MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Fri, Apr 3, 2020

Chapter 8: External Direct Products Cont'd.

Relative primality is preserved by the standard isomorphism map

Recall that $U(n) = \mathbb{Z}_n^{\times}$, the subset of $\mathbb{Z}_n$ consisting of the residue classes relatively prime to the modulus n, is a group under multiplication (mod n). We now have

Theorem 8.3: Let m and n be positive integers satisfying $(m, n) = 1$. Then

$$U(mn) \simeq U(m) \oplus U(n).$$

Theorem 8.3 will follow from the following

Lemma 8.3: When $(m,n) = 1$, the standard isomorphism map

$$\varphi_s : \mathbb{Z}_{mn} \to \mathbb{Z}_m \oplus \mathbb{Z}_n \qquad (*)$$

preserves relative primality. That is if $x \in \mathbb{Z}_{mn}$ and $\varphi_s(x) = (x_m, x_n)$, then

$$\gcd(x, mn) = 1 \iff (x_m, m) = 1 \text{ and } (x_n, n) = 1. \qquad (1)$$

Proof of Lemma: Begin by observing that for any integer x, we have

$$(x, mn) = 1 \iff (x, m) = 1 \text{ and } (x, n) = 1 \qquad (2)$$

Next, note that with (a,b) representing the gcd (a,b), we have

$$(x, m) = (x_m, m) \text{ and } (x, n) = (x_n, n) \qquad (3).$$

Thus Lemma 8.3 follows from (2) and (3).

Proof of Theorem 8.3: The standard isomorphism φ_s in $(*)$ viewed just as a bijection leads to a natural map (as a function)

$$\varphi_s \Big|_{U(mn)} : U(mn) \longrightarrow U(m) \oplus U(n)$$

by considering the restriction of the function φ_s to the subset $U(mn)$ of $\mathbb{Z}_{mn}$. The restriction is obviously one-to-one. Note that $|U(mn)| = \varphi(mn)$, where φ here is the Euler function and $|U(m)| = \varphi(m)$ & $|U(n)| = \varphi(n)$.

~~and~~ The Euler function satisfies

$$\varphi(mn) = \varphi(m)\varphi(n), \text{ if } (m,n)=1. \qquad (5)$$

The the restriction of φ_s to $U(mn)$ yields a bijection in (4). In making this restriction, the operation of addition is replaced by multiplication! Thus (4) is an isomorphism under multiplication. This proves Theorem 8,3.

Remark: We note that (3) holds even when $(m,n) \neq 1$. However we need $(m,n)=1$ for $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n$ to hold, and for (5) to hold.

Next given an integer $n > 1$ and a divisor k of n, $(k>0)$, consider

$$U_k(n) = \{ x \in U(n) \mid x \equiv 1 \pmod{k} \} \qquad (6).$$

Then we have

Theorem 8.3′: Let m and n be relatively prime, $m,n \in \mathbb{Z}^+$. Then

$$U_m(mn) \simeq U(n) \quad \text{and} \quad U_n(mn) \simeq U(m).$$

Proof: The isomorphisms $U_m(mn) \simeq U(n)$ and $U_n(mn) \simeq U(m)$ follow from the correspondences $x \pmod{mn} \to x_n$ and $x \pmod{mn} \to x_m$ respectively. □

Read the numerical example pertaining to $U(105)$ on p.161.

We will now work ~~of~~ out the details for $U(20)$ illustrating Thm 8.3′.

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ Write $20 = 4 \cdot 5$, $m=4$, $n=5$

$U_4(20) = \{ x \in U(20) \mid x \equiv 1 \pmod{4} \} = \{1, 9, 13, 17\}$

$U_5(20) = \{ x \in U(20) \mid x \equiv 1 \pmod{5} \} = \{1, 11\}$

$U(4) = \{1, 3 \pmod{4}\}$, $U(5) = \{1, 2, 3, 4 \pmod{5}\}$.

It is easy to check that

$U_4(20) = \{1, 9, 13, 17 \pmod{20}\} \simeq U(5) = \{1, 2, 3, 4 \pmod{5}\}$

by the correspondence

$$[1]_{20} \to [1]_5, \ [9]_{20} \to [4]_5, \ [13]_{20} \to [3]_5, \ [17]_{20} \to [2]_5.$$

Similarly $U_5(20) = \{1, 11 \pmod{20}\} \simeq U(4) = \{1, 3 \pmod{4}\}$

More problems from Chapter 8

problem 5, p168: Prove that $\mathbb{Z}\oplus\mathbb{Z}$ is not cyclic.

Proof: Suppose $\mathbb{Z}\oplus\mathbb{Z}$ is cyclic. Then $\mathbb{Z}\oplus\mathbb{Z} = \langle (m,n)\rangle$ for some $(m,n)\in\mathbb{Z}\oplus\mathbb{Z}$. But every element of $\langle (m,n)\rangle$ is of the form (mk, nk), with $k\in\mathbb{Z}$, which is an element (x,y) on the line $nx-my=0$ in the plane. Clearly not all elements of $\mathbb{Z}\oplus\mathbb{Z}$ satisfy this. Hence $\mathbb{Z}\oplus\mathbb{Z}$ is not cyclic.

Problem 22, p 168:

part (i): Determine the number of order 15 in $\mathbb{Z}_{30}\oplus\mathbb{Z}_{20}$

part (ii) Determine the number of cyclic groups of order 15 in $\mathbb{Z}_{30}\oplus\mathbb{Z}_{20}$.

