

$$\S 7.3 \text{ \#12. i) } GF(p, P(x)) = \mathbb{Z}_3.$$

$\therefore 2$  is the only primitive element

$\therefore$  product of all primitive elements is 2.

$$\text{ii) } GF(p, P(x)) \neq \mathbb{Z}_3.$$

$\therefore$  Let  $\xi$  be a primitive element of  $GF(p, P(x))$ .

Then  $\exists \xi^{-1}$  is also a primitive element &  $\xi \cdot \xi^{-1} = 1$ .

$\therefore$  the product of all the primitive elements is 1.

$\S 8.1 \text{ \#18.}$  by symmetry,  $\underbrace{1}_{\text{iii}}$ .

$$\text{\#21. } \binom{4}{2} = \frac{4 \cdot 3}{2 \cdot 1} = \underbrace{6}_{\text{iii}}$$

$$\S 8.2 \text{ \#2. } (1 \ 5)(2 \ 3 \ 4 \ 7)(8 \ 9)$$

$$\text{\#6. } (1)(2)(3), (1 \ 2)(3), (1 \ 3)(2), (2 \ 3)(1), (1 \ 2 \ 3), (1 \ 3 \ 2).$$

§7.1  
p137.#1.  $\text{GF}(2, x^3+x+1)$ :

$$\alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha(\alpha+1) = \alpha^2 + \alpha$$

$$\alpha^5 = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = (\alpha+1) + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^6 = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = (\alpha+1) + \alpha^2 + \alpha = \alpha^2 + 1$$

$$\alpha^7 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = (\alpha+1) + \alpha = 1.$$

#2.  $\text{GF}(2, x^4+x+1)$ 

$$\alpha, \alpha^2, \alpha^3, \alpha^4 = \alpha+1, \alpha^5 = \alpha(\alpha+1) = \alpha^2 + \alpha.$$

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

$$\alpha^7 = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = (\alpha+1) + \alpha^3 = \alpha^3 + \alpha + 1$$

$$\alpha^8 = \alpha(\alpha^3 + \alpha + 1) = (\alpha+1) + \alpha^2 + \alpha = \alpha^2 + 1$$

$$\alpha^9 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha$$

$$\alpha^{10} = \alpha(\alpha^3 + \alpha) = (\alpha+1) + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^{11} = \alpha(\alpha^2 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{12} = \alpha(\alpha^3 + \alpha^2 + \alpha) = (\alpha+1) + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^{13} = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = (\alpha+1) + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1$$

$$\alpha^{14} = \alpha(\alpha^3 + \alpha^2 + 1) = (\alpha+1) + \alpha^3 + \alpha = \alpha^3 + 1$$

$$\alpha^{15} = \alpha(\alpha^3 + 1) = (\alpha+1) + \alpha = 1$$

§7.1  
p137.

#6. If  $\alpha$  is the associated Galois imaginary, then  $\alpha^3 + 2\alpha + 1 = 0$  over  $\mathbb{Z}_3$ . So  $\alpha^3 = -2\alpha - 1 = \alpha + 2$ .

Consequently,

$$\alpha^4 = \alpha(\alpha + 2) = \alpha^2 + 2\alpha$$

$$\alpha^5 = \alpha(\alpha^2 + 2\alpha) = (\alpha + 2) + 2\alpha^2 = 2\alpha^2 + \alpha + 2$$

$$\alpha^6 = \alpha(2\alpha^2 + \alpha + 2) = 2(\alpha + 2) + \alpha^2 + 2\alpha = \alpha^2 + \alpha + 1$$

$$\alpha^7 = \alpha(\alpha^2 + \alpha + 1) = (\alpha + 2) + \alpha^2 + \alpha = \alpha^2 + 2\alpha + 2.$$

$$\alpha^8 = \alpha(\alpha^2 + 2\alpha + 2) = (\alpha + 2) + 2\alpha^2 + 2\alpha = 2\alpha^2 + 2$$

