Chap 21-22

<u>Def</u>: An ordered integral domain is an integral domain A with a relation, symbolized by $<$, having the following properties:

1. For any a and b in A, exactly one of the following is true:

$$a=b, \quad a<b \quad \text{or} \quad b<a$$

2. If $a<b$ and $b<c$, then $a<c$
3. If $a<b$, then $a+c<b+c$
4. $a<b \Rightarrow ac<bc$ on the condition that $0<c$.

<u>Thm</u>: Every integral system is isomorphic to $\mathbb{Z}$. In other words, $\mathbb{Z}$ is, up to isomorphism, the only integral system.

<u>Thm</u>: Let K represent a set of positive integers. Consider the following 2 conditions:

(i) 1 is in K

(ii) For any positive integer k, if $k \in K$, then also $k+1 \in K$.

If K is any set of positive integers satisfying these 2 conditions, then K consists of all positive integers.

<u>Thm</u>: (Principle of mathematical induction) Consider the following conditions

(i) S_1 is true

(ii) For any positive integer k, if S_k is true, then also S_{k+1} is true.

If conditions (i) and (ii) are satisfied, then S_n is true for every positive integer n

<u>Ex</u> Prove $1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2$

C.2:

- S_1 holds: $1^3=1^2$
- assume S_k holds: $1^3+2^3+\cdots+k^3=(1+2+\cdots+k)^2$. Then

$$1^3+2^3+\cdots+k^3+(k+1)^3=(1+2+\cdots+k)^2+(k+1)^3=\frac{k^2(k+1)^2}{4}+(k+1)^3=\frac{(k+1)^2}{4}(k^2+4(k+1))=\frac{(k+1)^2(k+2)^2}{4}$$

$$\frac{(k+1)^2(k+2)^2}{4} = \left(1+2+\cdots+k+(k+1)\right)^2$$

Principle of strong induction: If

(i) S_1 is true

(ii) For any positive integer k, if S_i is true for every $i<k$, then S_k is true

Then S_n is true for every positive integer n.

Thm 3: Division algorithm: If m and n are integers and n is positive, there exist unique integers q and r s.t. $m = nq + r$ and $0 \le r < n$.

We call q the quotient, and r the remainder, in the division of m by n.

Exer F.2: $n>0, k>0$, $m = nq + r_1 \Rightarrow m = n(kq_1 + r_2) + r_1 = (nk)q + nr_2 + r_1$

$q = kq_1 + r_2$

$0 \le r_1 \le n-1$, $0 \le r_2 \le k-1$ $\Rightarrow \underset{0}{\overset{\vee\!|}{nr_2 + r_1}} \le n(k-1) + n - 1 = nk - 1$ $\Rightarrow$ q is the quotient when m is divided by nk.

Exer C.7 $\frac{1}{2!} + \frac{2}{3!} + \cdots + \frac{n}{(n+1)!} = \frac{(n+1)!-1}{(n+1)!}$

- S_1: $\frac{1}{2!} = \frac{2!-1}{2} = \frac{1}{2}$
- Assume S_k holds: $\frac{1}{2!} + \frac{2}{3!} + \cdots + \frac{k}{(k+1)!} = \frac{(k+1)!-1}{(k+1)!}$

S_{k+1}: $\frac{1}{2!} + \frac{2}{3!} + \cdots + \frac{k}{(k+1)!} + \frac{k+1}{(k+2)!} = \frac{(k+1)!-1}{(k+1)!} + \frac{k+1}{(k+2)!} = \frac{(k+2)((k+1)!-1)+(k+1)}{(k+2)!}$

$= \frac{(k+2)!-1}{(k+2)!}$ $\underline{S_{k+1} \text{ holds}}$

So S_n holds for any $n \ge 1$.

Chap 22: Factoring into primes.

<u>Thm 1</u>: Every ideal of $\mathbb{Z}$ is principal.

<u>Proof</u>: Let J be an ideal of $\mathbb{Z}$. If $J \neq \{0\}$, Pick the least positive integer in J and call it n. Then $J = \langle n \rangle$: $\forall m \in J$. $m = qn + r$ with $0 \le r < n$

$$\underset{0 \le r < n}{\Rightarrow r = m - qn \in J} \Rightarrow r = 0 \Rightarrow m = qn$$

<u>Thm 2</u>: The only invertible elements of $\mathbb{Z}$ are 1 and -1.

<u>Pf</u>: s invertible $\Rightarrow \overset{\exists r \in \mathbb{Z}}{sr = 1} \Rightarrow s = 1, r = 1$ or $s = -1, r = -1$.

<u>Def</u>: An integer t is called a common divisor of integer r and s if $t | r$ and $t | s$.

A greatest common divisor of r and s is an integer t s.t. (i) $t | r$ and $t | s$, and (ii) For any integer u, if $u | r$ and $u | s$, then $u | t$.

<u>Thm 3</u>: Any two nonzero integers r and s have a greatest common divisor t. Furthermore, t is equal to a "linear combination" of r and s: $t = kr + ls$ for some integers k and l.

<u>Proof</u>: $J = \{ ur + vs ;\ u, v \in \mathbb{Z} \}$ is an ideal. By Thm 1, $J = \langle t \rangle$ for a $t \in \mathbb{Z}$.

