Week 11

Ring: R (Review)

$\mathcal{R}_1$. $< R, + >$ is an abelian group.

$\mathcal{R}_2$. Multiplication is associative.

$\mathcal{R}_3$. $\forall\ a, b, c \in R,\ a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c.$

Defn. (Boolean ring)

A ring R is a Boolean ring if $a^2 = a$ for all $a \in R$, i.e. every element is idempotent.

Theorem A Boolean ring is commutative.

Proof. $\forall\ a, b \in R$, $(a + b)^2 = a + b$, $ab + ba = 0$. $\forall\ x \in R$ $(x + x)^2 = 2x$. Hence $2x = 0$. $2ab + ba = ab \Rightarrow ba = ab$. ■

Exercise Prove or disprove that if R is a ring with $a^3 = a\ \forall\ a \in R$, then R is commutative.

Example (Boolean Algebra)

Let R be the set of all subsets of a nonempty set S, i.e., $R = P(S)$. Define $\forall\ A, B \in R$, $A + B = (A \cup B) \setminus (A \cap B)$ and $A \cdot B = A \cap B$. Then $< R, +, \cdot >$ is a Boolean ring.

Integral Domain

Defn. (Zero Divisor)

If a and b are nonzero elements of a ring R such that $ab = 0$, then a and b are **zero divisors**.

Theorem In $\mathbb{Z}_n$, the divisors of zero (zero divisor) are precisely those nonzero elements which are not coprime (relatively prime) to n.

Corollary Let p be a prime, then $\mathbb{Z}_p$ has no zero divisors.

Theorem The cancellation laws hold in a ring R if and only if R has no zero divisors.

Proof. ($\Rightarrow$) Suppose not. Let $a, b \neq 0$ and $ab = 0$. Since $ab = 0 = a0$, by cancellation law, $b = 0$.$\rightarrow\leftarrow$
($\Leftarrow$) Let $ab = ac$ where $a \neq 0$. Then $a(b - c) = 0$. Now, if $b - c \neq 0$, then a is a zero divisor. Hence $b - c = 0$ which implies $b = c$. ■

Defn. (Integral domain)

An integral domain D is a commutative ring with unity $1 \neq 0$ and containing no zero divisors.

Example $\mathbb{Z}$, $\mathbb{Z}_p$ (p is a prime) and $\mathbb{Z}[x]$ are integral domains.

Example $M_2(\mathbb{Z}_2)$, the set of all 2×2matrices with entries in $\mathbb{Z}_2$ is not an integral domain. (It is a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.)

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Theorem Every field F is an integral domain.

Proof. Since $ab = 0 \Rightarrow a = 0$ or $b = 0$, F is an integral domain. ■

Theorem Every finite integral domain R is a field.

Proof. Let $R = \{0, 1, a_1, a_2, \cdots, a_n\}$. $\forall\ a \neq 0,\ a \in R$,

$\{a1, aa_1, aa_2, \cdots, aa_n\} = \{1, a_1, a_2, \cdots, a_n\}$ (?)

Hence $aa_i = 1$ and a_i is the multiplicative inverse of a. ■

Corollary $\mathbb{Z}_p$ is a field if and only if p is a prime.

Defn. (The Characteristic of a Ring)

The least positive integer n (if exists) satisfying $na = 0$,

$\forall\ a \in R$(ring) is called the characteristic of R denoted by $ch(R)$.

Otherwise, R is of characteristic 0.

Example $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$ are of characteristic 0 and $\mathbb{Z}_n$, $\mathbb{Z}_n \times \mathbb{Z}_n$ are of characteristic n.

TheoremLet R be a ring with unity. Then $n \cdot 1 \neq 0 \ \forall n \in \mathbb{Z}^+$ implies that $ch(R) = 0$. If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such integer is the characteristic of R.

Proof. $na = a + a + \cdots + a = a \cdot (n \cdot 1)$. ■

Theorem If F is a field with finite elements, then $ch(F) = p$ for some prime p.

