Tutorial-3
2019MCS2574

Q1. Let $Q[\sqrt{3}] = \{a+b\sqrt{3} \mid a,b \in Q\}$. That $Q[\sqrt{3}]$ is a commutative ring with identity. Prove that $Q[\sqrt{3}]$ is a field.

Since $Q[\sqrt{3}]$ is a commutative ring with unity.
To prove $Q[\sqrt{3}]$ is also a field we need to show for any element (Non-zero) of $Q[\sqrt{3}]$ there exist a multiplicative inverse.

Let $a+b\sqrt{3} \in Q[\sqrt{3}]$ s.t $a \neq 0$ and $b \neq 0$
s.t $c+d\sqrt{3}$ is it's multiplicative inverse.

Hence $(a+b\sqrt{3})(c+d\sqrt{3}) = 1$

$$(ac+3bd) + (ad+bc)\sqrt{3} = 1$$

So
$$ac+3bd = 1$$
$$ad+bc = 0$$

Solving linear eq^n using matrix

$$\begin{bmatrix} a & 3b \\ b & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a & 3b \\ b & a \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$= \frac{1}{a^2-3b^2} \begin{bmatrix} a & -3b \\ -b & a \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} c \\ d \end{bmatrix} = \frac{1}{a^2-3b^2} \begin{bmatrix} a \\ -b \end{bmatrix}$$

Hence multiplicative inverse of $a+b\sqrt{3}$ is

$$\frac{a}{a^2-3b^2} - \left(\frac{b}{a^2-3b^2}\right)\sqrt{2} \in Q[\sqrt{3}]$$

Hence Proved.

Q2. Let Q be the field of rational numbers then show that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$

Let $A = Q(\sqrt{2}, \sqrt{3})$ and $B = Q(\sqrt{2}+\sqrt{3})$.

Since $\sqrt{2}, \sqrt{3} \in A$

Hence $\sqrt{2}+\sqrt{3} \in A$ [Linear combination]

So, it follows $B \subseteq A$ — ①

Next we need to show $\sqrt{2}, \sqrt{3} \in B$.

$$(\sqrt{2}+\sqrt{3})^2 = (2+3) + 2\sqrt{6}$$

$$\Rightarrow \sqrt{6} = \frac{(\sqrt{2}+\sqrt{3})^2 - (2+3)}{2}$$

$\therefore \sqrt{6} \in B$

Since
$$\frac{a(\sqrt{a}+\sqrt{b}) - \sqrt{ab}(\sqrt{a}+\sqrt{b})}{a-b}$$

$$= \frac{a\sqrt{a} + a\sqrt{b} - a\sqrt{b} - b\sqrt{a}}{a-b}$$

$$= \sqrt{a}$$

and
$$\frac{b(\sqrt{a}+\sqrt{b}) - \sqrt{ab}(\sqrt{a}+\sqrt{b})}{b-a}$$

$$= \sqrt{b}$$

replacing $a = \sqrt{2}$, $b = \sqrt{3}$

we get $\sqrt{2} \in B$ and $\sqrt{3} \in B$

$\therefore A \subseteq B$ — ②

using ① and ② we can say that

$A = B$

Hence $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$

Q3 Find a basis of $Q(\sqrt[5]{3})$ over Q.

Let w be root of polynomial $x^5 - 3 = 0$

By Eisenstein's Irreducibilty criterion using $P=3$, we can show that x^5-3 is irreducible over Q.

So we have $[Q(\sqrt[5]{3}) : Q] = 5$

And bases is $\{1, \sqrt[5]{3}, \sqrt[5]{3^2}, \sqrt[5]{3^3}, \sqrt[5]{3^4}\}$

Q4 Gaussian integer is a complex number such that it's real and imaginary parts are both integers. $Z[i] = \{a+ib \mid a, b \in Z\}$ is a ring of Gaussian integers. Prove that the ring of Gaussian integers modulo 3 is a field. Also find its characteristic :

Given $Z[i] = \{a+ib \mid a,b \in Z\}$ is a ring.

To prove ~~$\cancel{}$~~ $\{a+ib \mid a,b \in \mathbb{Z}_3\}$ is a field.

$a, b \in \{0, 1, 2\}$

1. Identity / unity element :

$a+ib \equiv 1 \bmod 3$

$a = 1, \quad b = 0$

2. Commutative :

$(a+ib)(c+id) \equiv (c+id)(a+ib) \bmod 3$

3. Multi-plicative Inverse of non-zero element.

Let $a+ib \in \mathbb{Z}_3$ s.t $a \neq 0$ and $b \neq 0$.

$$(a+ib)^{-1} = \frac{(a-ib)}{(a+ib) * (a-ib)} = \frac{a}{a^2+b^2} - \frac{ib}{a^2+b^2}$$

Since 3 is prime, hence $\gcd(a, 3) = 1$

as $a \in \mathbb{Z}_3$.