$$\alpha^9 = \alpha(2\alpha^2 + 2) = 2(\alpha + 2) + 2\alpha = \alpha + 1.$$

$$\alpha^{10} = \alpha(\alpha + 1) = \alpha^2 + \alpha$$

$$\alpha^{11} = \alpha(\alpha^2 + \alpha) = (\alpha + 2) + \alpha^2 = \alpha^2 + \alpha + 2$$

$$\alpha^{12} = \alpha(\alpha^2 + \alpha + 2) = (\alpha + 2) + \alpha^2 + 2\alpha = \alpha^2 + 2$$

$$\alpha^{13} = \alpha(\alpha^2 + 2) = (\alpha + 2) + 2\alpha = 2$$

$$\alpha^{14} = \alpha \cdot 2 = 2\alpha$$

$$\alpha^{15} = \alpha(2\alpha) = 2\alpha^2$$

$$\alpha^{16} = \alpha(2\alpha^2) = 2(\alpha + 2) = 2\alpha + 1$$

$$\alpha^{17} = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha$$

$$\alpha^{18} = \alpha(2\alpha^2 + \alpha) = 2(\alpha + 2) + \alpha^2 = \alpha^2 + 2\alpha + 1$$

$$\alpha^{19} = \alpha(\alpha^2 + 2\alpha + 1) = (\alpha + 2) + 2\alpha^2 + \alpha = 2\alpha^2 + 2\alpha + 2.$$

$$\alpha^{20} = \alpha(2\alpha^2 + 2\alpha + 2) = 2(\alpha + 2) + 2\alpha^2 + 2\alpha = 2\alpha^2 + \alpha + 1.$$

$$\alpha^{21} = \alpha(2\alpha^2 + \alpha + 1) = 2(\alpha + 2) + \alpha^2 + \alpha = \alpha^2 + 1$$

$$\alpha^{22} = \alpha(\alpha^2 + 1) = (\alpha + 2) + \alpha = 2\alpha + 2$$

$$\alpha^{23} = \alpha(2\alpha + 2) = 2\alpha^2 + 2\alpha$$

$$\alpha^{24} = \alpha(2\alpha^2 + 2\alpha) = 2(\alpha + 2) + 2\alpha^2 = 2\alpha^2 + 2\alpha + 1$$

$$\alpha^{25} = \alpha(2\alpha^2 + 2\alpha + 1) = 2(\alpha + 2) + 2\alpha^2 + \alpha = 2\alpha^2 + 1$$

§7.1 #6 continue —

$$d^{26} = d(2d^2+1) = 2(d+2)+d = 1$$

It follows that  $d$  is indeed a primitive element of

$$\text{GF}(3, x^3+2x+1)$$

§7.2 #2.  $\text{GF}(2, x^9+x+1)$

P141.

$d$	$o(d) = \frac{15}{(1, 15)} = 15$
$d^2$	$o(d) = \frac{15}{(2, 15)} = 15$
$d^3$	$o(d^3) = \frac{15}{(3, 15)} = 5$
$d^4 = d+1$	$o(d^4) = \frac{15}{(4, 15)} = 15$
$d^5 = d(d+1) = d^2+d$	$o(d^5) = \frac{15}{(5, 15)} = 3$
$d^6 = d(d^2+d) = d^3+d^2$	$o(d^6) = \frac{15}{(6, 15)} = 5$
$d^7 = d(d^3+d^2) = d+1+d^3$	$o(d^7) = \frac{15}{(7, 15)} = 15$
$d^8 = d(d^3+d+1) = (d+1)+d^2+d = d^2+1$	$o(d^8) = \frac{15}{(8, 15)} = 15$
$d^9 = d(d^2+1) = d^3+d$	$o(d^9) = \frac{15}{(9, 15)} = 5$
$d^{10} = d(d^3+d) = (d+1)+d^2 = d^2+d+1$	$o(d^{10}) = \frac{15}{(10, 15)} = 3$
$d^{11} = d(d^2+d+1) = d^3+d^2+d$	$o(d^{11}) = \frac{15}{(11, 15)} = 15$
$d^{12} = d(d^3+d^2+d) = (d+1)+d^3+d^2 = d^3+d^2+d+1$	$o(d^{12}) = \frac{15}{(12, 15)} = 5$
$d^{13} = d(d^3+d^2+d+1) = (d+1)+d^3+d^2+d = d^3+d^2+1$	$o(d^{13}) = \frac{15}{(13, 15)} = 15$
$d^{14} = d(d^3+d^2+1) = (d+1)+d^3+d = d^3+1$	$o(d^{14}) = \frac{15}{(14, 15)} = 15$
$d^{15} = d(d^3+1) = (d+1)+d = 1$	$o(d^{15}) = \frac{15}{(15, 15)} = 1.$

