Jason Tsang

Group 4

A^+ Excellent!

Algebra

48, Monic polynomial degree 2 in $\mathbb{Z}_2[X]$.

X^2	X^1	X^0
1	2	1
1	2	2
1	1	1
1	1	2

① $X^2+\bar{2}X+\bar{1} = X^2+\bar{1}$

② $X^2+\bar{2}X+\bar{2} = X^2 = XX$

③ $X^2+X+\bar{1} = X^2+X+\bar{1}$

④ $X^2+X+\bar{2} = X^2+X = X(X+1)$

① $X^2+\bar{1} = X^2-\bar{1} = (X+\bar{1})(X-\bar{1})$

③ Let $f(X) = X^2+X+\bar{1}$

$\mathbb{Z}_2[X] = \{\bar{0},\bar{1}\}$

$f(\bar{0}) = \bar{0}^2+\bar{0}+\bar{1} = \bar{1}$

$f(\bar{1}) = \bar{1}^2+\bar{1}+\bar{1} = \bar{3}$

No roots $\Rightarrow$ irreducible

in deg2 polynomial

So the only irreducible monic deg2 polynomial is $X^2+X+\bar{1}$. good

Monic polynomial degree 3 in $\mathbb{Z}_2[X]$

X^3	X^2	X^1	X^0
1	2	1	1
1	2	2	1
1	2	1	2
1	2	2	2
1	1	2	2
1	1	2	1
1	1	1	2
1	1	1	1

① $X^3+\bar{2}X^2+X+\bar{1} = X^3+X+\bar{1}$

② $X^3+\bar{2}X^2+\bar{2}X+\bar{1} = X^3+\bar{1}$

③ $X^3+\bar{2}X^2+X+\bar{2} = X^3+X = X(X^2+1)$

④ $X^3+\bar{2}X^2+\bar{2}X+\bar{2} = X^3 = XXX$

⑤ $X^3+X^2+\bar{2}X+\bar{2} = X^3+X^2 = X^2(X+1)$

⑥ $X^3+X^2+\bar{2}X+\bar{1} = X^3+X^2+\bar{1}$

⑦ $X^3+X^2+X+\bar{2} = X^3+X^2+X = X(X^2+X+$

⑧ $X^3+X^2+X+\bar{1} = X^3+X^2+X+\bar{1}$

Look at ①, ②, ⑥, ⑧

①, Let $f(X) = X^3 + X + \bar{1}$

$f(\bar{0}) = \bar{0}^3 + \bar{0} + \bar{1} = \bar{1}$

$f(\bar{1}) = \bar{1}^3 + \bar{1} + \bar{1} = \bar{3}$

② $X^3 + \bar{1} = (X + \bar{1})(X^2 - X + 1)$

⑥ Let $f(X) = X^3 + X^2 + \bar{1}$

$f(\bar{0}) = \bar{0}^3 + \bar{0}^2 + \bar{1} = \bar{1}$

$f(\bar{1}) = \bar{1}^3 + \bar{1}^2 + \bar{1} = \bar{3}$

⑧ $X^3 + X^2 + X + 1 = (X+\bar{1})(X^2+\bar{1})$ ✓

So the only irreducible degree 3 polynomials in $\mathbb{Z}_2[X]$ are

$X^3 + X + \bar{1}$ ✓ and $X^3 + X^2 + \bar{1}$ ✓ Excellent

52) $X^4 - \bar{2}$ in $\mathbb{Z}_7[X]$

$$X^4 - \bar{2} = X^4 - \bar{9} = (X^2 + \bar{3})(X^2 - \bar{3})$$
$$= (X^2 - \bar{4})(X^2 - \bar{3})$$
$$= (X + \bar{2})(X - \bar{2})(X^2 - \bar{3})$$ ✓ Nice

$X^3 - \bar{3}$ in $\mathbb{Z}_7[X]$

$\bar{1}^3 = \bar{1}$ $\quad \bar{0}^3 = \bar{7}^3 = \bar{0}$

$\bar{2}^3 = \bar{1}$

$\bar{3}^3 = \bar{6}$ $\quad \therefore X^3 - \bar{3}$ has no roots in $\mathbb{Z}_7[X]$ ✓ good

$\bar{4}^3 = \bar{1}$

$\bar{5}^3 = \bar{6}$ $\quad$ No roots in deg 3 polynomial $\Leftrightarrow$ irreducible.

