Homework 8

Due date: 2019. 6. 10.

1. Let a belong to a ring R. Let $S=\{x\in R|ax=0\}$. Show that S is a subring of R.

2. Let m and n be positive integers and let k be the least common multiple of m and n. Show that $m\mathbb{Z}\cap n\mathbb{Z}=k\mathbb{Z}$.

3. Give an example of a finite noncommutative ring. Give an example of an infinite noncommutative ring that does not have a unity.

4. Describe all the subrings of the ring of integers.

5. Let $R=\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}$ and $S=\{(a,b,c)\in R|a+b=c\}$. Prove or disprove that S is a subring of R.

6. Find a zero-divisor in $\mathbb{Z}_5[i]=\{a+bi|a,b\in\mathbb{Z}_5\}$.

7. Find all solutions of the equation $x^3-2x^2-3x=0$ in $\mathbb{Z}_{12}$.

8. Find all solutions of $x^2-5x+6=0$ in $\mathbb{Z}_7$.

9. Let x and y belong to a commutative ring R with prime characteristic p. Show that $(x+y)^p=x^p+y^p$.

10. Show that $\mathbb{Z}_7[\sqrt{3}]=\{a+b\sqrt{3}\,|a,b\in\mathbb{Z}_7\}$ is a field.

11. Let F be a field of order 2^n. Prove that $charF=2$.

정수론과암호수학 I – HW8

파이낸스경영학과
2017004093
양 준 우

#1. i) $a \cdot 0 = 0$
$\therefore 0 \in S \Rightarrow S$ is nonempty set.
ii) Let $x, y \in S$
Then $ax = 0$, $ay = 0$
$a(x-y) = ax - ay = 0 - 0 \quad \therefore x-y \in S$
iii) $a(xy) = (ax)y = 0 \cdot y = 0 \quad \Rightarrow xy \in S$
$\therefore S$ is a subring of R.

#2. Since every multiple of k is obviously multiple of both m and n, $k\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ is trivial
Let $x = am = bn$, i.e. $x \in m\mathbb{Z} \cap n\mathbb{Z}$
Let $x = qk + r$, $r < k$
Since x, k are both multiples of m, n then
so is $r = x - qk$
k is the least natural number, therefore $\nleftarrow$
$\therefore x$ is multiple of k
$\Rightarrow m\mathbb{Z} \cap n\mathbb{Z} \subset k\mathbb{Z}$
$\therefore m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$

#3. Example for finite noncommutative ring.
$M_2(\mathbb{Z}_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_p \right\}$, p is prime.
$M_2(\mathbb{Z}_p)$ is commutative group under addition.
matrix multiplication is not commutative.
Also, it satisfies that for all $x, y \in M_2(\mathbb{Z}_p)$,

$(xy)z = x(yz)$, $(x+y)z = xz+yz$

$\therefore M_2(\mathbb{Z}_p)$ is noncommutative ring.

Example for infinite noncommutative ring without unity

$\therefore M_2(2\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in 2\mathbb{Z} \right\}$

#4. $n\mathbb{Z}$ only.

All the subgroups of $\mathbb{Z}$ have the form $n\mathbb{Z}$, when $0 \leq n \in \mathbb{Z}$

need to show $n\mathbb{Z}$ is a subring

If $x, y \in n\mathbb{Z}$, then

$x = np$, $y = nq$ when $p, q \in \mathbb{Z}$

$xy = npnq = n^2pq = n(npq) \in \mathbb{Z}$

$\therefore n\mathbb{Z}$ is closed under multiplication

$\therefore n\mathbb{Z}$ is a subring of the ring of integers.

#5. Consider $x = (1,0,1)$ and $y = (0,1,1)$

Both x, y belong to S.

However $xy = (0,0,1)$, $xy \notin S$.

