H$  ( $H$  is closed). But then  $g_1 H \subseteq g_2 H$ , and by symmetry,  $g_2 H \subseteq g_1 H$ . thus  $g_1 H = g_2 H$ .  $\square$

**Corollary 4.**  $G = \sqcup_{g_i} g_i H = \sqcup_{g'_i} H g'_i$ , and each coset has the same cardinality. This means that if  $G$  is finite,  $\#G = r \cdot \#H$  (where  $r$  is the number of cosets). In particular,  $\#H \mid \#G$  and  $r$  is the index of  $H$  in  $G$  (number of distinct cosets).

This gives us the following theorem.

**Theorem 3** (Lagrange's theorem). If  $G$  is finite and  $H$  is a subgroup  $\implies \#H \mid \#G$ .

This means that orders of subgroups can't be random. They have to divide the order of the original group. (Evan Chen: any element's order must divide the order of  $G$ ).

**Remark 10.** The converse is false: if  $d \mid \#G$ , there need not be a subgroup of order  $d$ . Examples are hard to come by, but can find.

Notation:  $[G:H]$  = index of  $H$  in  $G$  = the number of distinct cosets of  $H$  (left or right, depending on what we're looking at). These values are the same for finite groups because  $[G:H] \cdot \#H = \#G$  ( $\#H$  is the size of a coset, which is the same whether it's a left coset or right coset).

Coset representatives: set of elements of  $G$ , one from each distinct coset. Example:  $G = \mathbb{Z}$ ,  $H = n\mathbb{Z}$ ,  $n > 1$ . Then the coset representatives are just the remainder classes,  $\{0, 1, 2, \dots, n-1\}$ , because the cosets are just  $x + kn, k \in \mathbb{Z} = x + H$  (additive notation).

We're taking a group, and we're cutting it up into pieces. All these pieces are of the same size, and they're all of size  $H$ .

Example:  $G = (\mathbb{Q}, +)$ ,  $H = \mathbb{Z}$ . Coset of  $x = \{x + k \mid k \in \mathbb{Z}\}$ . contains a unique  $r \in \mathbb{Q}, 0 \leq r < 1$ . Cosets represented by  $\{r \in \mathbb{Q}, 0 \leq r < 1\}$ .

$$\mathbb{Q} = \bigsqcup_{\substack{0 \leq r < 1 \\ r \in \mathbb{Q}}} \{r + k \mid k \in \mathbb{Z}\}$$

Cosets are a special case of equivalence classes: given  $G \supseteq H$ , define  $x \sim y$  to mean  $(x, y \in G) \iff \exists h \in H$  such that  $xh = y$ . Equivalence class  $[x] = xH$ . Can also define  $x \sim y \iff \exists h \in H, hx = y, [x] = Hx$ .

**Definition 8** (Quotient Map).  $G/H$  = set of cosets  $gH, g \in G$ , and  $H \backslash G$  = set of cosets  $Hg, g \in G$ . There exists unique functions  $\pi: G \rightarrow G/H$  or  $G \rightarrow H \backslash G$ , where  $g \mapsto gH, g \mapsto Hg$ .

Start with any  $G$  finite,  $H \subseteq G$  where  $H = \langle g \rangle, g \in G$ .  $\#H = \text{order}(g) < \infty$ . Lagrange's tells us that  $\#H \mid \#G \implies \text{order}(g) \mid \#G \forall g \in G$ , thus  $g^{\#G} = 1$  for all  $g \in G$ . Thus the  $\exp(G)$  is  $\leq \#G$ . This implies Lagrange's for cyclic groups, but not otherwise. (really?)

## 5.2 1.8

Is  $G/H$  (or  $H \backslash G$ ) a group in a natural way? "natural" means  $\pi: G \rightarrow G/H$  should be a homomorphism. The answer in general is no. This only works for special  $H$ , called a *normal* subgroups of  $G$ .

