ALGEBRA NOTES : CHAPTER 1

JOHNEW ZHANG

1. The Introduction toAbstract Algebra

The integers: $\mathbb{Z} = \{0, 1, 2, \ldots\}$
$[S_1]$ The integers consist of the set $\mathbb{Z}$ and the operations "+" and "$\cdot$".
$[A_1]$ $\forall$ a, b $\in \mathbb{Z}$, $a + b = b + a$ (*commutativity of addition*)
$[A_2]$ $\forall$ a, b, c $\in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ (*associativity of addition*)
$[A_3]$ There is an element $0 \in \mathbb{Z}$, such that $a + 0 = a$, $\forall$ a $\in \mathbb{Z}$ (*additive identity*)
$[A_4]$ $\forall$ a $\in \mathbb{Z}$, there is an element -a $\in \mathbb{Z}$, so that $a + (-a) = 0$ (*additive inverse property*)
$[M_1]$ $\forall$ a, b $\in \mathbb{Z}$, $ab = ba$ (*commutativity of multiplication*)
$[M_2]$ $\forall$ a, b, c $\in \mathbb{Z}$, $(ab)c = a(bc)$ (*associativity of multiplication*)
$[M_3]$ There is a and $1 \in \mathbb{Z}$, so that $1 \cdot a = a \cdot 1 = a$, $\forall$ a $\in \mathbb{Z}$ (*multiplicative identity*)
$[D_1]$ $\forall$ a, b, c $\in \mathbb{Z}$, $(a + b) \cdot c = ac + bc$, (*distributivity of multiplication*)

Other things that satisfy these properties
$\mathbb{R}$ (the set of real numbers) with usual "+" and "$\cdot$".
$\mathbb{Q}$ (the set of rational numbers)

A set $\mathbb{R}$ with the operations "+" and "$\cdot$"satisfies all of these properties is called a *commutative rings.* ■

E.G., let $\mathbb{F}_2(or\mathbb{Z}_2)$ be the set {0,1}

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

This is a commutative ring. ■

Sometimes we will study rings with an additional property.

$[M_4]$ $\forall\ a \neq 0$, there is an element a^{-1} such that $a \cdot a^{-1} = 1$ (*multiplicative inverse*)
A commutative ring satisfying M_4 is called a *field*.
E.G., $\mathbb{Q}$ is a field. $\mathbb{R}$ is a field. $\mathbb{Z}$ is not a field. $\mathbb{F}_2$ is a field.

Let M be the set of 2×2 matrices with integers entries
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$
$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & bf \\ cg & dh \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ It is not commutative rings.
$[D_2]$ $\forall a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$

2. Induction Principle

Induction Some statement about nature number n, suppose that P(1) holds and suppose that whenever P(k) is true for $(1 \geq k < n)$, then P(n) is true. Then P(n) holds for all n. ■

InductionSteps 1. Check the base case.
2. Assume that P(K) holds $\forall k \in [1, n)$
3. Prove that P(k + 1) holds
4. Conclusion

WellOrderingPrinciple : Every non-empty subset of $\mathbb{N}$ contains a least element.

Proof. Contrapositive
Let P(n) be "$n \notin S$", where S has no least element.
1. Base Case P(1) holds since if $1 \in S$, S has a least element.
2. Assume P(k) $\forall k \in [1, n)$ (n here is at least 2), so $k \notin S$. Then $n \notin S$. Therefore P(n) holds.
By induction, P(n) holds for all n, so $n \notin S, \forall n \notin \mathbb{N}$, $S = \emptyset$. In conclusion, the well ordering principle holds. □

3. Primes and Divisibility

Definition In a commutative rings, $\mathbb{R}$, if $a, b \in \mathbb{R}$, we say $a|b$ ("a divides b"), if and only if there exists $c \in \mathbb{R}$ such that $b = ac$.

Definition A prime (integer) is a positive integer $p \neq 1$, such that the only divisors of p in $\mathbb{Z}$ are ± 1, $\pm p$.

UniqueFactorization Every integer can be written in the form $\pm 1 \cdot p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, where $a_i > 0$, the p_i are primes. And this representation is unique to reordering.

Proof. (of existence)

Let $n \geq 1$, P(n) be the statement that there exists a way of writing $n = 1 \cdot p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$.

Base case, P(1) is true, since 1= 1.

Suppose P(k) holds $\forall k \in [1, n)$ $(n \geq 2)$.

If n is prime, then P(n) holds, $\because n = n$.

If n is not prime, we can write $n = ab$, where $1 \leq a, b < n$. We can write a and b as products of prime powers since P(a) and P(b) holds. Therefore we can write $n = ab$ as a product of prime powers. □

Theorem There are infinitely many primes.

Proof. Suppose not, and list all of the primes $p_1, p_2, \dots, p_n$. Then $p_1 p_2 p_3 \dots p_n + 1$ is divisible by any prime.

If $p_1 | p_1$ and $p_1 | p_1 p_2 p_3 \dots p_n + 1$, then $p_1 | (p_1 p_2 p_3 \dots p_n + 1) + (-p_2 p_3 \dots p_n) p_1 = 1$

Contradiction, so there are infinitely many primes. □

Definition 1. *Let* $\Pi(x)$ = *the number of primes less than* x. $\Pi(x) : \mathbb{R} \to \mathbb{N} \cup \{0\}$

Theorem Let P_n be the nth prime. Then $P_n \leq 2^{2^{n-1}}$.

Proof. Base case : $n = 1$, then $P_1 = 2 < 2^{2^{1-1}}$. it holds.

