Week 10

Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if $\exists\ g \in G$ s.t. $gx_1 = x_2$. The $\sim$ is an equivalence relation. Each cell in $X/_\sim$ is an orbit and the orbit contains x is denoted by Gx.

Theorem Let X be a G-set and $x \in X$. Then $|Gx| = (G : G_x)$ where $G_x = \{g \in G \mid gx = x\}$. If $|G|$ is finite, then $|Gx| \mid |G|$.

Proof. Note that $G_x \leq G$. Define a mapping from the set G_x into the collection of left cosets of G_x in G by

$$\psi(y) = g_1 G_x \quad \text{where} \quad g_1 x = y.$$

(Note. Since Gx is an orbit contains x, $\forall\ y \in Gx$, $\exists\ g \in G$, s.t. $gx = y$.)

First, we claim ψ is well-defined. Suppose that $g_2 x = y,\ g_2 \in G$. Then $g_1 x = g_2 x$. Hence $(g_2^{-1} g_1)x = x,\ g_2^{-1} g_1 \in G_x$. This implies that $g_1 G_x$ and $g_2 G_x$ are the same coset.

To conclude the proof, we claim that ψ is 1-1 and onto. Since $\psi(y) = \psi(y')$, $g_1 G_x = g_2 G_x$ where $g_1 x = y$ and $g_2 x = y'$. By $(g_2^{-1} g_1)x = x$, we have $y = y'$.

Finally, let $g_1 G_x$ be a left coset. Clearly, $g_1 x \in Gx$ and $g_1 x = x_1 \in Gx$. By definition $\psi(x_1) = g_1 G_x$, hence ψ is 1-1 and onto. This implies that $|Gx| = (G : G_x)$. ■

Theorem (Burnside's Formula)

Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then $r \cdot |G| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$.

Proof. It suffices to prove $r \cdot |G| = \sum_{x \in X} |G_x|$.

Since G is finite, for each $x \in G$, $|Gx| = |G|/|G_x|$. Therefore, $|G_x| = |G|/|Gx|$

$\sum_{x \in X} |G_x| = \sum_{x \in X} |G|/|Gx| = |G| \cdot \sum_{x \in X} \frac{1}{|Gx|} = |G| \cdot r.$ ■

Remark More applications in counting can be found in combinations. We omit the detail here.

Subnormal and Normal Series

Defn. A subnormal series od a group G is a finite sequence H_0, $H_1,\ H_2, \cdots, H_n$ of subgroups of G such that $H_i \overset{\lhd}{\neq} H_{i+1}$ with $H_0 = \{e\}$ and $H_n = G$. A normal series of G is a finite sequence $\{e\} = H_0 < H_1 < H_2 < \cdots < H_n = G$ such that for each i, $H_i \lhd G$.

$(*)$ A normal series is also a subnormal series. $H_i \lhd G \Rightarrow H_i \lhd H_{i+1}$.

Examples $\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$: Normal series

$\{0\} < 9\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$: Normal series

$\{\rho_0\} < \{\rho_0, \mu_1\} < \{\rho_0, \rho_2, \mu_1, \mu_2\} < D_4$: Subnormal series.

($\{\rho_0, \mu_1\}$ is not normal in D_4)

Defn. A subnormal(normal) series $\{K_j\}$ is a refinement of a subnormal(normal) series $\{H_i\}$ of a group G if $\{H_i\} \subseteq \{K_j\}$.

Example $\{0\} < 72\mathbb{Z} < 12\mathbb{Z} < \mathbb{Z}$

$\Downarrow$ refinement

$\{0\} < 144\mathbb{Z} < 72\mathbb{Z} < 36\mathbb{Z} < 12\mathbb{Z} < 3\mathbb{Z} < \mathbb{Z}$

Defn. (Composition series)

A subnormal series $\{H_i\}$ of a group is a composition series if all the factor groups H_{i+1}/H_i are simple. A normal series $\{H_i\}$ of G is a principal series if all the factor groups H_{i+1}/H_i are simple.

Fact $\mathbb{Z}$ has no composition series and also no principle series.

Proof. Let $\{0\} = H_0 < H_1 < H_2 < \cdots < H_n = \mathbb{Z}$ be a subnormal series. Then $H_1 = r\mathbb{Z}$ for some positive integer r. Since $H_1/H_0 = r\mathbb{Z}$ which is not simple. $\{H_i\}$ is not a composition series. $\{H_i\}$ is not a principle series follows by same reason. ■

Fact For $n \geq 5$, $\{e\} < A_n < S_n$ is a composition series.

Proof. $S_n/A_n \cong \mathbb{Z}_2$ (simple) and $A_n/\{e\} \cong A_n$ (simple for $n \geq 5$). ■

Defn. (Solvable group)

A group is solvable if it has a composition series $\{H_i\}$ such that all factor groups H_{i+1}/H_i are abelian.

Proposition The group S_5 is not solvable.

Proof. Since A_5 is not abelian and $\{e\} < A_5 < S_5$ is a composition series of S_5, S_5 is not solvable. (Note that all composition series of a group G are isomorphic by Jordan-Hölder Theorem.) ■

Remark 1 Since $A_5$is also not solvable. As a matter of fact A_5 of order 60 is the smallest group that is not solvable.