Hence $\left(\frac{1}{a^2+b^2}\right) \bmod 3$ is integer s.t $\in \mathbb{Z}_3$

Hence Inverse exists.

4. Characterstic : $x(a+ib) = 0 \bmod 3$, then x must be 3

as $3(a+ib) = 0 \bmod 3 \quad \forall a, b \in \mathbb{Z}_3$

Hence Characterstic $= 3$.

Scanned with CamScanner

Q5. Is $\sqrt{2} + \sqrt[3]{7}$ algebraic over the field of rational numbers? Justify.

To find/check if a ~~n~~ element is algebraic over Q.

Let $f(x) \in Q[x]$

If $f(\alpha) = 0$, ~~and~~ i.e it is root of $f(x)$ the α is algebraic over field Q.

Let $\alpha = \sqrt{2} + \sqrt[3]{7}$

$(\alpha - \sqrt{2}) = \sqrt[3]{7}$

Take cube on both side

$\alpha^3 - 2\sqrt{2} - 3\alpha^2\sqrt{2} + 6\alpha = 7$

$\alpha^3 + 6\alpha - 7 = \sqrt{2}(3\alpha^2 + 2)$

Take square on both side

$(\alpha^3 + 6\alpha - 7)^2 = 2(3\alpha^2 + 2)^2$

$\alpha^6 + 36\alpha^2 + 49 + 12\alpha^4 - 84\alpha - 14\alpha^3 = 18\alpha^4 + 12\alpha^2 + 8$

$\Rightarrow \cancel{\alpha^6 + 24}$

$\Rightarrow \alpha^6 + (-6\alpha^4) + (-14\alpha^3) + 24\alpha^2 + (-84\alpha) + 41 = 0$

Since all co-efficient of above eqn lie in Q

hence $f(x) \in Q[x]$

where $\alpha = \sqrt{2} + \sqrt[3]{7}$ is root of $f(x)$

Hence $\sqrt{2} + \sqrt[3]{7}$ is algebraic over field of ~~a~~ rational numbers.

Q6. Let F be the field of rational numbers and $f(x) = x^4 + x^2 + 1 \in F[x]$. Show that $F(\omega)$ where ω is cube root of unity is a splitting field of $f(x)$. Also determine the degree of splitting field $f(x)$ over F.

cube root of unity $= 1, \omega, \omega^2$

$$1 + \omega + \omega^2 = 0.$$

$f(x) = x^4 + x^2 + 1$

Let $x^2 = z$

$f(z) = z^2 + z + 1$

$z = \omega, \omega^2$

$\therefore x^2 = \omega, \omega^2$

$x = \pm\sqrt{\omega}, \pm \omega$

$\therefore f(x) = (x - \sqrt{\omega})(x + \sqrt{\omega})(x - \omega)(x + \omega)$

where $(x - \text{root})$ is a factor.

Hence $F(\omega)$ is a splitting field of $f(x)$.

Since $f(x)$ is monic irreducible in $F[x]$

Hence degree of splitting field $= 4$.

Q7. Show that $\sqrt{2+\sqrt{3}}$ is algebraic over Q.

Let $x = \sqrt{2+\sqrt{3}}$

squaring both sides

$x^2 = 2+\sqrt{3}$

$(x^2-2) = \sqrt{3}$

squaring both sides

$x^4 + 4 - 4x^2 = 3$

$f(x) \Rightarrow x^4 - 4x^2 + 1 = 0$

$f(x) \in Q[x]$

$x^4 - 4x^2 + 1$ is irreducible over Q.

$\therefore f(\alpha) = 0$, $\alpha = \sqrt{2+\sqrt{3}}$

Hence $\sqrt{2+\sqrt{3}}$ is algebraic over Q.

Q8 Prove that $F_3[x]/x^2+1$ is a field. How many elements does the field have?

$F_3 = \{0, 1, 2\}$

$f(x) = x^2 + 1$

$f(0) \neq 0, \; f(1) \neq 0, \; f(2) \neq 0$

Hence $f(x)$ is a monic irreducible polynomial of F_3

$\therefore \; F_3[x]/x^2+1 = g$

then $\deg(g) < \deg(x^2+1)$

$\therefore \; F_3[x]/(x^2+1)$ is a field as proved in class.

