Last time: • If $\gcd(a,b)=1$ then $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$

• $a^{\varphi(n)} \equiv 1 \bmod n$ if $\gcd(a,n)=1$

• An action of a group G on a set X is a function

$$a: G \times X \to X, \quad a(g,x) \equiv g \cdot x$$

so that 1) $e \cdot x = x \quad \forall x \in X$

2) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x, \quad \forall x \in X, \ \forall g_1, g_2 \in G$

Recall For any set X we have the set

$$\mathrm{Sym}(X) = \{ f: X \to X \mid f \text{ is invertible} \}$$

$\mathrm{Sym}(X)$ is a group with the group operation $\circ$ (composition) and $e_{\mathrm{Sym}(X)} = \mathrm{id}_X$, the identity map.

Lemma 18.1 Let G be a group and X a set. There is a bijection

$$\{ G \times X \xrightarrow{a} X \mid a \text{ is an action} \} \longleftrightarrow \{ \varphi: G \to \mathrm{Sym}(X) \mid \varphi \text{ is a homomorphism} \}$$

Proof Given a homomorphism $\varphi: G \to \mathrm{Sym}(X)$ define an action $a: G \times X \to X$ by

$$(g \cdot x =) a(g,x) = \varphi(g)(x) \quad \forall g \in G, x \in X$$

We check that a is an action.

Since φ is a homomorphism, $\varphi(e) = e_{\mathrm{Sym}(X)} = \mathrm{Id}_X$

$$\Rightarrow e \cdot x = (\varphi(e))(x) = \mathrm{id}_X(x) = x$$

Also since φ is a homomorphism $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$.

$$\Rightarrow g_1 \cdot (g_2 \cdot x) = \varphi(g_1)(\varphi(g_2)x) = (\varphi(g_1) \circ \varphi(g_2))(x)$$
$$= \varphi(g_1 g_2)(x) = (g_1 g_2) \cdot x$$

Conversely suppose we have an action $a: G \times X \to X$

For $g \in G$ define $\varphi(g): X \to X$ by $\varphi(g)x = g \cdot x$

We need to check: (i) $\varphi(g)$ is invertible $\forall g \in G$.

(ii) $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

For any $x \in X$, $\forall g \in G$

$$x = e \cdot x = (gg^{-1}) \cdot x = g \cdot (g^{-1} \cdot x) = \varphi(g)(\varphi(g^{-1})x)$$

$$\Rightarrow \quad \varphi(g) \circ \varphi(g^{-1}) = id_X$$

Similarly, $\varphi(g^{-1}) \circ \varphi(g) = id_X$

$\Rightarrow \varphi(g)$ is invertible, hence is in $Sym(X)$.

Since $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $x \in X$, $g_1, g_2 \in X$

$$\varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1 g_2)(x) \qquad \forall x \quad \forall g_1, g_2$$

$$\Rightarrow \varphi(g_1) \circ \varphi(g_2) = \varphi(g_1, g_2) \qquad \forall g_1, g_2.$$

$\Rightarrow \varphi$ is a homomorphism

Exercise Check that the two maps

$\{a : G \times X \to X \mid a \text{ is an action}\} \longrightarrow \{\varphi : G \to Sym(X) \mid \varphi \text{ homomorph}\}$

and $\{\varphi : G \to Sym(X)\} \longrightarrow \{a : G \times X \to X\}$

are inverses of each other. □

Remark. Goodman defines an action of a group G on a set X to be a homomorphism $\varphi : G \to Sym(X)$.

Definition Suppose a group G acts on a set X and $x \in X$. The orbit of x (for this action) is the set

$$\mathcal{O}(x) \equiv G \cdot x := \{g \cdot x \mid g \in G\}.$$

Ex $U(1)$ acts on $\mathbb{C}$ by complex multiplication:

$$e^{i\theta} \cdot z = e^{i\theta} z \qquad \forall e^{i\theta} \in U(1) \quad \forall z \in \mathbb{C}$$

$$S^1 \cdot z = \{e^{i\theta} z \mid e^{i\theta} \in U(1)\} = \{w \in \mathbb{C} \mid |w| = |z|\}$$

$$= \text{circle of radius } |z| \text{ centered at } 0$$

Ex Let G be a subgroup of a group H.

G acts on H by multiplication on the left:

$$G \times H \longrightarrow H, \quad g \cdot h = gh$$

(check that this is an action)

For $h \in H$, $G \cdot h = \{gh \mid g \in G\} = Gh$, the right coset of G through $h \in H$.

Lemma 18.2 Suppose a group G acts on a set X. Then the set of orbits $\{G \cdot x \mid x \in X\}$ is a partition of X:

$$\bigcup_{x \in X} G \cdot x = X \quad \text{and}$$

$$G \cdot x \cap G \cdot y \neq \emptyset \Rightarrow G \cdot x = G \cdot y$$

Proof Define a relation $\sim$ on X by $x_1 \sim x_2 \Leftrightarrow x_2 = g \cdot x_1$ for some $g \in G$. Then

(i) For any $x \in X$ $\quad e \cdot x = x \Rightarrow x \sim x$

(ii) If $x_2 = g \cdot x_1$ then $g^{-1} \cdot x_2 = g^{-1} \cdot (g \cdot x_1) = (g^{-1}g) \cdot x_1 = e \cdot x_1 = x_1$

So $x_1 \sim x_2 \Rightarrow x_2 \sim x_1$.

(iii) Suppose $x_1 \sim x_2$ and $x_2 \sim x_3$. Then $\exists\, a, b \in G$ s.t.

$$x_2 = a \cdot x_1, \quad x_3 = b \cdot x_2$$

$$\Rightarrow x_3 = b \cdot (a \cdot x_1) = (ba) \cdot x_1 \Rightarrow x_1 \sim x_3.$$

$\Rightarrow \sim$ is an equivalence relation.

Now, $\forall x \in X$, $[x] = \{x' \mid x \sim x'\} = \{x' \mid x' = g \cdot x \text{ for some } g \in G\}$

$$= \{g \cdot x \mid g \in G\} = G \cdot x.$$

$\Rightarrow$ equivalence classes of $\sim$ are G-orbits.

Equivalence classes & equivalence relations partition the set. $\Rightarrow$ orbits of a G-action partition X.

Definition A permutation $\tau \in S_n$ is a transposition if τ is a 2-cycle: $\tau = (i\,j)$ for some $i, j \in \{1, \ldots, n\}$.

We will show: There exists a homomorphism

$\text{sign}: S_n \longrightarrow \{\pm 1\}$

So that $\text{sign}(\tau) = -1$ for any transposition τ.