7.5.1

Fill in the details in the last example.

Solution:

The splitting field of x^2+x+2 over $\mathbb{F}_3$. Since $f(x)=x^2+x+2$ has no roots, in $\mathbb{F}_3$, it is irreducible by Proposition 5.5.1. We will now check that f is primitive. Let θ be a root of $f(x)$. The powers of θ are:

θ^0	1
θ^1	θ
θ^2	$-\theta+1$
θ^3	$-\theta-1$
θ^4	-1
θ^5	$-\theta$
θ^6	$\theta-1$
θ^7	$\theta+1$
θ^8	1

which is eight elements, so f is primitive.

We can factor x^2+x+2 as $x^2+x+2=(x-\theta)(x-\theta^j)$. To find j, we solve the equations: $\theta\theta^j=2=-1$, $-\theta x-\theta^j x=x$. From the table above and the first equation, we see that the only option is $j=3$, which also solves the second equation.

7.5.2

Find the splitting field of E of the polynomial $f(x)=x^3+x+1$ over $\mathbb{F}_2$. What is the degree $[E:\mathbb{F}_2]$?

Solution:

It is easy to check that f is irreducible since it has no roots in $\mathbb{F}_2$. Therfore, the splitting field is $\mathbb{F}_2[x]/(f(x))$. The resulting field is $\mathbb{F}_{2^3}$, so the degree of $[E:F]$ is 3.

7.5.4

Show that the formal derivative has the following familiar properties of deriviatives, for any $f,g\in F[x]$.

a) $(f+g)'=f'+g'$

b) $(fg)'=f'g+fg'$

c) $(f(x)^n)'=n(f(x)^{n-1})f'(x)$

Solution:

a) It suffices to check this for $f=ax^m$ and $g=bx^n$. In this case:

$$(f+g)'=amx^{m-1}+bnx^{n-1}=f'+g'.$$

b) After applying a) repeatedly, it will suffice to check for $f = ax^m$ and $g = bx^n$. In this case:

$$(fg') = ab(m+n)x^{m+n-1} = abmx^{mn-1} + abnx^{mn-1} = f'g + fg'.$$

c) We use item b) and induction. The base case $f(x)^1$ is clear. Assume $(f(x)^{n-1})' = (n-1)(f(x)^{n-2})f'(x)$. Then

$$(f(x)^n)'(f(x)f(x)^{n-1})' = f'(x)f(x)^{n-1} + f(x)(n-1)(f(x)^{n-2})f'(x) = n(f(x)^{n-1})f'(x)$$

7.5.7

Show that

a) the polynomial $f = x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$

b) the polynomial $f = x^4 + x + 1$ is primitive, that is, a root θ generates the multiplicative group $\mathbb{F}_{16}$

Solution:

1. Since f has an odd number of terms, and non-zero constant term, it has no linear factors. It remains to check that f is not a product of two irreducible degree 2 polynomials. The unique degree 2 irreducible polynomial over $\mathbb{F}_2$ is $x^2 + x + 1$, with square $(x^2 + x + 1)^2 = x^4 + x^2 + 1$. Since this is different from f, f must be irreducible.

2. Let $\theta \in \mathbb{F}_2[x]/(f)$ be the image of x. We compute powers of θ:

θ^0	1
θ^1	θ
θ^2	θ^2
θ^3	θ^3
θ^4	$\theta + 1$
θ^5	$\theta^2 + \theta$
θ^6	$\theta^3 + \theta^2$
θ^7	$\theta^3 + \theta + 1$
θ^8	$\theta^2 + 1$
θ^9	$\theta^3 + \theta$
θ^{10}	$\theta^2 + \theta + 1$
θ^{11}	$\theta^3 + \theta^2 + \theta$
θ^{12}	$\theta^3 + \theta^2 + \theta + 1$
θ^{13}	$\theta^3 + \theta^2 + 1$
θ^{14}	$\theta^3 + 1$
θ^{15}	1

7.5.8

Prove that if $m|n$, then the polynomial $(x^{p^m-1} - 1)$ divides $(x^{p^n-1} - 1)$ in $\mathbb{F}_p[x]$.

Solution:

We follow the hint. We first prove the following formula:

$$\frac{x^{sk}-1}{x^s-1} = (x^s)^{k-1} + (x^s)^{k-2} + \cdots + x^s + 1.$$

The well-known formula for the sum of a geometric progression is:

$$\sum_{i=0}^{k} z^i = \frac{z^{k-1}-1}{z-1} \tag{1}$$

Let $km = n$. Replacing z with p^m in the formula above, we see that $p^n - 1$ divides $p^m - 1$, say $p^n - 1 = lp^m - 1$.