Suppose $P_k \leq 2^{2^{k-1}}$, then

$$
\begin{aligned}
p_1 p_2 p_3 \dots p_{k-1} + 1 &\leq 2^{2^0} 2^{2^1} \dots 2^{2^{k-1}} + 1 \\
&= 2^{\frac{1-2^{k-1}}{1-2}} + 1 \\
&= 2^{2^{k-1}-1} + 1 \\
&= \frac{1}{2} 2^{2^{k-1}} + 1 \\
&\leq 2^{2^{k-1}}
\end{aligned}
$$

so $p_1 p_2 p_3 \dots p_{k-1} + 1 \leq 2^{2^{n-1}}$

But $p_1p_2p_3 \dots p_{k-1} + 1$ is divisible by some prime $q \geq P_n$ so that $P_n \leq q \leq p_1p_2p_3 \dots p_{k-1} + 1 \leq 2^{2^{k-1}}$.

By induction, the theorem holds. $\square$

In particular, $\Pi(x) \geq log_2(log_2(x))$ (for $x > 1$) $\blacksquare$

Theorem For primes, $\sum \frac{1}{p}$ diverges.

Proof. Suppose that $\sum_{n-1}^{\infty} \frac{1}{p_n}$ converges.

($p_n = nthprime$) If this is true, then there exists $k \geq 1$ such that $\sum_{n=k+1}^{\infty} \frac{1}{p_n} < \frac{1}{2}$.

Let $N = 4^{k+1}$, we'll count the elements of $1, 2, 3, 4, \dots, N$.

Let $X = \{1 \leq a \leq N : Pi|a$ for some $i \geq k+1\}$.

Let $Y = \{1 \leq a \leq N$: a is not in $X\}$.

It should be clear that $\#X + \#Y = Y$.

Each element of X is divisible by some prime p_i, $\forall i \geq k+1$

The number of integers from 1 to N.

Divisible by p_i is at most $\frac{N}{p_i}$.

Reason: If $p_i|x$, $x = p_im$, and $1 \leq m \leq \frac{N}{p_i}$.

$\therefore$#X $\leq \sum_{i=k+1}^{\infty}$(# of $1 \leq x \leq N$, divisible by p$_i$)$\leq \sum_{i=k+1}^{\infty} \frac{N}{p_i} = N \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{N}{2}$

Now we count the element of Y.

Every element of Y can be written as $p_i^{e_i} p_2^{e_2} \dots p_k^{e_k} \dots$ for some $e_i \geq 0$.

It follows that every element of Y can be written as $p_i^{a_i} p_2^{a_2} \dots p_k^{a_k} b^2$, where $a_i = 0$, or 1 for all i.

If $p_i^{a_i} p_2^{a_2} \dots p_k^{a_k} b^2 \leq N$, certainly $b \leq \sqrt{N}$ since b is an integer, this leaves at most $\sqrt{N}$ choices for b.

Since each a_i is either 0 or 1, there are only 2^k choices for $a_1, a_2, \dots a_k$.

Therefore the number of integers $1 \leq x \leq N$, which can be written in the form $x = p_i^{a_i} p_2^{a_2} \dots p_k^{a_k} b^2$, for $b \in \mathbb{N}$ and $a_i = 0$ or 1, is at most $2^k\sqrt{N}$, $\therefore$# Y$\leq 2^k\sqrt{N}$

$2^k\sqrt{N} = 2^k\sqrt{4^{k+1}} = 2^{2k+1} = \frac{1}{2}4^{k+1} = \frac{N}{2}$

$\#Y \leq \frac{N}{2}$

We assumed that $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converges and shows that for some N, $N = \#X + \#Y < N$.

Contradiction, the theorem holds.

$\square$

Theorem Let $a \geq 1$ and b be integers, then there exist integers q and $0 \leq r < a$ such that $b = aq + r$.

Proof. Let $S = \{s : s = b - aq$ for some $q \in \mathbb{Z}$ and $s \geq 0\}$

This is non-empty, since $a \geq 0$.
So we can choose q with $b - aq \geq 0$
$S \subseteq \{0, 1, 2, 3, \ldots\}$
So if $S \neq \emptyset$, S has a least element, call $r \in S$.
$r = b - aq$ for some $q \in \mathbb{Z}$
Also, $r \geq 0$,
Suppose $r \geq a$
Then $r - a \geq 0$, and $b = aq + r = a(q + 1) + (r - a)$
$\therefore$r-a$\in S$. But $r - a < r$.
contradiction, $r < a$.

□

Definition 2. *Let $a, b \in \mathbb{Z}$ be non-zero. Then $gcd(a, b)$ is the large $d \in \mathbb{Z}$ such that $d|a$ and $d|b$.*

Remarks :
1. If $d|a$, and $a \neq 0$, then $d \leq |a|$.
2. We can define $gcd(a, 0)$ if $a \neq 0$, just by $gcd(a, 0) = gcd(0, a) = a$. $gcd(0, 0)$ does not make sense.

EuclideanAlgorithm :
1. $(gcd(a, b))$, Set things up so that $b > a > 0$.
2. If $a = 0$, $gcd(b, a) = b$
3. Write $b = aq + r$, $0 \leq r < a$, and repeat to compute $gcd(a, r)$.

Bezaut'sidentity :If a and b are positive integers, then there exists integers s and t so that $as + bt = gcd(a, b)$. (note, this is called an "integer linear combination" of $a, b \in \mathbb{Z}$).

FatoringIntegers:
lemma: If a and b are non-zero integers with $gcd(a, b) = 1$ and $a|bc$, then $a|c$.
lemma: Let p be a prime and suppose that $p|a_1a_2 \ldots a_n$ $(a_i \in \mathbb{Z})$. Then $p|a_i$ for some i.

UniqueFactorizationOfIntegers :We have show that every $n \geq 2$ can be written as $n = p_1p_2p_3 \ldots p_r$ for some primes (they may repeat).