Abstract Algebra by Pinter, Chapter 27

Amir Taaki

Chapter 27 on Extensions of Fields

Contents

A. Recognizing Algebraic Elements

Q1

a.

$$p(x) = x^2 + 1 \implies p(i) = 0$$

b.

$$p(\sqrt{2}) = 0 \implies p(x) = x^2 - 2$$

c.

$$a = 2 + 3i \qquad (a-2)^2 = -9$$
$$p(x) = a^2 - 4a + 13$$

d.

$$p(\sqrt{1 + \sqrt[3]{2}}) = 0 \implies p(x) = (x^2 - 1)^3 - 2$$

e.

$$p(x) = (x^4 - 1)^2 - 8$$

f.

$$p(x) = (x^2 - 5)^2 - 24$$

g.

Let $x = \sqrt[3]{2}$, then $y = \sqrt[3]{2} + \sqrt[3]{4} = x + x^2$.

$$y^3 = x^6 + 3x^5 + 3x^4 + x^3 = 4 + 6x^2 + 6x + 2 = 6 + 6y$$

$$\implies p(y) = y^3 - 6y - 6$$

Q2

a.

$$p(x) = x^2 - \pi$$

b.

$$p(x) = x^4 - \pi^2$$

c.

$$p(x) = \pi^3 x - \pi^6 + \pi^3$$

B. Finding the Minimum Polynomial

Q1

a.

$$a = 1 + 2i$$
$$(a-1)^2 = -4$$
$$p(x) = x^2 - 2x + 5$$

Reducing the equation from $\mathbb{Q}$ to $\mathbb{Z}_3$ then $\bar{p}(x) = x^2 + x + 2$ which has no roots in the field and so is irreducible.

b.

```
sage: p = lambda x: (x - 1)**2 - 2
sage: p(x + 1)
x^2 - 2
sage: p(x + 2)
x^2 + 2*x - 1
sage: p(x + 3)
x^2 + 4*x + 2
```

By Eisenstein's criterion with $p = 2$, then this polynomial is irreducible.

c.

```
sage: p = lambda x: (x - 1)**4 - ((2*I)**(1/2))**4
sage: p(x)
x^4 - 4*x^3 + 6*x^2 - 4*x + 5
```

Let $h : \mathbb{Q} \to \mathbb{Z}_3$ then $h(p(x)) = x^4 + 2x^3 + 2x + 2$ which by Eisenstein's criterion means the polynomial is irreducible.

d.

```
sage: p = lambda x: (x^2 - 2)**3 - 3
sage: p(x)
x^6 - 6*x^4 + 12*x^2 - 11
```

TODO: finish this

e.

```
sage: p = lambda x: (x**2 - 3 - 5)**2 - 4*3*5
sage: p(x)
x^4 - 16*x^2 + 4
```

$$a + c = 0$$
$$ac + b + d = -16$$
$$bc + ad = 0$$
$$bd = 4$$

$$\implies b = \pm 1, \pm 2, \pm 4$$
$$a + c = 0 \implies a = -c$$
$$bc + ad = bc - dc = 0 \implies b = d \implies b = \pm 2$$
$$ac + b + d = -c^2 \pm 4 = -16$$
$$\implies c^2 = 16 \pm 4$$
$$\implies c^2 = 12, 20$$

which has no roots in $\mathbb{Z}$.

f.

```
sage: p = lambda x: (x^2 - 1)^2 - 2
sage: p(x)
x^4 - 2*x^2 - 1
sage: p(x + 1)
x^4 + 4*x^3 + 4*x^2 - 2
```

By Eisenstein's criterion with $p = 2$, this polynomial is irreducible.