§7.3 #1.  $d^2 = d+1$ ,  $d^3 = d(d+1) = (d+1)+d = 1$ .

P144  $o(1) = 1$   $o(d) = \frac{3}{(1, 3)} = 3$ ,  $o(d^2) = \frac{3}{(2, 3)} = 3$ .

$\therefore$  primitive elements:  $d, d+1$ .

7.3 p145

11,  $F = GF(p, P(x))$ ,  $\deg P = r$ ,  $r \neq 0 \pmod{p-1}$

$$\text{Show } \sum_{x \in F} x^r = 0,$$

Pf Let  $\xi$  be a primitive element of  $F^*$ .

Then if  $y \in F$ ,  $y \neq 0$ ,  $y = \xi^s$ , some  $s$ .

$\xi$  has order  $p^r - 1$ . Let  $\eta = \xi^r$ .

Then  $\eta$  has order  $(\frac{p^r - 1}{r}, r) = n$ .

$$\text{Thus } \sum_{x \in F} x^r = 0 + \sum_{s=1}^{\frac{p^r - 1}{r}} (\xi^s)^r = 0 + \sum_{s=1}^{\frac{p^r - 1}{r}} \eta^s.$$

But  $\eta$  is a primitive  $n = (\frac{p^r - 1}{r}, r)$  root of unity, so

$$Q(x) = \prod_{s=1}^n (x - \eta^s) = x^n - 1, \text{ so}$$

$$1 + \eta + \eta^2 + \dots + \eta^{n-1} = 0$$

$$\text{But } \sum_{s=1}^{\frac{p^r - 1}{r}} = (1 + \eta + \dots + \eta^{n-1}) + (\eta^n + \dots + \eta^{2n-1})$$

$$= \frac{p^r - 1}{n} (1 + \eta + \dots + \eta^{n-1}) = 0.$$

7.3 p 145

12 For each prime  $p$   $x^p - x - 1$  is irreducible over  $\mathbb{F}_p$ .

Proof Suppose  $\mathbb{F}_p \subset F$  and  $\xi \in F$  is a root. Then from the equation  $\xi^p = \xi + 1$ . But since  $x^p - x - 1 \in \mathbb{F}_p[x]$ , if  $\xi$  is a root, then  $\xi^p$  is also a root  
( $(\xi^p)^p - (\xi^p) - 1 = (\xi^p - \xi - 1)^p = 0$ )

Hence  $\xi^p = \xi + 1$  is a root.

$$\xi^{p^2} = \xi^p + 1 = \xi + 1 + 1 = \xi + 2$$

$$\xi^{p^s} = \xi + s \quad \forall \quad 0 < s < p$$

Hence  $\{\xi, \xi^p, \dots, \xi^{p^{p-1}}\}$  is a

complete set of roots for  $x^p - x - 1 = 0$ . and

$$x^p - x - 1 = \prod_{s=0}^{p-1} (x - (\xi + s)) \text{ in } F[x]$$

If  $P(x) = x^p - x - 1 = Q(x)S(x)$ , where

$Q(x) \in \mathbb{F}_p[x]$  is irreducible and

$r = \deg Q < p = \deg P$ , then

$P$  has root  $\xi$  in  $\mathbb{F}_p[x]/(Q(x))$  and it

satisfies equation  $\xi^p = \xi \neq \xi + 1$ , Contradiction.