Solution, part (i): The elements (α,β) of order 15 are those that satisfy

$$\mathrm{lcm}\,[|\alpha|, |\beta|] = 15. \tag{7}$$

Since $3\nmid 20$, in order for (7) to be satisfied with $|\beta|\,\big|\,20$, we must have $|\beta| = 1$ or 5. So we have two mutually exclusive cases:

Case 1: $|\beta|=1 \Rightarrow \beta$ is the identity in $\mathbb{Z}_{20}$.

This means $|\alpha|=15$ in $\mathbb{Z}_{30}$. Since $\mathbb{Z}_{30}$ is cyclic, the number of elements of order 15 is $\varphi(15)=8$, where φ is the Euler function.

Case 2: $|\beta|=5$. Since $\mathbb{Z}_{20}$ is cyclic, the number of such β is $\varphi(5)=4$. For each one of these elements β, the element (α,β) will have order 15 only if $|\alpha|=3$ or $|\alpha|=15$, since $|\alpha|\,\big|\,30$, and (7) has to hold.

The # of elements $\alpha\in\mathbb{Z}_{30}$ with $|\alpha|=3$ is $\varphi(3)=2$.

The # of elements $\alpha\in\mathbb{Z}_{30}$ with $|\alpha|=15$ is $\varphi(15)=8$

So the number of elements $\alpha\in\mathbb{Z}_{30}$ with $|\alpha|=1$ or 3 is $2+8=10$.

Thus for each β with $|\beta|=5$, there are 10 elements $(\alpha,\beta)\in\mathbb{Z}_{30}\oplus\mathbb{Z}_{20}$ with order 15. Since there are 4 elements $\beta\in\mathbb{Z}_{20}$ of order 5, the total number of (α,β) counted by Case 2 is

$$4\times 10 = 40.$$

So the total number of $(\alpha,\beta) \in \mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$ enumerated by the two mutually exclusive cases is

$$40 + 8 = 48.$$

This is the answer to part (ii).

<u>Solution to part (iii)</u>: Each element of order 15 generates a cyclic group of order 15 which has $\varphi(15) = 8$ <u>generators</u> (all of order 15). Give two different cyclic subgroups of $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$ of order 15, their sets of generators have no common element. Thus the number of cyclic groups of order 15 is

$$\frac{\#\text{ of elements of order } 15}{\varphi(15)} = \frac{48}{8} = 6.$$

Thus $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$ will have 6 cyclic subgroups of order 15.

<u>Problem 59, p. 170</u>: Let p be prime. Prove that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has exactly $p+1$ subgroups of order p.

<u>Proof</u>: A subgroup of order p is cyclic since p is prime.

First we determine the number of elements of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Let $(\alpha,\beta) \in \mathbb{Z}_p \oplus \mathbb{Z}_p$, with (α,β) <u>not</u> the identity ie $(\alpha,\beta) \neq (0,0)$.

Then

$$|(\alpha,\beta)| = \operatorname{lcm}[|\alpha|, |\beta|] = p$$

since $|\alpha| = 1$ or p, $|\beta| = 1$ or p and $|\alpha| = |\beta| = 1$ is <u>not</u> possible since $(\alpha,\beta) \neq (0,0)$. Thus <u>all</u> non-identity elements of $\mathbb{Z}_p \oplus \mathbb{Z}_p$ have order p, and the number of non-identity elements is $p^2 - 1$. Thus the number of (cyclic) subgroups of order p is

$$\frac{\#\text{ of elements of order } p}{\varphi(p)} = \frac{p^2-1}{p-1} = p+1.$$

Problem 41, p170: List the elements of $U_7(35)$ and $U_5(35)$.

Solution: $U(35) = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

$U_7(35) = \{x \in U(35) \mid x \equiv 1 \pmod 7\} = \{1, 8, 22, 29\} \pmod{35}$

$U_5(35) = \{x \in U(35) \mid x \equiv 1 \pmod 5\} = \{1, 6, 11, 16, 26, 31\} \pmod{35}$.

Note that $U_7(35) \simeq U(5) = \{1, 2, 3, 4\} \pmod 5$ in view of the correspondence

$[1]_{35} \to [1]_5$, $[22]_{35} \to [2]_5$, $[8]_{35} \to [3]_5$, $[29]_{35} \to [4]_5$

Similarly, $U_5(35) \simeq U(7) = \{1, 2, 3, 4, 5, 6\} \pmod 7$ in view of the correspondence

$[1]_{35} \to [1]_7$, $[16]_{35} \to [2]_7$, $[31]_{35} \to [3]_7$, $[11]_{35} \to [4]_7$, $[26]_{35} \to [5]_7$, $[6]_{35} \to [6]_7$

Problem #63, p171: Express $U(165)$ as an external direct product of U-groups in 4 different ways.

Solution: First decompose 165 as a product of primes

$$165 = 3 \times 5 \times 11$$

We may write 165 as the product $m \cdot n$ ~~with~~ in three ways as

$$165 = (3 \times 5) \times 11 = (3 \times 11) \times 5 = (5 \times 11) \times 3$$
$$= 15 \times 11 = 33 \times 5 = 55 \times 3.$$

Thus

$$U(165) \simeq U(3) \oplus U(5) \oplus U(11) \simeq U(15) \oplus U(11) \simeq U(33) \oplus U(5) \simeq U(55) \oplus U(3)$$

yielding the four external direct products (desired) of U-groups of different sizes.

Note: Order in the direct product does not matter since

$$G \oplus H \simeq H \oplus G$$

which trivially follows from the correspondence $(g, h) \to (h, g)$.