Q2

a.

$$a = \sqrt{2} + i$$
$$(a - \sqrt{2})^2 = -1$$
$$x - 2\sqrt{2}x + 3$$

b.

$$a = \sqrt{2} + i$$
$$a^2 = 1 + 2\sqrt{2}i$$
$$(a^2 - 1)^2 = a^4 - 2a^2 + 1 = -8$$
$$x^4 - 2x^2 + 9$$

c.

$$a = \sqrt{2} + i$$
$$(a - i)^2 = a^2 - 2ai - 1 = 2$$
$$x^2 - 2ix - 3$$

Q3

$\sqrt{3} + i$

$\mathbb{R}$

```
sage: ((x - 3**(1/2))**2 + 1).expand()
x^2 - 2*sqrt(3)*x + 4
```

$\mathbb{Q}$

```
sage: (x^2 - 2)**2 + 2*3
x^4 - 4*x^2 + 10
```

$\mathbb{Q}(i)$

```
sage: ((x - I)**2 - 3).expand()
x^2 - 2*I*x - 4
```

$\mathbb{Q}(\sqrt{3})$

```
sage: ((x - 3**(1/2))**2 + 1).expand()
x^2 - 2*sqrt(3)*x + 4
```

$\sqrt{i + \sqrt{2}}$

$\mathbb{R}$

```
sage: ((x^2 - 2**(1/2))**2 + 1).expand()
x^4 - 2*sqrt(2)*x^2 + 3
```

$\mathbb{Q}(i)$

```
sage: ((x^2 - I)^2 - 2).expand()
x^4 - 2*I*x^2 - 3
```

$\mathbb{Q}(\sqrt{2})$

```
sage: ((x^2 - 2**(1/2))**2 + 1).expand()
x^4 - 2*sqrt(2)*x^2 + 3
```

$\mathbb{Q}$

```
sage: ((x^4 - 1)^2 + 8).expand()
x^8 - 2*x^4 + 9
```

Q4

a.

$$(x+1)^2 - 8 = 0$$
$$x = \pm sqrt 8 - 1$$

b.

$$(x^2+1)^2 - 2 = 0$$
$$x^2 = \pm sqrt 2 - 1$$
$$x = \pm\sqrt{\pm\sqrt{2} - 1}$$

c.

$$(x^2-5)^2 - 24 = 0$$
$$x^2 = \pm 2\sqrt{6} + 5$$
$$x = \pm\sqrt{\pm 2\sqrt{6} + 5}$$

Q5

a.

$$\sigma_{\sqrt{2}}(a(x)) = a(\sqrt{2})$$
$$J = \langle p(x) \rangle \implies p(\sqrt{2}) = 0$$
$$p(x) = x^2 - 2$$

b.

Same as 27B1b:

$$x^2 + 4x + 2$$

c.

Same as 27B1f:

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

C. The Structure of Fields $F[x]/\langle p(x) \rangle$

Q1

$$t(x) \in F[x], t(x) = p(x)q(x) + r(x) : \deg r(x) < \deg p(x)$$
$$p(c) = 0 \implies t(c) = 0 + r(c) = r(c)$$

Q2

$s(c) = t(c) \implies J + s(x) = J + t(x)$, $J = \langle p(x) \rangle$, but $\deg s(x) < \deg p(x)$ and $\forall a(x) \in J + s(x), a(x) = p(x)q(x) + s(x)$. Since $\deg t(x) < \deg p(x)$, then

$$t(x) = 0 + s(x) = s(x)$$

Q3

Every element in $F(c)$ can be written as $r(c)$ where $\deg r(x) < \deg p(x)$, which is unique since for any $s(c) = t(c)$ where the degree $< n$, then $s(x) = t(x)$.

$$\forall t(x) \in F[x], t(x) = p(x)q(x) + r(x) \implies t(x) \equiv r(x) \pmod{p(x)}$$

Q4

Every element in $F(c)$ can be written as $r(c)$ where $\deg r(x) < \deg p(x) = x^2 + x + 1/$

$$0, 1, c, c+1$$

$$\begin{gathered} c^2 + c + 1 = 0 \\ \implies c^2 = c + 1 \\ (c+1)^2 = c^2 + 1 = c \\ c(c+1) = c^2 + c = 1 \end{gathered}$$

$$\begin{gathered} J = \{0, x^2 + x + 1\} \\ J + 1 = \{1, x^2 + x\} \\ J + x = \{x, x^2 + 1\} \\ J + x + 1 = \{x + 1, x^2\} \end{gathered}$$

