Quiz Friday on G/N, homomorphism theorem.

10/10/2018
We

17.1

Last time

1) Homomorphism (1st isomorphism) theorem:

Let $f: G \to H$ be a homomorphism, $N = \ker f$.

Then $\bar{f}: G/N \to H$, $\bar{f}(aN) = f(a)$ is a well-defined injective homomorphism.

Moreover $\bar{f}: G/H \to f(G)$ is an isomorphism.

---

2) If $f: K \to H$, $\ell: K \to G$ are two homomorphisms then

$f \times \ell: K \to H \times G$, $(f \times \ell)(k) = (f(k), \ell(k))$

is a homomorphism.

Ex Suppose $a, b \in \mathbb{N}$, $\gcd(a,b) = 1$.

Then $\mathbb{Z}_{ab}$ is isomorphic to $\mathbb{Z}_a \times \mathbb{Z}_b$.

Proof $f: \mathbb{Z} \to \mathbb{Z}_a$, $f(n) = [n]_a$, $\ell: \mathbb{Z} \to \mathbb{Z}_b$, $\ell(n) = [n]_b$

are homomorphisms

$\Rightarrow$ $f \times \ell: \mathbb{Z} \to \mathbb{Z}_a \times \mathbb{Z}_b$, $(f \times \ell)(n) = ([n]_a, [n]_b)$

is a homomorphism.

$\ker(f \times \ell) = \{ n \mid [n]_a = [0]_a \text{ and } [n]_b = [0]_b \}$

$= \{ n \mid a \mid n \text{ and } b \mid n \}$

Now $a \mid n \Rightarrow n = qa$ for some $q \in \mathbb{Z}$

$b \mid (qa)$ and $\gcd(b, a) = 1 \Rightarrow b \mid q$

$\Rightarrow q = bm$ for some $m \in \mathbb{Z}$. $\Rightarrow n = (ab) \cdot m$

Thus $\ker(f \times \ell) = ab\mathbb{Z}$

Homomorphism theorem $\Rightarrow$

$\overline{f \times \ell}: \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$

$(\overline{f \times \ell})([n]_{ab}) = ([n]_a, [n]_b)$

is a well-defined injective homomorphism.

Now $|\mathbb{Z}_{ab}| = ab = |\mathbb{Z}_a| \, |\mathbb{Z}_b| = |\mathbb{Z}_a \times \mathbb{Z}_b|$

$\Rightarrow$ $\overline{f \times \ell}$ is also onto hence an isomorphism.

In particular, given $[x]_a \in \mathbb{Z}_a$ and $[y]_b \in \mathbb{Z}_b$ there is a unique $[z]_{ab} \in \mathbb{Z}_{ab}$ so that

$$[z]_a = [x]_a \quad \text{and} \quad [z]_b = [y]_b.$$

We can restate above discussion as:

Chinese Remainder / Sun Tzu, theorem: given $a, b \in \mathbb{N}$ with $\gcd(a,b)=1$, and given integers x, y there is an integer z so that

$$z \equiv x \bmod a \quad \text{and} \quad z \equiv y \bmod b.$$

Moreover, if $z' \equiv x \bmod a$ and $z' \equiv y \bmod b$ then $(z - z') \equiv 0 \bmod ab$ (or $z \equiv z' \bmod ab$)

Euler's theorem

Recall: i) $[k] \in \mathbb{Z}_n$ is a unit if there is $[\ell] \in \mathbb{Z}_n$ s.t.

$$[k][\ell] = [1]$$

ii) $[k] \in \mathbb{Z}_n$ is a unit $\iff \gcd(k,n) = 1$.

Lemma 17.1 The set $\mathbb{Z}_n^\times := \{[\ell] \in \mathbb{Z}_n \mid [\ell] \text{ is a unit}\}$ is a group under the multiplication in $\mathbb{Z}_n$.

Proof Since $[1] \in \mathbb{Z}_n^\times$, $\mathbb{Z}_n^\times$ has a (multiplicate) identity.

If $[\ell] \in \mathbb{Z}_n^\times$ $\exists$ $[k] \in \mathbb{Z}_n^\times$ s.t. $[k][\ell] = [1]$.

So $[k] = ([\ell])^{-1}$.

Finally we need to check that if $[k], [k'] \in \mathbb{Z}_n^\times$ then $[k]\cdot[k'] \in \mathbb{Z}_n^\times$ as well.

