GROUPS: SUPPLEMENTARY TOPICS

Theorem (see Proposition 2.59, page 172):

If G is a finite abelian group, then G has a subgroup of order d for every divisor d of $|G|$.

Theorem (Cayley) (see Theorem 2.66, page 178):

Every group G is isomorphic to a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof:

For each $a \in G$, define $\tau_a : G \longrightarrow G$ by

$$\tau_a(x) = ax$$

for every $x \in G$ (note that if $a \neq 1$, then τ_a is not a homomorphism, since $\tau_a(1) = a \cdot 1 = a \neq 1$). We show that τ_a is a permutation (bijection) of elements from G. In fact, first note that for any $a, b \in G$ we have

$$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x),$$

so $\tau_a\tau_b = \tau_{ab}$. It follows that each τ_a is a bijection, since its inverse is $\tau_{a^{-1}}$:

$$\tau_a\tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = 1_G = \tau_{a^{-1}a},$$

and so $\tau_a \in S_G$, i.e. τ is a permutation.

Define

$$\varphi : G \longrightarrow S_G$$

by $\varphi(a) = \tau_a$. Rewriting, we get

$$\varphi(a)\varphi(b) = \tau_a\tau_b = \tau_{ab} = \varphi(ab),$$

so that φ is a homomorphism. Finally, φ is an injection. If $\varphi(a) = \varphi(b)$, then $\tau_a = \tau_b$, which means

$$\tau_a(x) = \tau_b(x)$$

for all $x \in G$; in particular, when $x = 1$, this gives $a = b$, as desired.

Finally, to prove the last statement, we note that if X is a set with $|X| = n$, then

$$S_X \cong S_n.$$

(however, this is an exercise). ■

Theorem (see Propositions 2.68, 2.69, page 180):

(a) Every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or the four-group $\mathbf{V}$. Moreover, $\mathbb{Z}_4$ and $\mathbf{V}$ are not isomorphic.

(b) Every group of order 6 is isomorphic to either $\mathbb{Z}_6$ or S_3. Moreover, $\mathbb{Z}_6$ and S_3 are not isomorphic.

Remark:

Classifying groups of order 8 and higher is more difficult. For details, see page 182.

COMMUTATIVE RINGS

Definition:

A commutative ring R is a set with two operations, addition and multiplication, such that:

(i) R is an abelian group under addition;

(ii) $ab = ba$ for all $a, b \in R$ (commutative law);

(iii) $a(bc) = (ab)c$ for any $a, b, c \in R$ (associative law);

(iv) there is an element $1 \in R$ with $1 \neq 0$ and with $1 \cdot a = a \cdot 1 = a$ for any $a \in R$;

(v) $a(b + c) = ab + ac$ for any $a, b, c \in R$ (distributive law).

Example:

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative rings.
2. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a commutative ring.
3. $\{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a commutative ring.
4. $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Z}\}$ is not a ring. Moreover, $\{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ is not a ring.
5. The set of all 2×2 matrices is a noncommutative ring.
6. $\mathbb{Z}_m$ is a commutative ring.

Theorem:

Let R be a commutative ring. We have:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to a, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$.

Proof:

(i) The distributive law gives

$$0 + 0 \cdot a = 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a,$$

so

$$0 + 0 \cdot a = 0 \cdot a + 0 \cdot a.$$

Subtracting $0 \cdot a$ from both sides gives $0 = 0 \cdot a$.

(ii) By (i) and the distributive law we have

$$0 = 0(-a) = (-1 + 1)(-a) = (-1)(-a) + (-a).$$

Adding a to both sides gives $a = (-1)(-a)$.

(iii) By (ii) we have $(-1)(-a) = a$. Multiplying both sides by -1 gives

$$(-1)(-1)(-a) = (-1)a.$$

But $(-1)(-1) = 1$ by (ii), therefore $-a = (-1)a$. ■

Theorem:

If G is a finite abelian group, then G has a subgroup of order d for every divisor d of $|G|$.

Theorem (Cayley):

Every group G is isomorphic to a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Theorem:

(a) Every group of order 4 is isomorphic to either Z_4 or the four-group V. Moreover, Z_4 and V are not isomorphic.

(b) Every group of order 6 is isomorphic to either Z_6 or S_3. Moreover, Z_6 and S_3 are not isomorphic.

Remark:

Classifying groups of order 8 and higher is more difficult.

Definition:

A commutative ring R is a set with two operations, addition and multiplication, such that:

(i) R is an abelian group under addition;

(ii) $ab = ba$ for all $a, b \in R$ (commutative law);

(iii) $a(bc) = (ab)c$ for any $a, b, c \in R$ (associative law);

(iv) there is an element $1 \in R$ with $1 \neq 0$ and with $1 \cdot a = a \cdot 1 = a$ for any $a \in R$;

(v) $a(b+c) = ab+ac$ for any $a, b, c \in R$ (distributive law).

Example:

1. Z, Q, R, C **are commutative rings.**

2. $Z[i] = \{a + bi : a, b \in Z\}$ **is a commutative ring.**

3. $\{a+b\sqrt{2} : a, b \in Z\}$ **is a commutative ring.**

4. $\{a + b\sqrt[3]{2} : a, b \in Z\}$ **is not a ring. Moreover,** $\{a + b\sqrt[3]{2} : a, b \in Q\}$ **is not a ring.**

5. The set of all 2×2 **matrices is a noncommutative ring.**

6. Z_m **is a commutative ring.**

Theorem:

Let R be a commutative ring. We have:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to a, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$.

(i) The distributive law gives

$$0+0\cdot a = 0\cdot a = (0+0)\cdot a = 0\cdot a+0\cdot a,$$

so

$$0+0\cdot a = 0\cdot a+0\cdot a.$$

Subtracting $0\cdot a$ from both sides gives $0 = 0\cdot a$.

(ii) By (i) and the distributive law we have

$$\begin{aligned} 0 &= 0(-a) \\ &= (-1+1)(-a) \\ &= (-1)(-a) + (-a). \end{aligned}$$

Adding a to both sides gives $a = (-1)(-a)$.

(iii) By (ii) we have

$$(-1)(-a) = a.$$

Multiplying both sides by -1 gives

$$(-1)(-1)(-a) = (-1)a.$$

But $(-1)(-1) = 1$ by (ii), therefore

$$-a = (-1)a. \blacksquare$$