Q5

$$\begin{aligned} J &= \{0, x^3 + x + 1\} \\ J + 1 &= \{1, x^3 + x\} \\ J + x &= \{x, x^3 + 1\} \\ J + x + 1 &= \{x + 1, x^3\} \end{aligned}$$

```
sage: x = PolynomialRing(IntegerModRing(2, is_field=True), 'x').gen()
sage: (x^3 + x^2)%(x^3 + x + 1)
x^2 + x + 1
sage: (x^3 + x^2 + 1)%(x^3 + x + 1)
x^2 + x
sage: (x^3 + x^2 + x)%(x^3 + x + 1)
x^2 + 1
sage: (x^3 + x^2 + x + 1)%(x^3 + x + 1)
x^2
```

$$\begin{aligned} J + x^2 &= \{x^2, x^3 + x^2 + x + 1\} \\ J + x^2 + x &= \{x^2 + x, x^3 + x^2 + 1\} \\ J + x^2 + 1 &= \{x^2 + 1, x^3 + x^2 + x\} \\ J + x^2 + x + 1 &= \{x^2 + x + 1, x^3 + x^2\} \end{aligned}$$

Q6

```
sage: x = PolynomialRing(IntegerModRing(3, is_field=True), 'x').gen()
sage: rem = lambda px: px % (x^3 + x^2 + 2)
sage: rem(x), rem(2*x)
(x, 2*x)
sage: rem(x^2)
x^2
```

```
sage: rem(x^2 + x), rem(x^2 + 2*x)
(x^2 + x, x^2 + 2*x)
sage: rem(x^2 + 1), rem(x^2 + 2)
(x^2 + 1, x^2 + 2)
sage: rem(x^2 + x + 1)
x^2 + x + 1
sage: rem(x^3)
2*x^2 + 1
sage: rem(x^3), rem(x^3 + 1), rem(x^3 + 2)
(2*x^2 + 1, 2*x^2 + 2, 2*x^2)
sage: rem(x^3 + x), rem(x^3 + 2*x)
(2*x^2 + x + 1, 2*x^2 + 2*x + 1)
sage: rem(x^3 + x + 1), rem(x^3 + x + 2)
(2*x^2 + x + 2, 2*x^2 + x)
sage: rem(x^3 + 2*x + 1), rem(x^3 + 2*x + 2)
(2*x^2 + 2*x + 2, 2*x^2 + 2*x)
sage: rem(x^3 + x^2), rem(x^3 + 2*x^2)
(1, x^2 + 1)
sage: rem(x^3 + x^2 + 1), rem(x^3 + x^2 + 2)
(2, 0)
sage: rem(x^3 + 2*x^2 + 1), rem(x^3 + 2*x^2 + 2)
(x^2 + 2, x^2)
sage: rem(x^3 + x^2 + x), rem(x^3 + x^2 + 2*x)
(x + 1, 2*x + 1)
sage: rem(x^3 + 2*x^2 + x), rem(x^3 + 2*x^2 + 2*x)
(x^2 + x + 1, x^2 + 2*x + 1)
sage: rem(x^3 + x^2 + x + 1), rem(x^3 + x^2 + 2*x + 2)
(x + 2, 2*x)
sage: rem(x^3 + 2*x^2 + x + 1), rem(x^3 + 2*x^2 + 2*x + 2)
(x^2 + x + 2, x^2 + 2*x)
```