Therefore S is not a subring of $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$

#6. Since $(3+i)(2+i) = 5+5i = 0+0i$

$3+i$ is a zero divisor in $\mathbb{Z}_5[i]$

#7. Let $f(x) = x^3 - 2x^2 - 3x$ in $\mathbb{Z}_{12}$

then $f(0) = 0$

$f(1) = 1 - 2 - 3 = -4 = 8$

$f(2) = 8 - 2 \cdot 4 - 3 \cdot 2 = -6 = 6$

$f(3) = 27 - 2 \cdot 9 - 3 \cdot 3 = 0$

$f(4) = 64 - 2\cdot 16 - 3\cdot 4 = 20 = 8$

$f(5) = 125 - 2\cdot 25 - 3\cdot 5 = 60 = 0$

$f(6) = 216 - 2\cdot 36 - 3\cdot 6 = 126 = 6$

$f(7) = 343 - 2\cdot 49 - 3\cdot 7 = 224 = 8$

$f(8) = 512 - 2\cdot 64 - 3\cdot 8 = 360 = 0$

$f(9) = 729 - 2\cdot 81 - 3\cdot 9 = 540 = 0$

$f(10) = 1000 - 2\cdot 100 - 3\cdot 10 = 770 = 2$

$f(11) = 1331 - 2\cdot 121 - 3\cdot 11 = 1056 = 0$

$\therefore \{0, 3, 5, 8, 9, 11\}$

#8. All these rings we can factorize the polynomial $x^2 - 5x + 6 = 0$ to $(x-2)(x-3)$
Since $\mathbb{Z}_7$ is a field, we must have either $x-2=0$ or $x-3=0$. $\therefore x = 2, 3$

#9. Binomial theorem, $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} \cdot y^k$
For $1 \le k \le p-1$, we have that $\frac{p!}{(p-k)!k!} = \binom{p}{k} \in \mathbb{Z}$
$\Rightarrow (p-k)!\,k! \mid p!$
Since $1 \le k \le p-1$ and p is prime, it follows that $(p-k)!\,k!$ is coprime to p $\Rightarrow (p-k)!\,k! \mid (p-1)!$
$\therefore (p-k)!\,k! \cdot n_k = (p-1)!$ for some $n_k \in \mathbb{Z}$
Thus, $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}\right) + y^p$
$= x^p + \left(\sum_{k=1}^{p-1} n_k x^k y^{p-k}\right) + y^p$
$= x^p + y^p$, since R has characteristic p.

#10. For $a + b\sqrt{3}$, define its norm as function
$N : \mathbb{Z}_7[\sqrt{3}] \to \mathbb{Z}$ with $N(a+b\sqrt{3}) = a^2 - 3b^2$
$N(x,y) = N(x) \cdot N(y)$ is obvious.
Assume that $xy = 0$, for some $x, y \neq 0 \in \mathbb{Z}_7[\sqrt{3}]$

Then $N(xy) = N(x) \cdot N(y) = N(0) = 0$.
$\Rightarrow N(x) = 0$ or $N(y) = 0$, since $N(x), N(y) \in \mathbb{Z}$
Assume $N(x) = 0$, $x = a + b\sqrt{3}$
Then $a^2 - 3b^2 = 0$ for some $a, b \in \mathbb{Z}_7$
Consider this equation in modulo 7.
$k^2 \equiv 0, 1, 2, 4 \pmod 7$
$3l^2 \equiv 0, 3, 5, 6 \pmod 7$ for $\forall k, l \in \mathbb{Z}$
no combination exists for equation $a^2 - 3b^2 = 0$ except $(0,0)$
$\therefore a^2 - 3b^2 = 0$ implies $a = b = 0$
$\Rightarrow$ There are no zero divisors in $\mathbb{Z}_7[\sqrt{3}]$
$\therefore \mathbb{Z}_7[\sqrt{3}]$ is a field.

#11. F: field of 2^n
we know that char F = 1!1
Since the order of the field is 2^n, the order of 1 divides 2^n. But F is a field and all fields are integral domains.
By Thm 13.4, we know that the characteristic of an integral domain is eigher 0 or prime.
$\therefore$ The characteristic of F is a prime and devides 2^n
$\therefore$ char F = 2