MTH 339

External Direct Products

Def Let $G_1, G_2, \dots, G_n$ be a finite collection of groups. The external direct product of $G_1, \dots, G_n$ written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{ (g_1, g_2, \dots, g_n) \mid g_i \in G_i \}$$

Example: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Clearly, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is an Abelian group of order 6. Is it related to $\mathbb{Z}_6$?
Remember that the operation is addition in each component.

Now we have $(1,1) = (1,1)$, $2(1,1) = (0,2)$

$3(1,1) = (1,0)$, $4(1,1) = (0,1)$

$5(1,1) = (1,2)$, $6(1,1) = (0,0)$

Hence, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic. Hence, it is isomorphic to $\mathbb{Z}_6$.

Thm The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \cdots, g_n)| = \text{lcm}(|g_1|, |g_2|, \cdots, |g_n|)$$

Proof: Denote the identity of G_i by e_i. Let $s = \text{lcm}(|g_1|, \cdots, |g_n|)$ and $t = |(g_1, \cdots, g_n)|$. Since s is a multiple of each $|g_i|$, we have

$$(g_1, \cdots, g_n)^s = (g_1^s, \cdots, g_n^s) = (e_1, \cdots, e_n)$$

Therefore, $t \leq s$. On the other hand,

$(g_1^t, \ldots, g_n^t) = (g_1, \ldots, g_n)^t = (e_1, \ldots, e_n)$

so t is a common multiple of $|g_1|, \ldots, |g_n|$.

Thus, $s \leq t$.

□

Example: Let m and n be positive integers that are divisible by 5.

We want to know the number of elements of order 5 in $\mathbb{Z}_m \oplus \mathbb{Z}_n$. We need to count the number of elements $(a,b) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ with $5 = |(a,b)| = \text{lcm}(|a|, |b|)$. Clearly $|a| = 1$ or 5 or $|b| = 1$ or 5, but not $(a,b) = (0,0)$

Since both $\mathbb{Z}_m$ and $\mathbb{Z}_n$ each have a unique subgroup of order 5, there are exactly 5 choices for a and 5 choices for b, therefore 25 choices for (a,b), including $(0,0)$.

So there are exactly 24 elements in $\mathbb{Z}_n \oplus \mathbb{Z}_m$ of order 5.

Thm Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

"$\Rightarrow$" Assume $G \oplus H$ is cyclic, $|G| = m$, $|H| = n$ and $|G \oplus H| = mn$. Suppose $\gcd(m,n) = d$ and (g,h) is a generator of $G \oplus H$.

$$(g,h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e^{n/d}, e^{m/d})$$

$$= (e,e)$$

$$\Rightarrow \quad mn = |(g,h)| \leq mn/d \Rightarrow d = 1$$

"$\Leftarrow$" Let $G = \langle g \rangle$ and $H = \langle h \rangle$ and suppose $\gcd(m,n) = 1$. Then $|(g,h)| = \operatorname{lcm}(m,n)$ $= mn = |G \oplus H|$, so that (g,h) is a generator of $G \oplus H$.

Corollary: $G_1 \oplus \cdots \oplus G_n$ (finite number of finite cyclic groups) is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Corollary: Let $m = n_1 n_2 \cdots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Example: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$

$\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$

(First step: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$ as 2 and 3 are relatively prime. Then $\mathbb{Z}_6 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_{30}$ as 5 and 6 are relatively prime.

Def Let $U_k(n) = \{ x \in U(n) \mid x \bmod k = 1 \}$

$U_k(n)$ is a subgroup of $U(n)$.

Thm Suppose s and t are relatively prime. Then $U(st) \approx U(s) \oplus U(t)$. Moreover, $U_s(st) \approx U(t)$ and $U_t(st) \approx U(s)$.

Proof: $\phi : U(st) \to U(s) \oplus U(t)$

$\phi(x) = (x \bmod s,\ x \bmod t)$

is an isomorphism (details: HW)

$\tilde{\phi} : U_s(st) \to U(t)$

$\tilde{\phi}(x) = x \bmod t$

is also an isomorphism.

(And $\tilde{\tilde{\phi}} : U_t(st) \to U(s)$

$\tilde{\tilde{\phi}}(x) = x \bmod s$ as well)

Example: $\mathcal{U}(105) \approx \mathcal{U}(7) \oplus \mathcal{U}(15)$

$\mathcal{U}(105) \approx \mathcal{U}(21) \oplus \mathcal{U}(5)$

$\mathcal{U}(105) \approx \mathcal{U}(3) \oplus \mathcal{U}(5) \oplus \mathcal{U}(7)$

$\mathcal{U}(7) \approx \mathcal{U}_{15}(105) = \{1, 16, 31, 46, 61, 76\}$

$\mathcal{U}(15) \approx \mathcal{U}_{7}(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}$

Application: Data Security

Consider addition in $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$. Elements can be added componentwise.