$$
\begin{aligned}
J &= \{0, x^3 + x^2 + 2, 2x^3 + 2x^2 + 1\} \\
J + 1 &= \{1, x^3 + x^2, 2x^3 + 2x^2 + 2\} \\
J + 2 &= \{2, x^3 + x^2 + 1, 2x^3 + 2x^2\} \\
J + x &= \{x, x^3 + x^2 + x + 2, 2x^3 + 2x^2 + x + 1\} \\
J + x + 1 &= \{x + 1, x^3 + x^2 + x, 2x^3 + 2x^2 + x + 2\} \\
J + x + 2 &= \{x + 2, x^3 + x^2 + x + 1, 2x^3 + 2x^2 + x\} \\
J + 2x &= \{2x, x^3 + x^2 + 2x + 2, 2x^3 + 2x^2 + 2x + 1\} \\
J + 2x + 1 &= \{2x + 1, x^3 + x^2 + 2x, 2x^3 + 2x^2 + 2x + 2\} \\
J + 2x + 2 &= \{2x + 2, x^3 + x^2 + 2x + 1, 2x^3 + 2x^2 + 2x\} \\
&\dots
\end{aligned}
$$

D. Short Questions Relating of Field Extensions

Q1

c is algebraic over F, means there is a polynomial $p(x) \in F[x] : p(c) = 0$. Let $a(x) = p(x-1)$, then $a(c+1) = p(x) = 0$, and so $c+1$ is algebraic over F.

Likewise since F is a field then every nonzero $k \in F$ has an inverse k^{-1}. Let $a(x) = p(k^{-1}x)$, then $a(kc) = p(k^{-1}kx) = 0$ and so kc where $k \in F$ is algebraic over F.

Q2

See 25G5.

Q3

$g(x) = p(xd) \implies g(c) = 0$, so c is algebraic over $F(d)$. Likewise with $g(x) = p(x + d)$.

Q4

$\deg p(x) = 1 \implies p(x) = x - b$ where $b \in F$, but $p(a) = a - b = 0 \implies a = b \implies a \in F$.

Q5

$p(a) = 0 \implies p(x) \in J$, but J is generated by a monic polynomial $\bar{p}(x)$, so $p(x) = \bar{p}(x)q(x)$, but $p(x)$ is irreducible so $p(x) = \bar{p}(x)$.

Q6

```
sage: (x^5 + 2*x^3 + 4*x^2 + 6).find_root(-100,100)
-1.5236546776809101
```

$\mathbb{Z}(-1.5236546776809101)$

Q7

$$
\begin{aligned}
a &= 1 \pm i \\
(a-1)^2 &= (\pm i)^2 \\
a^2 - 2a + 1 &= -1 \\
a^2 - 2a + 2 &= 0 \\
\implies \mathbb{Q}(1+i) &\cong \mathbb{Q}(1-i)
\end{aligned}
$$

For the second part, there is no values $a, b \in \mathbb{Q}$ such that $(\sqrt{2})^2 = (a\sqrt{3} + b)^2$.

All the elements of $\mathbb{Q}(\sqrt{3})$ are of the form $a\sqrt{3} + b$ because $(\sqrt{3})^2 \in \mathbb{Q}$, so any higher power of $\sqrt{3}$ is either in $\mathbb{Q}$ or a multiple of $\sqrt{3}$.

Q8

$$\frac{F[x]}{\langle p(x) \rangle} \cong F(\alpha)$$

$$(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$$

Then $p(x) = x^2 - bx + c$, with $b \in F$ where $b = \alpha + \beta$. Since $b \in F, \alpha \in F(\alpha)$, then also $\beta \in F(\alpha)$.

E. Simple Extensions

Q1

$$c \implies F \implies -c \in F \implies (a + c) - c \in F(a + c) \implies a \in F(a + c) \implies F(a + c) = F(a)$$

Likewise F is a field, and $c \in F \implies c^{-1} \in F$.

Q2

From 27D4, the minimum polynomial is degree 2 or higher. Let the minimum polynomial be

$$p(x) = \cdots + a_2x^2 + a_1x + a_0$$

and

$$a_2a^2 + a_1a + a_0 = 0$$

so $a^2 \in F(a)$. The reverse is not true as $F(i) \neq F(i^2) = F(-1)$.

$F(a, b)$ forms an extension field containing both a and b, so includes $a + b$. The converse isn't true since if a is not in F, and a^2 is the root of a polynomial in $F(a^2)$ then a is not necessarily in $F(a^2)$. Likewise for $F(a + b)$.

