Last time $a, b \in \mathbb{Z}$ not both zero, then $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ where $d = \gcd(a, b)$. So $d = am + bn$ with $m, n \in \mathbb{Z}$. A consequence is then that if $c \mid a$ and $c \mid b$ then $c \mid d$ (since $c \mid am + bn$).

If p is prime and $p \nmid a$ then $\gcd(a, p) = 1$. Thus $1 = am + pn$, where $m, n \in \mathbb{Z}$. Also, $1 = am \mod p$ ($-am + 1 \in p\mathbb{Z}$). This implies that $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ is a group under multiplication (this in fact makes $\mathbb{Z}/p\mathbb{Z}$ a field).

This type of multiplicative group is often denoted by $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$ is a group under multiplication.

Definition .0.1

For any group G and any subgroup H define an equivalence relation on G by

$$g_1 \sim g_2 \iff g_1^{-1}g_2 \in H \iff g_1H = g_2H$$

It's a standard check that this is an equivalence relation. Furthermore the conditions above are equivalent as:

$$g_1^{-1}g_2 \in H \iff g_1^{-1}g_2H = H \iff g_2H = g_1H$$

Note how the condition $g_1^{-1}g_2 \in H$ matches the condition from modular arithmetic that $a = b \mod n$ provided that $-a + b \in n\mathbb{Z}$ (which we saw above).

Also note that $H \to gH$ given by $h \mapsto gh$ is a bijection. Further g_1H and g_2H are either equal or disjoint.

We now recall **??**

**

Extremely Useful Idea: Think of G as inducing permutations on G/H, the set of cosets of H, where $g \in G$ maps $g_1H \mapsto gg_1H$.

Corollary .0.1

If a group G has prime order then it is cyclic.

Proof. If $g \in G$ isn't 1_G then g generates a subgroup $\langle g \rangle$ of G. $|\langle g \rangle|$ divides the prime $|G|$, but $|\langle g \rangle|$ isn't one. Thus $|\langle g \rangle| = |G|$, so $\langle g \rangle = G$.

We now begin to relate groups to each other via particular nice types of functions.

Definition .0.2

A **homomorphism** $f : G_1 \to G_2$ between groups G_1, G_2 is a function such that

$$f(xy) = f(x)f(y)$$

for all $x, y \in G_1$.

Lemma .0.2

If $f : G_1 \to G_2$ is a homomorphism then $f(1_{G_1}) = 1_{G_2}$ and $f(g^{-1}) = f(g)^{-1}$.

Furthermore $f(G_1)$ is a subgroup of G_2.

Proof. We prove these by simple algebraic manipulation:

$$f(1_{G_1}) = f(1_{G_1} \cdot 1_{G_1}) = f(1_{G_1}) \cdot f(1_{G_1})$$
$$f(1_{G_1}) = 1_{G_2}$$

We also may write:

$$f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$$
$$f(g^{-1}) = f(g)^{-1}$$

The fact that $f(G_1)$ is a subgroup immediately follows, as it contains the identity, inverses, and is closed under multiplication 

Example .0.1

$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$, where $\mathrm{GL}_n(\mathbb{R})$ are the invertible matrices under multiplication and $\mathbb{R}^\times$ is the nonzero reals under multiplication.

$\exp : \mathbb{R}^+ \to \mathbb{R}^\times$, where $\mathbb{R}^+$ is the group of reals under addition. We also have $|\cdot| : \mathbb{C}^\times \to \mathbb{R}^\times$.

The trivial homomorphism $G_1 \to G_2$ which takes everything to 1, as $g \mapsto 1$.

We now generalize a definition from linear algebra that turns out to be extremely extremely useful.

Definition .0.3

Let $f : G_1 \to G_2$ be some homomorphism. Then define the **kernel** of f to be

$$\ker f \coloneqq \{g \in G_1 \mid f(g) = 1\}.$$

This will be a subgroup of G_1 (exercise!), and it will satisfy some very nice properties. Namely if $b \in \ker f$ and $a \in G_1$ then $aba^{-1} \in \ker f$.

$$f(aba^{-1}) = f(a)f(b)f(a)^{-1} = f(a)f(a)^{-1} = 1$$

Definition .0.4

Define a **normal subgroup** N of G to be a subgroup such that $gng^{-1} \in N$ for all $n \in N$ and $g \in G$. We notation this as $N \trianglelefteq G$.

So, if $f : G_1 \to G_2$ is a homomorphism then $\ker(f)$ is a normal subgroup of G_1. Later we will show the converse, if N is a normal subgroup of G then N is the kernel of some homomorphism $G \to \widetilde{G}$ (in fact, as a set $\widetilde{G} = G/N$).

If $f : G_1 \to G_2$ is a homomorphism, then

$$f(x) = f(y) \iff f(x)^{-1}f(y) = 1 \iff f(x^{-1})f(y) = f(x^{-1}y) = 1$$
$$\iff x^{-1}y \in \ker f \iff x\ker(f) = y\ker(f)$$

This implies that for any $g \in f(G_1)$, $\left|f^{-1}(g)\right| = |\ker(f)|$.

Corollary .0.3

For a group homomorphism f, f is injective if and only if $\ker(f) = \{1\}$.