$F_3[x]/x^2+1 = \{a + b\alpha : a, b \in F_3$, where α satisfy $f(x)\}$

i.e $\alpha^2 + 1 = 0$

~~Addition~~ Total # elements in field $= (3)^2 = 9$.

Addition Table

$+$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	2α
2	2	0	1	$2+\alpha$	$2+2\alpha$	α	2α	$1+\alpha$	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	0	$1+2\alpha$	1	$2+2\alpha$	2
2α	2α	$1+2\alpha$	$2+2\alpha$	0	α	1	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	1	$2+2\alpha$	2	2α	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	$1+\alpha$	2	$2+\alpha$	0	α
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2	2α	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	$2+\alpha$	0	α	1	$1+\alpha$

multiplication Table

$\times$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$\alpha+2$	$2\alpha+1$	$1+\alpha$
α	0	α	2α	2	1	$2+\alpha$	$\alpha+1$	$2\alpha+2$	$1+2\alpha$
2α	0	2α	α	1	2	$1+2\alpha$	$2\alpha+2$	$\alpha+1$	$\alpha+2$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	α	2α	1
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2\alpha+2$	$\alpha+1$	1	2α	α	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$\alpha+2$	α	1	2	2α

Hence every non-zero element has a unique multiplicative inverse.

Q9. Prove that every non-zero element in $GF(2^n)$ possesses a unique multiplicative inverse.

Proof by contradiction.

For every non-zero element
Let $a \in GF(2^n)$ s.t it has more than one multiplicative inverse, say b, c

$\therefore \; ab \equiv ac \equiv 1 \bmod p(x)$

where $p(x) = a_{n-1} x^{n-1} + \cdots + a_0$

s.t $a_i \in GF(2)$ (Prime field)

$\therefore a_i \in \{0, 1\}$

$ab \equiv 1 \bmod p(x)$
$ac \equiv 1 \bmod p(x)$ [b, c are assumed multiplicative inverse]

$(ab - ac) = 0 \bmod p(x)$

$a(b-c) \equiv 0 \bmod p(x)$

Since $a \neq 0$ by defn

$\therefore b - c = 0$

$\Rightarrow \; b = c$

Hence there exists a unique multiplicative inverse for all non-zero element in $GF(2^n)$

Q10. construct the field F_{49}.

We will construct field as $\mathbb{Z}_7[x]/P(x)$, s.t $p(x)$ is a monic irreducible polynomial over $\mathbb{Z}_7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

Let $P(x) = x^2 + x + 3$

$P(0) \neq 0$ $\quad$ $P(3) \neq 0$ $\quad$ $P(6)$

$P(1) \neq 0$ $\quad$ $P(4) \neq 0$

$P(2) \neq 0$ $\quad$ $P(5) \neq 0$.

$\therefore \mathbb{Z}_7[x] / x^2+x+3 = g$

s.t $\deg(g) < \deg(P(x))$

$\therefore \deg(g) < 2$

So, $\mathbb{Z}_7[x]/(x^2+x+3) = \{a + b\alpha ;$ s.t α satisfies $P(x)\}$

$\therefore a + b\alpha$

$a, b \in \{0, 1, 2, 3, 4, 5, 6\}$

Hence Total No of elements $= (7)^2 = 49$.

elements $= \{$

$0, \alpha, 2\alpha, 3\alpha, 4\alpha, 5\alpha, 6\alpha,$

$1, 1+\alpha, 1+2\alpha, 1+3\alpha, 1+4\alpha, 1+5\alpha, 1+6\alpha,$

$2, 2+\alpha, 2+2\alpha, 2+3\alpha, 2+4\alpha, 2+5\alpha, 2+6\alpha,$

$3, 3+\alpha, 3+2\alpha, 3+3\alpha, 3+4\alpha, 3+5\alpha, 3+6\alpha,$

$4, 4+\alpha, 4+2\alpha, 4+3\alpha, 4+4\alpha, 4+5\alpha, 4+6\alpha,$

$5, 5+\alpha, 5+2\alpha, 5+3\alpha, 5+4\alpha, 5+5\alpha, 5+6\alpha,$

$6, 6+\alpha, 6+2\alpha, 6+3\alpha, 6+4\alpha, 6+5\alpha, 6+6\alpha$ $\} = F_{49}$