Reason: fix  $g_1, g_2 \in G$ .

$$\begin{aligned} \pi(g_1) &= g_1H \in G/H \\ \pi(g_2) &= g_2H \\ \pi(g_1g_2) &= (g_1g_2)H \end{aligned}$$

If it is a homomorphism, we have to have

$$\pi(g_1g_2) = \pi(g_1)\pi(g_2)$$

but

$$\pi(g_1g_2) = g_1g_2H = (g_1H) \cdot (g_2H)$$

where this multiplication (if it exists) is in  $G/H$ . Problem: this is not a well-defined multiplication of cosets. Explicitly: the rule is given 2 cosets  $X, Y \in G/H$ ,  $X \cdot Y = Z$  is defined by choosing representatives  $g_1 \in X, g_2 \in Y$ , setting  $Z = [g_1g_2]$ . Point: different choices of  $g_1, g_2$  in  $X, Y$  will produce different  $Z$ 's!

Example: pick  $X = [g], Y = [g^{-1}], Z = [gg^{-1}] = [1] = H$ . Now we change  $g$  with  $gh \in gH$  (this is a different representative of the same coset). Now we get  $z = [ghg^{-1}] \neq H = [1]$ . In general,  $ghg^{-1} \notin H$  (can't commute  $h$  and  $g$ ). We need some further conditions on  $G$  to make this work out, we need  $ghg^{-1} \in H$ . This leads us to the definition of a normal subgroup.

**Definition 9** (Normal Subgroup).  $H \subseteq G$  is a *normal* subgroup if  $\forall g \in G, \forall h \in H, ghg^{-1} \in H$ .

**Theorem 4.** If  $H$  is a normal subgroup, then  $G/H = H \backslash G$  and the maps  $G \rightarrow G/H$  and  $G \rightarrow H \backslash G$  are homomorphisms.

In this case, write  $G/H = H \backslash G$  (normally only use the first), called the *quotient* group of  $G \bmod H$ . Example: if  $G$  is commutative, all subgroups are normal ( $\mathbb{Z} \supseteq n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} = \text{integers mod } n$ ).

Will do the proof of the theorem next time. For next time, read the relevant section in the text. The presentation is a bit more elaborate than needed, but really going through the conditions for it to be a homomorphism (what we did with the  $X, Y, Z$ ).



## 6 October 5

Changing order a little from textbook. ff I completely missed the first page.

Question: can we make  $G/H$  or  $H \backslash G$  a group such that  $\pi$  is a homomorphism? Answer: no, necessary condition  $\forall g \in G, h \in H, ghg^{-1} \in H$  (\*). Reason: definition of  $\pi$  is  $\pi(x_1x_2) = x_1x_2H$ ,  $\pi(x_1) = x_1H$ ,  $\pi(x_2) = x_2H$ .

$\pi$  is a homomorphism iff  $\pi(x_1, x_2) = \pi(x_1)$  ff

$G/H$  to be defined by

$$\pi(x_1)\pi(x_2) = (x_1H)(x_2H) = (x_1x_2)H = \pi(x_1x_2)$$

for all  $x_1, x_2$  (\*\*). This is not well defined unless (\*) holds. E.g.  $x_1H = (x_1h)H, \forall h \in H$ . But  $(x_1H)(x_2H) = (x_1hH)(x_2H) = (x_1hx_2)H \neq x_1x_2H$  since  $x_1hx_2H = x_1x_2H \iff x)1hx_2$ .

Hmm, I might just throw this lecture, I've already behind and doing piazzas.

Some notes about normal groups (end of page 6). Every group has normal subgroups, namely the identity and itself. A group that does not have any normal subgroups not these two are called simple.  $D_n$  and even permutations?? And alternating group? Galois theory says that there is a formula for the roots of an equation iff there is some condition on the normal subgroups.

This is the place where students start getting hopelessly lost, so make sure you know what everything is saying. The homomorphism theorems are like the IVT and MVT in calculus: once you introduce it, just going to use it quickly and without mention at times.

