0 Preliminaries

Properties of Integers

Theorem 0.1 (Well Ordering Principle)**.** *Every non-empty subset of the positive integers has a least element.*

Theorem 0.2 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r such that*

$$a = bq + r \text{ and } 0 \le r < b.$$

Example.
(i) $a = 13, b = 5$. We have that $13 = 5 \cdot 2 + 3$.
(ii) $a = -13, b = 5$. We have that $-13 = 5 \cdot (-3) + 2$.

Sketch of Proof of Theorem. Let $a, b \in \mathbb{Z}$ and $b > 0$. let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk \ge 0\}$.
Case 1: $0 \in S$. Then $a - bk = 0$ for some $k \in \mathbb{Z}$ and $a = bk$ and $a = bq + r$ where $q = k$ and $r = 0$.
Case 2: $0 \notin S$. Then S is a subset of the positive integers.

Exercise. Show S is nonempty.

By the Well Ordering Principle, S has a least element. Let r be this least element. Then $r = a - bq$ for some $q \in \mathbb{Z}$. Show $r < b$, and show uniqueness of q and r.

Definition 0.1. Let $a, b \in \mathbb{Z}$. We say a divides b and write $a \mid b$ if $b = ac$ for some $c \in \mathbb{Z}$. We say a is a divisor of b.

Example. $8 \mid 24$ since $24 = 8 \cdot 3$ and $3 \in \mathbb{Z}$.

Definition 0.2. Let $a, b \in \mathbb{Z}$ where a, b are not both zero. Then the greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the largest integer d such that $d \mid a$ and $d \mid b$.

Note. In number theory $\gcd(a, b)$ is denoted by (a, b).

Example. $\gcd(8, 60) = 4$.

Theorem 0.3. *Let $a, b \in \mathbb{Z}$, where a, b are not both zero. Then* $\gcd(a, b) = \min\{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$

Sketch of Proof. Let $a, b \in \mathbb{Z}$ not both be zero. Then let $S = \{as + bt \mid s, t \in \mathbb{Z}, as + bt > 0\}$. See that S is nonempty because $a, -a, b, -b \in S$.
So S is a nonempty set of positive integers. By the Well Ordering Principle, S has a least element d. We show $d = \gcd(a, b)$.
So $d = as + bt$ for some $s, t \in \mathbb{Z}$. Then by the Division Algorithm, $a = dq + r$ fo some integers q, r where $0 \le r < d$.

1 previous chapters TODO

2 previous chapters TODO

3 Cyclic Groups

Let $a \in G$ where G is a group. The cyclic group generated by a is

$$\langle a \rangle \coloneqq \{a^n : n \in \mathbb{Z}\}.$$

Theorem 3.1. *Let G be a group and suppose $a \in G$.*
(1) If a has infinite order then $a^i = a^j$ $(i, j \in \mathbb{Z})$ if and only if $i = j$.
(2) If a has finite order n, then

$$\langle a \rangle = \left\{e, a^1, a^2, \ldots, a^{n-1}\right\},$$

and $a^i = a^j$ $(i, j \in \mathbb{Z})$ if and only if $i \equiv j \pmod n$

Proof. Let G be a group and suppose $a \in G$.

(1) Suppose a has infinite order. If n is a positive integer then $a^n \neq e$. Suppose $a^i = a^j$ where $i, j \in \mathbb{Z}$, and without loss of generality, $i \leq j$. Then $a^{j-i} = a^j \left(a^i\right)^- 1 = a^i \left(a^i\right)^- 1 = e$. It follows that $j - i = 0$ since $j - i \in \mathbb{Z}$ and $j - i \geq 0$, so $i = j$.

Conversely, if $i = j$, then $a^i = a^j$.

(2) Suppose a has finite order n.

Case 1: $n = 1$. Then $a^1 = a = e$, so

$$\langle a \rangle = \{e^n : n \in \mathbb{Z}\} = \{e\}.$$

Note that □

4 Isomorphisms?

...

Example. Find $\mathrm{Aut}(\mathbb{Z}_8)$.

Suppose $\alpha \in \mathrm{Aut}(\mathbb{Z}_8)$. Then $\alpha : \mathbb{Z}_8 \to \mathbb{Z}_8$ is an isomorphism.

$x = x \cdot 1$	$\lvert x\rvert = \dfrac{8}{\gcd(x,8)}$
0	1
1	8
2	4
3	8
4	2
5	8
6	4
7	8

$|1| = 8$ and 1 is a generator of $\mathbb{Z}_8$.

By a previous theorem, $|\alpha(1)| = 8$ and hence $\alpha(1) = 1, 3, 5$, or 7.

Let $x \in \mathbb{Z}_8$. Then $x = x \cdot 1 = \overbrace{1 + \cdots + 1}^{x\text{-times}}$. So $\alpha(x) = \alpha(1) + \cdots + \alpha(1) = x\alpha(1)$.

The automorphism α is completely determined by the value of $\alpha(1)$.

For $j = 1, 3, 5$, or 7, we define $\alpha_j : \mathbb{Z}_8 \to \mathbb{Z}_8$ by $\alpha_j(x) = xj \pmod 8 = \overbrace{j + \cdots + j}^{x\text{-times}} \pmod 8$.

