Math 332, Thursday Feb 26

Today: * Chinese remainder thm
* class equation
* products

* Announce talk, concert

I. Chinese remainder thm. Suppose $n_1, \dots, n_k$ relatively prime integers.

Define

$$\varphi : \mathbb{Z}_{n_1 \cdots n_k} \longrightarrow \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

$$a \longmapsto (a \bmod n_1, \dots, a \bmod n_k)$$

Examples

$\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_6 \times \mathbb{Z}_5$

$\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Then φ is an isomorphism. To construct the inverse:

$\hat{n}_1 n_2 \cdots n_k$, $n_1 \hat{n}_2 n_3 \cdots n_k$, $n_1 n_2 \hat{n}_3 n_4 \cdots n_k$, $\dots$, $n_1 n_2 \cdots n_{k-1} \hat{n}_k$ have gcd $= 1$.

So $\exists\, l_1, \dots, l_k$ s.t. $\sum l_i (n_1 \cdots \hat{n}_i \cdots n_k) = 1$.

Define

$$\psi : \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \longrightarrow \mathbb{Z}_{n_1 \cdots n_k}$$

$$(a_1, \dots, a_k) \longmapsto \sum a_i l_i (n_1 \cdots \hat{n}_i \cdots n_k)$$

Example $\varphi : \mathbb{Z}_{30} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$$\boxed{-1}\, 3\cdot 5 + \boxed{1}\, 2\cdot 5 + \boxed{1}\, 2\cdot 3$$

$$\underset{15}{} \qquad \underset{10}{} \qquad \underset{6}{}$$

$$\varphi^{-1}(a_1, a_2, a_3) = -15\, a_1 + 10\, a_2 + 6\, a_3$$

$$\varphi(8) = (0,2,3), \qquad \psi\,(0,2,3) = -15\cdot 0 + 10\cdot 2 + 6\cdot 3 = 38 = 8.$$

In general It's easy to check φ, ψ are well-defined homomorphisms, $\varphi(1) = (1,\dots,1)$, $\psi(1,\dots,1) = \sum 1\cdot l_i (n_1 \cdots \hat{n}_i \cdots n_k) = 1$. So generators are sent to generators. (By lemmas in the text, we know these groups are cyclic, so this is enough since φ and ψ do the right thing to generators.)

II. Class equation

Let G act on itself by conjugation:

$$G \times G \to G$$
$$(g, h) \mapsto ghg^{-1}$$

$\mathrm{Stab}(h) = \{g \in G : ghg^{-1} = h\} = \{g \in G : gh = hg\}$

$= \{g \in G : g \text{ commutes with } h\} =: C(h) =$ centralizer of h

☆ This is a subgroup of G. [Check!]

$\mathrm{Orb}(h) = \{ghg^{-1} : g \in G\} =:$ conjugacy class of $h = \mathrm{conj}(h)$

$\mathrm{Fix}(g) = \{h \in G : ghg^{-1} = h\} = \{h \in G : h \text{ commutes with } g\} =$ centralizer of g

Orbit-stabilizer thm: If G is finite, for each $h \in G$, we have

$|G| = |\mathrm{Orb}(h)|\,|\mathrm{Stab}(h)| = (\#\text{ conjugates of } h) \times (\text{order of the centralizer})$

Stated another way: # of conjugates of h = index of the centralizer of $h = \dfrac{|G|}{|C(h)|}$.

Burnside's thm. If G is finite,

$$\#\text{ orbits} = \frac{1}{|G|}\sum_{g\in G} |\text{Fix}(g)| \Longrightarrow \#\text{ of conjugacy classes} = \frac{1}{|G|}\sum |C(g)|$$

Class equation

The dot signifies a disjoint union.

Partition G into disjoint conjugacy classes: $G = \bigcup_{i=1}^{t}\!\!\!\cdot\;\; \text{Conj}(g_i)$

By the orbit stabilizer theorem,

$$|G| = \sum_{i=1}^{t} |\text{Conj}(h_i)| = \sum_{i=1}^{t} [G : C(h_i)] = \sum_{i=1}^{t} \frac{|G|}{|C(h_i)|}$$

Note: $h \in \text{Center}(G) \iff |\text{Conj}(h)| = 1$ [$g^{-1}hg = h$ if h commutes with g]

So

$$\boxed{|G| = |\text{Center}(G)| + \sum_{i : |\text{Conj}(h_i)| > 1} [G : C(h_i)]}$$

The class equation.