Proof. Since F is finite, $ch(F)$ must be finite, let $ch(F) = n$. If n is not a prime, then $n = n_1 n_2$ where n_1, $n_2 \in \mathbb{Z}^+$ and n_1, $n_2 > 1$. By the fact that $n \cdot 1 = 0 \Rightarrow n_1 n_2 \cdot 1 = 0 \Rightarrow (n_1 \cdot 1)(n_2 \cdot 1) = 0$. This implies that $n_1 \in F$ and $n_1 \cdot 1$ is a zero divisor. $\rightarrow\leftarrow$ ■

We can use the idea of group to discover basic properties of Number Theory.

$(*)$ Let F be a field. Then $F^* = F \setminus \{0\}$ is a **group under the field multiplication**.

$(**)$ The multiplication in $\mathbb{Z}_n$ is defined as follows:
$\forall\ 0 \leq a, b \leq n-1$, $(a + \mathbb{Z}_n)(b + \mathbb{Z}_n) = ab + \mathbb{Z}_n$.
$(a + rn)(b + sn) = ab + (as + br + rsn)n \ \in \ ab + \mathbb{Z}_n$.

(Fact) $< \mathbb{Z}_p^*, \cdot >$ is a group of order $p - 1$.
(Fact) $\forall\ \bar{a} \in \mathbb{Z}_p^*\ \ (\bar{a})^{p-1} = \bar{1}$, i.e., $a^{p-1} \equiv 1 (\text{mod } p)$.

Theorem (Little theorem of Fermat)

If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$, i.e., $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof. Since $a \not\equiv 0 \pmod{p}$, $a + \mathbb{Z}_p \in \mathbb{Z}_p^*$. $(a + \mathbb{Z}_p)^{p-1} = 1 + \mathbb{Z}_p$. This implies that $a^{p-1} \equiv 1 (\text{mod } p)$. ■

Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.

Proof. First, if $a \equiv 0 \pmod{p}$, then $a^p \equiv 0 \equiv a \pmod{p}$. Otherwise $a \not\equiv 0 \pmod{p}$ and thus $gcd(a, p) = 1$. By $a^{p-1} \equiv 1 \pmod{p}$, we have $a^p \equiv a \pmod{p}$. ■

Example Prove that $2^{11,213} - 1$ is not divisible by 11.

pf. $2^{11,213} \equiv 2^{10 \cdot 1121 + 3} \equiv 2^3 \pmod{11}$.

Hence $2^{11,213} - 1 \equiv 7 (\text{mod } 11)$. ■

Note $2^{11,213} - 1$ is a prime. (Mersenne primes: $2^p - 1$ where p is a prime.)

Theorem (Euler)

If $gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. Let G_n be the set of elements $\bar{a} = a + \mathbb{Z}_n$ where $a \in (0, n)$ such that $gcd(a, n) = 1$. Clearly, $|G_n| = \varphi(n)$.

We claim that G_n forms a subgroup of $\mathbb{Z}_n^*$ under multiplication.

(i) $\forall a, b \in G_n$ $gcd(a, n) = 1$ and $gcd(b, n) = 1$, hence $gcd(ab, n) = 1$.

(ii) $1 \in G_n$.

(iii) Since $gcd(a, n) = 1$, there exists an a' s.t. $a'a \equiv 1 \pmod{n}$.

This implies that a' is a multiplication inverse of a. (Note that $gcd(a', n) = 1$). ■

Theorem (Wilson)

If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. First, we claim that 1 and $p-1$ are the only two elements in $\mathbb{Z}_p$ whose inverse (multiplication) are themselves. $1^2 \equiv (p-1)^2 \equiv 1 \pmod{p}$ is easy to see. Let $1 < a < p-1$ $(p \geq 3)$. Since $a^2 \equiv 1 \pmod{p}$ implies that $a-1$ and $a+1$ are zero divisors, we have the proof. a can not be its own inverse element. Now,

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv 1 \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}$.(?) ■