Now, replacing z with x^{p^m-1} and k with l in (1), we get that

$$(x^{p^n-1}-1) = (x^{p^m-1}-1)(\sum_{i=0}^{l}(x^{p^m-1})^i)$$

7.5.10

Find all the generators of the multiplicative group of units of $\mathbb{F}_9 \simeq \mathbb{F}_3[i]$, where $i^2+1=0$.

Solution:

The multiplicative group of units is a cyclic group of order 8, so it has $\phi(8) = 4$ generators. One generator is $(1+i)$. The quickest way to check this is to check that the order of $(1+i)$ is 8 by computing $(1+i)^2 = 2i$, $(2i)^2 = i^2 = -1$, $(-1)^2 = 1$. From our knowledge of the cyclic group of order 8, we know that the other generators are: $(1+i)^3 = 1-i, (1+i)^5 = -1-i, (1+i)^7 = -1+i$

7.5.13

Check that $x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1)$ over $\mathbb{F}_2$ by multiplying the polynomial out on the right.

Solution:

A straightforward compuation gives

$$x(x-1)(x^3+x+1)(x^3+x^2+1) = x^8 + 2x^5 - 2x^4 - x$$

After remembering that we are working in $\mathbb{F}_2$, we see that this is the same as $x^8 - x$.

7.5.14

Show that $\mathbb{F}_{p^n}$ is the splitting field of some irreducible polynomial of degree n over $\mathbb{F}_p$.

Solution:

We know that $f = x^{p^n} - x$ factors over $\mathbb{F}_p$ as the product of all the distinct monic irreducible polynomials of degree dividing n. (p.239) Take any irreducible degree n factor g of f. Then $\mathbb{F}_{p^n} \simeq \mathbb{F}[x]/g$. Since f splits over $\mathbb{F}_{p^n}$, g must also split over $\mathbb{F}_{p^n}$ since it is a factor of f. On the other hand, there must be a some factor g of f that does not split over any field smaller than $\mathbb{F}_{p^n}$, since $\mathbb{F}_{p^n}$ is the splitting field of f. This g must have degree n.

7.5.15

Factor the polynomial $x^9 - x$ completely into irreducible factors over $\mathbb{F}_3$. Which factors are primitive?

Solution:

We use repeatedly that $(a^2 - 1) = (a+1)(a-1)$ over any field, and recall that we factored $(x^4 + 1)$ into irreducible factors last week to get:

$$\begin{aligned} x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1) &= x(x^2 - 1)(x^2 + 1)(x^2 + x - 1)(x^2 - x - 1) \\ &= x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1) \end{aligned}$$

We separate these into primitive and non-primitive:

primitive	non-primitive
$x+1$	x
x^2+x-1	$x-1$
x^2-x-1	x^2+1

$x^2 + 1$ is not primitive, since the roots have order 4, not 8. The two other degree 2 polynomials are primitive. We checked one of them in 7.5.1 and checking the other is analogous.

Appendix

We prove the following statement, used in 7.5.14: The polynomial $f = x^{p^n} - x$ in $\mathbb{F}_p[x]$ is the product of all monic irreducible polyomials of degree dividing n.

Solution

We will make frequent use of the following lemma:

Lemma 0.1. *Let g be a monic irreducible polynomial with a root α. Then g is the unique monic minimal polynomial for α*

Proof. Let h be the monic minimal polynomial of α. By the division algorithm we can write $g = fh + r$ for polynomials f, r, with $\deg(r) < \deg(h)$. We see that $r(\alpha)$ must be 0, so by minimality of h, $r = 0$. Thus h divides g. Since g is monic and irreducible, the only possibility is that $g = h$. □

Let g be a monic irreducible polynomial dividing f, and let $\deg(g) = m$. Let α be a root of g in its splitting field. Since g is irreducible, it must be the minimal polynomial for α, and since g has degree m, the field extension $\mathbb{F}_p(\alpha)$ has degree m, so $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^m}$. But also, $f(\alpha) = \alpha^{p^n} - \alpha = 0$ since g divides f, so α is an element of $\mathbb{F}_{p^n}$, the splitting field of f. Therefore $\mathbb{F}_{p^m} \simeq \mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$, so by proposition 7.5.1 m divides n.

Conversely, assume g is a monic irreducible polynomial of degree m, where m divides n. Let α be a root of g in its splitting field. Since g is irreducible, it must be the minimal polynomial of α. Then $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = m$, so $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. So $\alpha \subset \mathbb{F}_{p^n}$, so by Lagrange's theorem $0 = \alpha^{p^n} - \alpha = f(\alpha)$. Since g is the minimal polynomial for α, g must divide f. (Use the same idea as in the proof of the lemma above)

Finally, since f has no repeated roots in its splitting field (Exercise 7.5.3) no factor can occur more than once.