Q3

$p(a+c)=0$ so $a+c$ is a root of $p(x)$, and a is a root of $g(x)=p(x+c)$. Likewise let $g(x)=p(cx)$, then $g(a)=0$ and $p(ca)=0$.

Q4

From 27E1, $F(a)=F(a+c)$ so

$$F[x]/\langle p(x+c)\rangle \cong F[x]/\langle p(x)\rangle$$

Q5

$$F(a)=F(ca)$$

$$F[x]/\langle p(cx)\rangle \cong F[x]/\langle p(x)\rangle$$

Q6

a.

Let $p(x)=x^2+1$, then $p(x+6)=x^2+12x+36+1=x^2+x+4$ in $\mathbb{Z}_{11} \implies \mathbb{Z}_{11}(\alpha)=\mathbb{Z}_{11}(\alpha+6)$ where α is the root of $p(x)$.

b.

$$p(x)=x^2-2, p(x-2)=x^2-4x+2$$

c.

$$p(x)=x^2-2, p(2x)=4(x^2-1/2)$$

F. Quadratic Extensions

Q1

$$x^2+bx+c=0$$

$$(x+\frac{b}{2})^2-(\frac{b}{2})^2+c=0$$

$$x=\pm\sqrt{(\frac{b}{2})^2-c}-\frac{b}{2}$$

Both $b,c\in F$, so $\frac{b}{2}\in F$ and $(\frac{b}{2})^2-c\in F$, thus $a=(\frac{b}{2})^2-c\in F$, and $\pm\sqrt{a}-\frac{b}{2}$ is a root of x^2+bx+c.

Since $F(\sqrt{a}-\frac{b}{2})=F(\sqrt{a})$, any quadratic extension of F is of the form $F(\sqrt{a})$.

Q2

$p(x)$ and $q(x)$ are irreducible, so there is no $\sqrt{a}$ or $\sqrt{b}$ in F. If there was, then $p(x)$ could be factored as $(x-\sqrt{a})(x+\sqrt{a})$ and likewise for $q(x)$.

Thus a and b are non-squares, so by the theorem a/b is square.

Lastly $c=\sqrt{a}/\sqrt{b}$, so $\sqrt{a}=c\sqrt{b}$, and $p(\sqrt{a})=p(c\sqrt{b})=0 \implies \sqrt{b}$ is a root of $p(cx)$.

Q3

$g(x)=p(cx), g(\sqrt{b})=0 \implies F(\sqrt{b})\cong F[x]/\langle g(x)\rangle \implies F(\sqrt{b})\cong F[x]/\langle p(cx)\rangle$, but $F[x]/\langle p(cx)\rangle \cong F[x]/\langle p(x)\rangle$ and $F(\sqrt{a})\cong F[x]/\langle p(x)\rangle \implies F(\sqrt{a})=F(\sqrt{b})$.

Q4

$F(\sqrt{a})\cong F(\sqrt{b}) \implies$ there exists an isomorphism $h: F(\sqrt{a})\to F(\sqrt{b})$. This comes automatically from the fundamental isomorphism theorem.

Q5

For any number in the field of reals $\mathbb{R}$ that is not a square (does not have a square root in $\mathbb{R}$), then a/b is a square by the theorem since $\mathbb{R}$ is a field. Therefore for any number $a \in \mathbb{R}$, such that $\sqrt{a} \notin \mathbb{R} \implies \sqrt{a} \in \mathbb{C}$, then

$$F(\sqrt{a}) \cong F(\sqrt{b}) \cong F(\sqrt{c}) \cong \cdots$$
$$\implies F(\sqrt{a}) \cong \mathbb{C}$$

G. Questions Relating to Transcendental Elements

Q1

c is transcendental so the ideal is $J = \{0\} \implies F(c) = \{a(c) : a(x) \in F[x]\} \cong F[x]$.

Q2

Q is a field of quotients of $F(c) = \{a(c) : a(x) \in F[x]\}$ but $F(c)$ contains every possible polynomial so $Q \subseteq F(c)$, but since $F(c)$ by definition is the minimum field containing both F and c, then $F(c) \subseteq Q$, so $F(c) = Q$.