Any homomorphism will obey the picture (page 9). So knowing the kernel tells you a lot about the homomorphism. If you have a homomorphism, you can make a normal subgroup (the kernel), and if you have a normal subgroup, you make a homomorphism, kinda tricky because both direction... but saying that these are fundamentally the same thing.

Every point in the coset has exactly one image. The cosets are getting crunched into one image in the  $\phi$ .

Nike: Understanding of group theory isn't linear, it goes from being mystical to being obvious. It's like a step function. Grades normally go up as the term goes on.

Today has mostly been 1.8 and 1.9. Really suggest reading it.

Herstein is extremely user friendly, and students tend to like it in the beginning. Dummit and Foote is good, but it's a word salad. They take complicated things... he thinks it's really hard to find anything. Jacobson is a little abstract and terse, but you will come to appreciate.

Next section is on fundamental theorem of homomorphisms, 1.10. Would suggest pre-reading it. There's a lot of notation, really need to see it a little before. Make sure you understand 1.8, 1.9, but 1.10 might be a bit rough. Midterm will be whatever we cover up to a week before.

## 7 October 10

Midterm 1: Thursday, next week, up to and including 1.10.

Recall last time: homomorphisms and quotients.

$$G_1 \xrightarrow{\phi} G_2$$

$K = \text{kernel}(\phi) = \ker(\phi) = \phi^{-1}(1_{G_2})$ .  $K$  is a normal subgroup,  $G_1/K \cong \phi(G_1) \subseteq G_2$ . We saw (draw picture ff page 1).

**Corollary 5.** If  $\phi$  is surjective,  $\phi(G_1) \cong G_1/K$ .

Notation (exact sequence):  $G$  group  $K \subseteq G$  normal.  $1 \rightarrow K \rightarrow G \xrightarrow{\pi} G/K \rightarrow 1$  means the image of each group on the left of the arrow is the kernel of the next map (arrows are homomorphisms).  $1 \rightarrow K$  subset (is injective) and  $K \rightarrow G$  subset (injective). (Yoo it's like the thing Sebastian drew for the de Rham cohomology). Some clarity: can draw  $G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3$ , means that  $\phi_1(G_1) = \ker(\phi_2(G_2))$ .

The point is  $G$  is "built" from  $K, G/K$ . Our goal is to study  $G$  by analysing the smaller pieces  $K, G/K$ . Answer (partial): fundamental theorems.

The first fundamental theorem relates subgroups of  $G/K$  with certain subgroups of  $G$ . Note that this numbering is specific to Jacobson.

**Theorem 5** (First Fundamental Theorem (Part a)). *Construction:*  $H \subseteq G/K$  a subgroup.  $\pi^{-1}(H) = H' \subseteq G$ . Then  $H \leftrightarrow H'$  is a bijective correspondence between subgroups of  $G/K$  and subgroups of  $G$  which contain  $K$ .

*Proof.* Note that since  $H$  is a subgroup of  $G/K$ ,  $\pi^{-1}(H) = H' =$  subgroup of  $G$ , contains  $K$ . Want to show bijection, so show  $\pi^{-1}$  has an inverse.??? If  $H'$  is a subgroup of  $G$  containing  $K$ , then  $H = \pi(H')$  and is a subgroup of  $G/K$ . We are going from subgroups of  $G$  that contain  $K$  to subgroups of  $G/K$ . Note that this is the inverse of the previous function,  $\phi(\phi^{-1}(x)) = x, \forall x \in G/K$ . Thus  $H \xrightarrow{\text{preimage}} H' \xrightarrow{\pi} H$  follows. For a bijection, have to check inverse on the other side as well. So start with  $H' \supseteq K$ , subgroup of  $G$ . Send to  $H = \pi(H')$ , take preimage. Do we get  $H'$  back? Recall  $\pi: G \rightarrow G/K, x \mapsto xK$ . So  $\pi^{-1}(\pi(x)) = xK \subseteq G$  (the whole coset). Thus, for any  $x \in G$ ,  $\pi(x) = xK$ ,  $\pi^{-1}(\pi(x)) = \pi^{-1}(xK) = xK \subseteq G = \{xk \mid k \in K\}$ . Thus  $\pi^{-1}(\pi(H')) = \{h'k \mid k \in K, h' \in H'\} =$  union of cosets coming from  $H' = H'$  since  $K \subseteq H'$  by assumption.  $\square$

Really important to understand this. This is only part a in theorem 1, and will use alot.