Q11. Find the number of monic irreducible polynomial in $F_3[x]$ of degree 12

irreducible polynomial of degree m over $\mathbb{Z}_p$ is given by

$$N_p(m) = \frac{1}{m} \sum_{d|m} \mu(d)\, p^{m/d}$$

$p = 3, \quad m = 12$

$$\frac{1}{12}\Big[\mu(1)\cdot 3^{12} + \mu(2)\cdot 3^{6} + \mu(3)\cdot 3^{4} + \mu(4)\cdot 3^{3} + \mu(6)\cdot 3^{2} + \mu(12)\cdot 3^{1}\Big]$$

$$= \frac{1}{12}\Big[3^{12} + (-1)\cdot 3^{6} + (-1)3^{4} + 0 + (-1)^{2}\cdot 3^{2} + 0\Big]$$

$$= \frac{530640}{12} = 44220$$

Scanned with CamScanner

Q 12. If a is an algebraic integer and m is an ordinary integer, prove.

a) $a+m$ is an algebraic integer

b) ma is an algebraic integer

a) a is given to be algebraic integer and m is an ordinary integer.

So, $f(a)=0$ in some $f(x)$ over F.

Let $f(x) = \alpha_n x^n + \cdots \alpha_0$

$f(a) = \alpha_n a^n + \alpha_{n-1} a^{n-1} + \cdots \alpha_0$

Now for $x = a+m$

$g(x) = \alpha_n (x-m)^n + \alpha_{n-1} (x-m)^{n-1} + \cdots \alpha_0$

This $g(x)$ will still be $\in$ F as 'm' is an ordinary integer hence co-efficient of $g(x)$ still lie in same field F.

Thus $a+m$ is also algebraic integer. with Polynomial $g(x)$.

Scanned with CamScanner

b) Let $f(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} \dots \alpha_0$

be polynomial for which $f(a) = 0$

$\therefore$ we multiply m^n to polynomial, we get

$m^n f(a) = g(ma)$

$\alpha^n (ma)^n + \alpha_{n-1} m (ma)^{n-1} + \dots \alpha_1 m^{n-1} (ma) + \alpha_0 m^n = 0$

$\therefore$ for this polynomial $g(x)$

'ma' is an algebraic integer.

Scanned with CamScanner

Q 13 a) Let α be a root of $x^2+1=0$, and K be the Field $F_3[\alpha]$. Write down basis for K, considered as a vector space over F_3. Write out the elements of F_1 explicitly.

b) Deduce that if you repeat the construction in a) with different quadratic polynomial irreducible over F_3 (instead of x^2+1), you get the same field K.

a) $f(x) = x^2+1$

$K = F_3[\alpha]$ $\{0,1,2\}$

Basis of K over F_3 = $\{1, \alpha\}$

elements of F_1 = $\{0, 1, -1, \alpha, 1+\alpha, -1+\alpha, -\alpha, 1-\alpha, -1-\alpha\}$

b) If we use any different polynomial (quadratic) other than x^2+1, still all the roots of all polynomial will be in F_1.

So, we will again get same field with 9 elements as in F_1.

Scanned with CamScanner

Q14. Find all the primitive elements of the field $GF(3^2) = GF(3)/(x^2+x+2)$.

$GF(3^2) = GF(3)/(x^2+x+2)$

~~let~~ $a \in GF(3^2)$

$\deg(a) < \deg(x^2+x+2)$

$GF(3^2) = \{a + b\alpha \mid \alpha \text{ satisfies } x^2+x+2\}$

Hence # elements in $GF(3^2) = (3)^2 = 9$

$= \{0, 1, 2, \alpha, 2\alpha, \alpha+1, \alpha+2, 2\alpha+1, 2\alpha+2\}$

To find primitive element we need to find an element $a \in GF(3^2)$

s.t $a^8 \equiv 1 \bmod p(a)$

let $a = 1$ Not primitive] cannot generate α

$a = 2$ Not primitive

$a = \alpha$ $\{\alpha^1 = \alpha,\ \alpha^2 = 2\alpha+1,\ \alpha^3 = 2\alpha+2$

$\alpha^4 = 2,\ \alpha^5 = 2\alpha,\ \alpha^6 = \alpha+2,$

$\alpha^7 = \alpha+1,\ \alpha^8 = 1\}$

Hence 'α' is a primitive root

So, all generators are α^g s.t $\gcd(g, 8) = 1$

$\therefore g = 3, 5, 7$

$\alpha, \alpha^3, \alpha^5, \alpha^7$ are primitive roots :

$\alpha, 2\alpha+2, 2\alpha, \alpha+1$ are the 4 primitive roots of $GF(3^2)$.