Thm p prime, $n \in \mathbb{Z}_{>0}$. Let G be a group of order p^n. Then G has a nontrivial center.

Pf/ Class equation. Each $C(h_i)$ with $|\mathrm{Conj}(h_i)| > 1$ is a proper subgroup of G. So $[G : C(h_i)]$ is divisible by p.

Taking the class equation mod p gives

$$0 = |\mathrm{Center}(G)| + 0 \mod p,$$

and $1 \in \mathrm{Center}(G)$, so $|\mathrm{Center}(G)| \geq 1$.. $\square$

III. Products

Direct products

<u>Def</u> For each i in an index set I, let G_i be a group. The **direct product** of $\{G_i\}_{i\in I}$ is the Cartesian product $\prod_{i\in I} G_i$ with componentwise multiplication: for $f=(f_i)_{i\in I}$, $g=(g_i)_{i\in I}$ in $\prod_{i\in I} G_i$, $fg=(f_ig_i)_{i\in I}$.

(Sage: direct_product_permgroups)

Example: $\mathbb{Z}_4 \times S_3 = \{(0,1),(0,\rho),(0,\rho^2),\ldots,(3,\rho^2\phi)\}$

$$(2,\rho\phi)\cdot(1,\phi) = (2+1,\rho\phi\cdot\phi) = (3,\rho).$$

Projection mappings For each $j \in I$, we have the projection homomorphism

$$\pi_j : \prod_{i\in I} G_i \longrightarrow G_j$$
$$(g_i)_{i\in I} \longmapsto g_j$$

Example: $G_1 = \mathbb{Z}_4$, $G_2 = S_3$, $(2,\rho\phi) \in G_1 \times G_2$, $\pi_1(2,\rho\phi) = 2$, $\pi_2(2,\rho\phi) = \rho\phi$.

Universal property Suppose H is a group and $\phi_i : H \to G_i \ \forall i$.
Then $\exists!\, \phi : H \to \prod_{i\in I} G_i$ s.t. $\pi_i \circ \phi = \phi_i \ \forall i$.

$$\begin{tikzcd}
H \arrow[r, "\exists!\phi"] \arrow[dr, "\phi_i"'] & \prod_{i\in I} G_i \arrow[d, "\pi_i"] \arrow[dl, phantom, "\circlearrowright"] \\
& G_i
\end{tikzcd}$$

The ϕ that works:

$\phi(h) := (\phi_i(h))_{i\in I}$.

Direct sums (coproducts)

The direct sum of groups $\{G_i\}_{i \in I}$ is

$$\bigoplus_{i \in I} G = \{ (g_i)_{i \in I} : g_i = 1 \text{ for all but finitely many } i \} \leq \prod_{i \in I} G_i$$

* If I is finite, then $\bigoplus_{i \in I} G_i = \prod_{i \in I} G_i$.

Universal property (reverse the arrows in the universal property of the direct product)

$\exists$ inclusion homomorphisms $s_j : G_j \longrightarrow \bigoplus \prod_{i \in I} G_i$ for each j: $s(g)_i = \begin{cases} 1 & i \neq j \\ g & i = j \end{cases}$.

Given homomorphisms $\phi_i : G_i \to H$ $\forall i$, $\exists!\ \phi : \bigoplus G_i \to H$ such that $\phi \circ s_i = \phi_i$ $\forall i$.

$$\begin{tikzcd} H & \bigoplus_{i \in I} G_i \arrow[l, "\exists!\ \phi"'] \arrow[dl, phantom, "\circlearrowleft"] \\ & G_i \arrow[u, "s_i"'] \arrow[ul, "\phi_i"] \end{tikzcd}$$

$$\phi((g_i)_{i \in I}) = \prod_{i \in I} \phi_i(g_i)$$

This makes sense since $\phi_i(g_i) \neq 1$ only finitely often.