We show that t is a greatest common divisor of r and s

(i) $r \in \langle t \rangle \Rightarrow t | s$, $s \in \langle t \rangle \Rightarrow t | s$

(ii) If $m | r$ and $m | s$, then $m | ur + vs, \forall u, v \in \mathbb{Z} \Rightarrow m | t$.

<u>Warning</u>: m is a linear combination of r and s $\not\Rightarrow m = \gcd(r, s)$:

$5 = 2 + 3$ but $5 \nmid 2, 5 \nmid 3$

However:

$$\boxed{\gcd(r, s) = 1 \Longleftrightarrow \exists\, k, l \in \mathbb{Z} \text{ s.t. } kr + ls = 1}$$

r.s are relatively prime

- Composite number lemma: If a positive integer m is composite, then $m=rs$ where $1<r<m$ and $1<s<m$.

- Euclid's lemma: Let m and n be integers, and let p be a prime.

  If $p \mid (mn)$, then either $p \mid m$ or $p \mid n$.

  Pf. If $p \nmid m$, then $(p,m)=1 \Rightarrow pk+ml=1 \Rightarrow pkn+mnl=n$

$$\Downarrow$$

$$p \mid n$$

Cor: Let $m_1,\cdots,m_t$ be integers, and let p be a prime. If $p \mid (m_1\cdots m_t)$, then $p \mid m_i$ for one of the factors m_i among $m_1,\cdots,m_t$.

Cor: Let $q_1,\cdots,q_t$ and p be positive primes. If $p \mid (q_1\cdots q_t)$, then p is equal to one of the factors $q_1,\cdots,q_t$.

Thm 4 (Factorization into primes) Every integer $n>1$ can be expressed as a product of positive primes: $n=p_1p_2\cdots p_r$

Thm 5 (Unique factorization) Suppose n can be factored into positive primes in two ways, $n=p_1\cdots p_r=q_1\cdots q_t$. Then $r=t$ and the p_i are the same number q_j except possibly for the order in which they appear.

Exer B.7: $\gcd(a,b)=c$, $a=ca'$ and $b=c\cdot b' \Rightarrow \gcd(a',b')=1$

Pf: If $\gcd(a',b')=d>1$ then $a=ca'=cd\cdot\left(\frac{a'}{d}\right)$, $b=c\cdot b'=cd\left(\frac{b'}{d}\right) \Rightarrow \begin{array}{l} cd \mid a \\ cd \mid b \end{array}$

$cd \nmid c$. this contradicts the assumption that $c=\gcd(a,b)$

$cd>c$

Exer C.3 If $a \mid d$ and $c \mid d$ and $\gcd(a,c)=1$, then $ac \mid d$

Pf: $d=ak=cl$ $\quad \gcd(a,c)=1 \Rightarrow ar+cs=1$. $r,s\in\mathbb{Z}$

$\Rightarrow d=d1=dar+dcs=clar+akcs=ac(lr+ks) \Rightarrow ac \mid d$.

Exer D.3 $d=\gcd(a,b)$. For any integer x, $d|x$ iff x is a linear combination of a and b

$d=\gcd(a,b) \Rightarrow d=au+bv$ for $u,v\in\mathbb{Z}$.

$d|x \Leftrightarrow x\in(d) \Rightarrow x=dk=(au+bv)k=a(uk)+b(vk)$ for $k\in\mathbb{Z}$

Conversely. $x=ar+bs \Rightarrow \gcd(a,b)|x$.

Exer E.1: Suppose a is odd and b is even or vice versa. Then
$\gcd(a,b)=\gcd(a+b,a-b)$.

Pf: $\gcd(a,b)|a+b$, $\gcd(a,b)|a-b$ $\Rightarrow \gcd(a,b)\,|\,\gcd(a+b,a-b)$

Let $d=\gcd(a+b,a-b)$. Then $d|2a$, $d|2b$. a odd, b even $\Rightarrow a+b$ is odd $\Rightarrow d$ is odd $\Leftrightarrow (d,2)=1$

$2a=(a+b)+(a-b)$
$2b=(a+b)-(a-b)$.

$\Downarrow$ $d|a$ and $d|b \Rightarrow d|\gcd(a,b)$

So $\gcd(a,b)=\gcd(a+b,a-b)$.

Exer F.9 $\gcd(a,b)=c$, and $\mathrm{lcm}(a,b)=d$. Then $cd=ab$

$$\mathrm{lcm}(a,b)=\frac{ab}{\gcd(a,b)} \Rightarrow \mathrm{lcm}(a,b)\cdot\gcd(a,b)=ab.$$

G.4. If $c=\mathrm{lcm}(a,b)$. then $(a)\cap(b)=(c)$

Pf. $m\in(a)\cap(b) \Leftrightarrow a|m$ and $b|m \Leftrightarrow c|m \Leftrightarrow m\in(c)$

Ex: $a|m$, $b|m$ $\gcd(a,b)=1 \Rightarrow ab|m$.

Pf. $\mathrm{lcm}(a,b)=\dfrac{ab}{\gcd(a,b)}=ab \Rightarrow ab|m$