$11000111 + 01110110 = 10110001$

$10011100 + 10011100 = 00000000$

Use key to encrypt credit card.

S (credit card)	10101100
key (Amazon)	00111101
Sum	10010001

add key again:

encrypted	10010001
key	00111101
Sum	10101100

original string (credit card)

Application: Public key Cryptography

Idea: method to scramble message known publicly, but only receiver can unscramble it.

How does it work? Receiver chooses a pair of large primes p and q, $m = \text{lcm}(p-1, q-1)$ and $1 < e < m$ (encryption exponent).

Note: e needs to be relatively prime to m.

Now the receiver calculates $n = pq$ (n is called "key") and asks that messages are sent as $M^e \bmod n$ (where M is the message).

Note: Although this encryption method is public, only the receiver can decrypt it, knowing the factorization $n = pq$.

Example: $M =$ "YES", convert to string by

$A = 01$, $B = 02$, $C = 03$, ...

$M = 25\,05\,19$ (Y E S)

We will send the messages in blocks of size 4, fill blanks with zeros.

So: $M =$ "2505" and "1900" (two blocks)

Now choose p and q, $p = 37$ and $q = 73$ and e relatively prime with $\text{lcm}(p-1, q-1) = 72$, say $e = 5$. The receiver publishes $n = 37 \cdot 73 = 2701$ and $e = 5$.

So we will send the two blocks as

$(2505)^5 \bmod 2701$ and

$(1900)^5 \bmod 2701$

$(2505)^5 \bmod 2701 = 2415$

How does the receiver unscramble "2415" to get 2505 back?

First, using $n = pq$, the receiver knows that $\operatorname{lcm}(p-1, q-1) = \operatorname{lcm}(36, 72) = 72$.

Next, the receiver finds $e^{-1} = d$ in $\mathcal{U}(72)$, the solution of $5 \cdot d = 1 \bmod 72$.

The solution is $d = 29$.

Now the receiver computes $(2415)^{29} \bmod 2701$

$= 2505$

to recover the original message.

Note that it is essential to find $d = e^{-1}$ and this only works if we know how $n = pq$ factors.

Why does this method work?

$U(n) \approx U(p) \oplus U(q) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$

So x^m in $U(n)$ corresponds to an element of the form $(mx_1, mx_2) \in \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$

Since $m = \text{lcm}(p-1, q-1)$ we can write $m = s(p-1)$ and $m = t(q-1)$. Then

$(mx_1, mx_2) = (s(p-1)x_1, t(q-1)x_2) = (0,0)$

in $\mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$. Therefore, $x^m = 1$ in $U(n)$.

Now we encode $R = M^e \bmod n$. Now e was chosen such that $ed = 1 + km$ for some k, hence we have (modulo n):

$R^d = (M^e)^d = M^{1+km} = M(M^m)^k = M1^k = M$

□

MTH 339 Do now

1./ Show that $U_7(105) = \{1, 8, 22, 43, 64, 71, 92\}$

2./ Prove that $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.
Hint: Assume $\mathbb{Z} \oplus \mathbb{Z} = \langle (a,b) \rangle$
and find $x \in \mathbb{Z} \oplus \mathbb{Z}$ with $x \notin \langle (a,b) \rangle$.

3./ Let G be a group and let $H = \{(g,g) \mid g \in G\}$.
Show that H is a subgroup of $G \oplus G$.

MTH 339 - HW

1./ Show that the external direct product of groups is itself a group.

2./ Show that the mapping $\phi : \mathcal{U}(st) \to \mathcal{U}(s) \oplus \mathcal{U}(t)$ $\phi(x) = (x \bmod s, x \bmod t)$ is indeed an isomorphism.

3./ Let (a,b) belong to $\mathbb{Z}_m \oplus \mathbb{Z}_n$. Prove that $|(a,b)|$ divides $\text{lcm}(m,n)$.

4./ Let p be a prime. Prove that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has exactly $p+1$ subgroups of order p.

5./ Express $\mathcal{U}(165)$ as an external direct product of $\mathcal{U}$-groups in four different ways.

6./ What is the smallest positive integer k, such that $x^k = e$ for all $x \in \mathcal{U}(7 \cdot 17)$?