We show that each α_j is an automorphism of $\mathbb{Z}_8$. Clearly each α_j is well-defined. Let $j = 1, 3, 5$, or 7. Suppose $x_1, x_2 \in \mathbb{Z}_8$ and $\alpha_j(x_1) = \alpha_j(x_2)$. Then $jx_1 \equiv jx_2 \pmod 8$.

Observe that $j \in \{1, 3, 5, 7\} = U(8)$. The operation in $U(8)$ is multiplication mod 8. Each j has a multiplicative inverse $\bar{j} \pmod 8$, i.e. $\bar{j}j \equiv 1 \pmod 8$.

In this example, $\bar{j} = j$. Then

$$\begin{aligned}
\bar{j}\,(jx_1) &\equiv \bar{j}\,(jx_2) \pmod 8\\
(\bar{j}j)\,x_1 &\equiv (\bar{j}j)\,x_2 \pmod 8\\
1x_1 &\equiv 1x_2 \pmod 8\\
x_1 &\equiv x_2 \pmod 8
\end{aligned}$$

so that $x_1 = x_2$ in $\mathbb{Z}_8$. So α_j is one-to-one.

Let $y \in \mathbb{Z}_8$. Then $\alpha_j(\bar{j}y) = j\,(\bar{j}y) \pmod 8 = (j\bar{j})\,y \pmod 8 = y \pmod 8$. Then $\alpha_j(\bar{j}y) = y$, so α_j is onto.

Then

$$\begin{aligned}\alpha_j(x_1+x_2) &= j(x_1+x_2) \pmod 8\\ &= (jx_1+jx_2) \pmod 8\\ &= (jx_1 \pmod 8) + (jx_1 \pmod 8)\\ &= \alpha_j(x_1)+\alpha_j(x_2)\end{aligned}$$

So α_j preserves the group operation and α_j is an automorphism.

Note. $\alpha_1, \alpha_3, \alpha_5, \alpha_7$ are the automorphisms of $\mathbb{Z}_8$, i.e.

$$\operatorname{Aut}\mathbb{Z}_8 = \{\alpha_1, \alpha_3, \alpha_5, \alpha_7\}.$$

Note. $\operatorname{Aut}\mathbb{Z}_8 \approx U(8)$.

Proof. Define $T : \{\alpha_1, \alpha_3, \alpha_5, \alpha_7\} \to U(8)$ by $T(\alpha_j) = j$. So

$$\begin{aligned}\alpha_1 &\to 1\\ \alpha_3 &\to 3\\ \alpha_5 &\to 5\\ \alpha_7 &\to 7\end{aligned}$$

T is clearly well-defined, one-to-one, and onto. Let $i, j \in U(8)$. Suppose $ij = k$ in $U(8)$, i.e. $ij \equiv k \pmod 8$.

Then

$$T(\alpha_i \circ \alpha_j) = T(\alpha_k) = k$$

$$= i \cdot j \pmod 8 = T(\alpha_i)T(\alpha_j) \pmod 8$$

since $\alpha_i \circ \alpha_j = \alpha_k$, which is true because

$$(\alpha_i \circ \alpha_j)(x) \equiv \alpha_i(\alpha_j(x)) \equiv i(jx) \pmod 8$$

$$\equiv (ij)x \equiv kx \pmod 8 = \alpha_k(x)$$

for any $x \in U(8)$. Hence T is an isomorphism and so $\operatorname{Aut}(\mathbb{Z}_8) \approx U(8)$. □

Similarly, we have the following theorem:

Theorem 4.1. *$\operatorname{Aut}(\mathbb{Z}_n) \approx U(n)$.*

Example. Suppose $\Phi : \mathbb{Z}_8 \to \mathbb{Z}_8$ is an automorphism and $\Phi(5) = 7$. Find a formula for $\Phi(x)$.

Hint. $5 \cdot 5 = 1$ in $\mathbb{Z}_8$.

To find a formula for $\Phi(x)$ we only need to find $\Phi(1)$ since $\Phi(x) = \Phi(x \cdot 1) = x\Phi(1)$. So from the hint given we find that $\Phi(1) = \Phi(5 \cdot 5) = 5\Phi(5) = 5 \cdot 7 = 35 \equiv 3 \pmod 8$. So $\Phi(1) = 3$, which means $\Phi(x) = x\Phi(1) = x \cdot 3$.

Hence $\Phi(x) = 3x \pmod 8$.

5 Cosets and Lagrange's Theorem (ch7)

Definition 5.1. Let H be a subset of a group G. Let $a \in G$. Define

$$aH = \{ah : h \in H\}$$

and

$$Ha = \{ha : h \in H\}.$$

When H is a subgroup of G the set aH is called the left coset of H in G containing a, and Ha is called the right coset of H in G containing a.

Example. Let $H = \{e, (1\,2)\} = \langle(1\,2)\rangle$ and $G = S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

Then

$$\begin{aligned}
eH &= H = \{e, (1\,2)\}\\
(1\,2)H &= \{(1\,2), e\} = H\\
(1\,3)H &= \{(1\,3), (1\,3)(1\,2)\} = \{(1\,2), (1\,2\,3)\}\\
(2\,3)H &= \{\}
\end{aligned}$$