Since $[k], [k'] \in \mathbb{Z}_n^\times$, $\exists [\ell], [\ell'] \in \mathbb{Z}_n^\times$ s.t. $[k][\ell] = [1]$ and $[k'][\ell'] = [1]$. Then

$$[k][k'][\ell'][\ell] = [1]. \Rightarrow [k][k'] \in \mathbb{Z}_n^\times.$$

Def Euler φ function:

$$\varphi(n) = |\mathbb{Z}_n^\times| = \{k \in \mathbb{Z} \mid 0 \le k < n, \gcd(k,n) = 1\}$$

"Example" If p is prime $\mathbb{Z}_p^\times = \{[1], [2], \dots [n-1]\}$

So $\varphi(p) = p-1$.

$\mathbb{Z}_6^\times = \{[1], [5]\}$ So $\varphi(6) = 2$

and so on.

Euler's theorem Fix $n \in \mathbb{N}$. Suppose $a \in \mathbb{N}$ st $\gcd(a,n) = 1$.

Then $a^{\varphi(n)} \equiv 1 \bmod n$

We first prove:

Lemma 17.2 Suppose G is a finite group, $g \in G$. Then

$g^{|G|} = e$.

Proof By Lagrange's theorem $|G| = |G/\langle g\rangle|\,|\langle g\rangle|$.

Let $n = \langle g\rangle$. Then, as we have seen (last time)

$\mathbb{Z}_n \longrightarrow \langle g\rangle$, $[k] \longmapsto g^k$ is an isomorphism

In particular, $g^n = e$.

$$\Rightarrow \quad e = (g^n)^{|G/\langle g\rangle|} = \left(g^{|\langle g\rangle|}\right)^{|G/\langle g\rangle|} = g^{|G|}$$ ∎

Proof of Euler's theorem

By 17.2, $\forall\ [a] \in \mathbb{Z}_n^\times$, $\left([a]\right)^{|\mathbb{Z}_n^\times|} = [1]$ in $\mathbb{Z}_n$.

$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$.

And $\gcd(a,n) = 1 \iff [a] \in \mathbb{Z}_n^\times$. □

Group actions (ch 5 in Goodman)

Definition An action of a group G on a set X is a function $G \times X \to X$, $(g,x) \mapsto g \cdot x$

so that 1) $e \cdot x = x$ for all $x \in X$

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

Example $G = GL(2,\mathbb{R}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0\}$

$X = \mathbb{R}^2$

$GL(2,\mathbb{R}) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(A, \vec{v}) \mapsto A\vec{v}$ (mult. of $\vec{v}$ by A)

is an action.

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in $GL(2,\mathbb{R})$ and $I\vec{v} = \vec{v}$ $\forall\, \vec{v} \in \mathbb{R}^2$

$\forall\, A, B \in GL(2,\mathbb{R})$, $\forall\, \vec{v} \in \mathbb{R}^2$

$A \cdot (B \cdot \vec{v}) = (AB)\vec{v}$ (matrix multiplication)

Example A group G acts on itself ($X = G$) by conjugation

$G \times G \to G$, $g \cdot x := gxg^{-1}$

is an action.

Check 1) $e \cdot x = exe^{-1} = x$ ✓

2) $g_1 \cdot (g_2 \cdot x) = g_1 (g_2 x g_2^{-1}) g_1^{-1} = (g_1 g_2) x (g_2^{-1} g_1^{-1})$

$= (g_1 g_2) x (g_1 g_2)^{-1}$

$= (g_1 g_2) \cdot x.$

Ex $S^1 = \{\lambda \in \mathbb{C} \mid |\lambda| = 1\}$ acts on $\mathbb{C}$ by complex multiplication: $\lambda \cdot w = \lambda w$ (action; $*$ mult in $\mathbb{C}$)

Check 1) $1 \cdot w = 1w = w$ ✓

2) $\lambda_1 \cdot (\lambda_2 \cdot w) = \lambda_1 (\lambda_2 w) = (\lambda_1 \lambda_2) w = (\lambda_1 \lambda_2) \cdot w$ (mult. in S^1; action)

$D_n = \langle \rho, \tau \mid \rho(z) = e^{2\pi i/n} z,\ \tau(z) = \bar{z} \rangle$ acts on $\mathbb{C}$:

$(\rho^k \tau) \cdot z = \rho^k(\tau(z))$