$\bar{6}^3 = \bar{6}$

53, $f(x) = 2x^5 - 3x^2 + 3$

$b \mid 3$ and $c \mid 2$

$b = \pm 1$ or $b = \pm 3$ $\quad$ $c = \pm 1$ or $c = \pm 2$

Candidate roots are $\pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2}$ ✓

$$f(1) = 2 \neq 0$$
$$f(-1) = 4 \neq 0$$
$$f(3) = 462 \neq 0$$
$$f(-3) = -510 \neq 0$$
$$f(\tfrac{1}{2}) = \tfrac{37}{16} \neq 0$$
$$f(-\tfrac{1}{2}) = \tfrac{35}{16} \neq 0$$
$$f(\tfrac{3}{2}) = \tfrac{183}{16} \neq 0$$
$$f(-\tfrac{3}{2}) = -\tfrac{303}{16} \neq 0$$ ✓

Hence $2x^5 - 3x^2 + 3$ has no rational roots. ✓

Let $h(x) = 7x^4 - 2x^3 + 35x - 10$

$b \mid -10$ $\quad$ $c \mid 7$

$b = \pm 1, b = \pm 2, b = \pm 5$ $\quad$ $c = \pm 1, \pm 7$

$b = \pm 10$

Candidate roots are $\pm 1, \pm 2, \pm 5, \pm 10, \pm \frac{1}{7}, \pm \frac{2}{7}, \pm \frac{5}{7}, \pm \frac{10}{7}$ ✓

$f(\frac{2}{7}) = 0$ ✓

So now $h(x) = (x - \frac{2}{7})(7x^3 + 35)$
$= (7x - 2)(x^3 + 5)$ ✓

$b \mid 5$ $\quad c \mid 1$

$b = \pm 1,\ b = \pm 5$ $\quad c = \pm 1$

New candidate roots are ± 1, ± 5

$h(1) = 30 \neq 0$
$h(-1) = -36 \neq 0$
$h(5) = 4290 \neq 0$
$h(-5) = 4440$

So $7X^4 - 2X^3 + 35X - 10$ has one rational root which is $\frac{2}{7}$. ✓

Let $g(X) = X^{12} + 37X - 4$

$b \mid 4$ $\quad c \mid 1$

$b = \pm 4, \pm 2, \pm 1$ $\quad c = \pm 1$

Candidate roots are ± 4, ± 2 and ± 1 ✓

$f(4) = 16777360 \neq 0$
$f(-4) = 16777064 \neq 0$
$f(2) = 4166$
$f(-2) = 4018$
$f(1) = 34$
$f(-1) = -40$

Hence there are no rational roots in $X^{12} + 37X - 4$. ✓

Perfect!

Every finite integral domain is a field.

~~Let R be a finite integral domain~~. Since a integral domain satisfies all the axioms to be a field except the multiplicative inverse axiom. Only need to prove that every element has a multiplicative inverse. ✓

Let R be a finite integral domain and $a \in R$ with $a \neq 0$. Since R is finite, there exist positive integers j and k with $j < k$ such that $a^j = a^k$ ✓ Thus $a^k - a^j = 0$. Since $j < k$ and j and k are positive integers, $k-j$ is a positive integer. Therefore, $a^j(a^{k-j} - 1) = 0$. Since $a \neq 0$ and R is an integral domain, $a^j \neq 0$. Thus $a^{k-j} - 1 = 0$. ✓ Hence $a^{k-j} = 1$. Since $k-j$ is a positive integer, $k-j-1$ is a nonnegative integer. ✓ Thus, $a^{k-j-1} \in R$. Note that $a \cdot a^{k-j-1} = a^{k-j} = 1$. ✓ Hence, a has a multiplicative inverse in R. It follows that R is a field. ✓

Lovely!

– keep up the good work! ☺