**Corollary 6.** Assume that  $H' \supseteq K$ .

(a).  $H$  is normal in  $G/K \iff H'$  is normal in  $G$ .

(b). If so,  $(G/K)/H \cong G/H'$

Intuitively,  $G \supseteq H' \supseteq K$ , divide by  $K$  to get  $G/K$ , divide again by  $H = \pi(H')$ , this is the same as dividing by  $H'$  in one step.

Modding out by  $K$  squashes kernel to identity, and we do it twice (from  $G$  to  $G/K$  and then to  $(G/K)/H$ , or just  $G/H'$ ).

Example (Abelian setting where everything is normal):  $\mathbb{Z} \supseteq 2\mathbb{Z} \supseteq 6\mathbb{Z}$ . Here,  $G = \mathbb{Z}, H' = 2\mathbb{Z}, K = 6\mathbb{Z}$ .  $G/H' =$  cyclic of order 2.  $G/K =$  cyclic of order 6  $\supseteq$  a subgroup of  $H$  of order 3.  $\underbrace{(G/K)}_{\text{order 6}} / \underbrace{H}_{\text{order 3}}$  has order 2  $\cong \mathbb{Z}/H'$ .

Explicitly:  $G/K = \mathbb{Z}/6\mathbb{Z}$  are the cosets:  $\{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, \dots\}$ . We have  $\pi: x \mapsto x + 6\mathbb{Z}$ . We now have  $H = \pi(H') = \{0 + \mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$ . So then  $G/H' = \{0 + 2\mathbb{Z}, 1 + 2\mathbb{Z}\}$ . Again, to see this more explicitly, we have  $H = \{[0], [2], [4]\}$ , and  $[1] \in G/K$ , we have  $1 + H = [1], [3], [5]$ . So  $G/K = H \sqcup [1] + H$ . Could have just modded out by  $H'$  at the beginning (cutting group up into evens and odds).

*Proof.* (a). Is easy. Suppose  $H'$  is normal in  $G$ . This means that  $gH'g^{-1} \subseteq H' \iff gh'g^{-1} \in H' \forall g \in G, h' \in H'$ .

We have to show  $\pi(H') = H$  is normal in  $G/K$ . But note we have  $\pi(x)\pi(h')\pi(x)^{-1} = \pi(xh'x^{-1}) \in H$ , and since  $xh'x^{-1} \in H'$  and  $\pi(H') = H$ . Thus  $H'$  normal in  $G \implies H$  normal in  $G/K$ .

Conversely, given  $H$  normal in  $G/K$  and want  $H' = \pi^{-1}(H)$  is normal in  $G$ . By definition, this means  $\forall g \in G, h' \in H', gh'g^{-1} \in H'$ , which is true if and only if  $\pi(gh'g^{-1}) \in H$ . But recall that  $\pi(gh'g^{-1}) = \pi(g)\pi(h')\pi(g^{-1}) = (gK)(h'K)(gK)^{-1} \in H$  (elements of  $H$  are cosets). But by assumption,  $H$  is normal, so we are done.

(b). (Sketch) Consider  $G \supseteq H \supseteq K$  ( $K, H'$  both normal). Then  $H' \supseteq K$  means we can write  $H' = \sqcup h'_i K$ . Then each coset  $xH' = \sqcup xh'_i K$  ( $h'_i K \in H = \pi(H')$ ). So cosets of  $H'$  break up as cosets of  $K$ . Dividing by  $K$  and then by the image of  $H'$  turns out to be the same as first grouping according to cosets of  $K$ , then some of these cosets together to get cosets of  $H'$ .  $\square$