Remark 2 This fact is closely connected with the fact that a polynomial equation of degree 5 is not in general solvable by radicals. (Ref. Theorem 56.6)

Rings and Fields

Defn. (Ring)

A Ring $< R, +, \cdot >$ is a set R together with two binary operations "$+$" and "$\cdot$", we call "addition" and "multiplication", defined on R such that the following axioms are satisfied:

$\mathcal{R}_1$. $< R, + >$ is an abelian group.

$\mathcal{R}_2$. multiplication is association.

$\mathcal{R}_3$. $\forall a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.(left distributive law and right distributive law)

Examples

1. $< \mathbb{Z}_n, +, \cdot >$ is a ring. (Multiplication is taken modulo n.)
2. $< \mathbb{Z}, +, \cdot >$ is a ring.
3. $< \mathbb{R}, +, \cdot >$, $< \mathbb{Q}, +, \cdot >$, $< \mathbb{C}, +, \cdot >$ are rings.
4. $\mathbb{R}[x]$, $\mathbb{Z}[x]$ The set of all polynomials with coefficients in $\mathbb{R}$ and $\mathbb{Z}$ respectively form rings.
5. Let R be a ring. The set of all $n \times n$ matrices having entries in R, $< M_n(R), +, \cdot >$ is a ring.

Notations

If $n \in \mathbb{Z}^+$, then we use na to denote $a + a + \cdots + a$ (n $a's$) where $a \in R$(ring). If $n \in \mathbb{Z}^-$, then $na = (-a) + (-a) + \cdots + (-a)$ (n $(-a)'s$) where $-a$ is the additive inverse of a. Finally, for each $a \in R$, $0a = \mathbf{0}$ where the left $0 \in \mathbb{Z}$ and the other $\mathbf{0} \in R$.

Theorem $\forall\ a, b, \mathbf{0} \in R$(ring), we have
(1) $\mathbf{0}a = a\mathbf{0} = \mathbf{0}$.
(2) $a(-b) = (-a)b = -ab$.
(3) $(-a)(-b) = ab$.

Proof.
(1) $(\mathbf{0} + \mathbf{0})a = \mathbf{0}a$ and ($\mathbf{0}$+$\mathbf{0}$)a=$\mathbf{0}$a+$\mathbf{0}$a. Hence, $\mathbf{0}a = \mathbf{0}$. $a\mathbf{0} = \mathbf{0}$ can be obtained by the same idea.

(2) Since $ab + a(-b) = a(b + (-b)) = a\mathbf{0} = \mathbf{0}$, $-ab = a(-b)$.

(3) By similar argument. ■

Defn. (Ring Homomorphism)

For rings R and R', a map $\varphi : R \to R'$ is a homo. if the following two conditions are satisfied for all $a, b \in R$:

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$.

(2) $\varphi(ab) = \varphi(a)\varphi(b)$.

Note More precisely, $R = < R, \oplus, \odot >$, $R' = < R', +, \cdot >$,
(1) $\varphi(a \oplus b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(a \odot b) = \varphi(a) \cdot \varphi(b)$.

Example $F = \mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$

$< F, +, \cdot >$ is a ring and $\varphi_a(f) = f(a)$ defines a homo. from F into $\mathbb{R}$. (The additions and multiplications in F are different from $\mathbb{R}$.)

Example $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(a) = a \pmod{n}$ is a homo. from $\mathbb{Z}$ onto $\mathbb{Z}_n$.

Example $\varphi : \mathbb{Z} \to 3\mathbb{Z}$ defined by $\varphi(x) = 3x \ \forall \ x \in \mathbb{Z}$ is a one-to-one homo. from $\mathbb{Z}$ onto $3\mathbb{Z}$.

Defn. (Ring Isomorphism)

A one-to-one and onto homo. from R onto R' is an isomorphism from R onto R'. We say R and R' are isomorphic.

Defn. (Commutative Ring)

A ring in which the multiplication is commutative ring.

Defn. (Ring with Unity)

A ring with a multiplicative identity element unity.

Defn. (Unit)

An element a in R with unity $1 \neq 0$ which has a multiplicative inverse a^{-1} is called a unit of R.

Defn. (Division Ring or Skew Field)

If every nonzero element of R is a unit, then R is a division ring (or skew field).

Defn. (Field)

A field is a commutative division ring. A noncommutative division ring is called a strictly skew field.

Example Let p be a prime. Then $< \mathbb{Z}_p, +, \cdot >$ is a field.

Proof. $\forall\ x \in \mathbb{Z}_p^* = \mathbb{Z}_p/\{0\},\ \ gcd(x, p) = 1$. Hence, $\exists\ a, b \in \mathbb{Z}$, s.t. $ax + bp = 1$. Hence $ax \equiv 1 \pmod{p}$. Let $x' \in \mathbb{Z}_p$ and $x' \equiv x \pmod{p}$. Then $ax' = ax = 1 \pmod{p}$. x' is an inverse (multiplicative) of a. ■