Since c is transcendental and $F(c)$ contains all quotients of $a(c)$, thus $F(c) \cong F(x)$.

Q3

c is transcendental, so there is no $p(x) \neq 0 : p(c) = 0$, so there is no $q(x)$ such that $q(c+1) = 0$ or $q(kc) = 0$, because then $p(x) = q(x-1)$ or $p(x) = q(k^{-1}x)$ would make c a root and algebraic.

If c^2 is algebraic over $F[x]$, then there is a $p(x) = a_n x^n + \cdots + a_0$ such that $p(c^2) = 0$. Let $g(x) = p(x^2)$, then $g(c) = p(c^2)$ and hence c is algebraic - a contradiction.

Q4

Every element of $F(c)$ can be written as $a_0 + a_1 c + \cdots + a_n c^n$.

Generalizing the argument previously, for any $n \in \mathbb{Z}$, c is transcendental over $F \iff c^n$ is transcendental. Likewise for $kc : k \in F$ and $c + k$.

So every polynomial of degree 1 or more containing c is transcendental over F.

H. Common Factors of Two Polynomials: Over F and over Extensions of F

Q1

$a(c) = 0 = b(c) \implies a(x), b(x) \in J$ but $J = \langle p(x) \rangle$ where $p(x)$ is a monic irreducible polynomial in $F[x]$. So $a(x)$ and $b(x)$ are both multiples of $p(x)$ and share $p(x)$ as a common factor.

Q2

$a(x), b(x) \in F[x]$ and

$$s(x)a(x) + t(x)b(x) = 1$$

remains true in $K[x]$. Likewise the converse holds.

I. Derivatives and Their Properties

Q1

$$\begin{aligned}
[a(x) + b(x)]' &= [a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n + b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots + b_n x^n]' \\
&= a_1 + b_1 + 2a_2 x + 2b_2 x + 3a_3 x^2 + 3b_3 x^2 + \cdots + n a_n x^{n-1} + n b_n x^{n-1}
\end{aligned}$$

$$[a(x) + b(x)]' = a'(x) + b'(x)$$

Q2

$$a(x)b(x) = a_0b_0 + (a_0b_1 + b_0a_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n}$$

$$\begin{aligned}[a(x)b(x)]' &= (a_0b_1 + b_0a_1) + 2(a_0b_2 + a_1b_1 + a_2b_0)x + \cdots + 2na_nb_nx^{2n-1} \\ &= c_0 + c_1x + \cdots + c_{2n-1}x^{2n-1}\end{aligned}$$

$$\text{where } c_k = \sum_{i+j=k+1} [(k+1)(a_i + b_j)] = (k+1) \sum_{i+j=k+1} (a_i + b_j)$$

Now by definition we have $a'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ and likewise for $b(x)$ giving us

$$\begin{aligned}a'(x)b(x) &= a_1b_0 + (a_1b_1 + 2a_2b_0)x + \cdots + na_nb_nx^{2n-1} \\ &= d_0 + d_1x + \cdots + d_{2n-1}x^{2n-1}\end{aligned}$$

$$d_k = \sum_{(i-1)+j=k} ia_ib_j$$

$$\begin{aligned}a(x)b'(x) &= a_0b_1 + (a_1b_1 + 2a_0b_2)x + \cdots + na_nb_nx^{2n-1} \\ &= e_0 + e_1x + \cdots + e_{2n-1}x^{2n-1}\end{aligned}$$

$$e_k = \sum_{i+(j-1)=k} ja_ib_j$$

$$a'(x)b(x) + a(x)b'(x) = (a_0b_1 + b_0a_1) + 2(a_0b_2 + a_1b_1 + a_2b_0)x + \cdots + 2na_nb_nx^{2n-1} = \sum_{k=0}^{2n-1} (d_k + e_k)x^k$$

$$\begin{aligned}d_k + e_k &= \sum_{(i-1)+j=k} ia_ib_j + \sum_{i+(j-1)=k} ja_ib_j \\ &= \sum_{i+j=k+1} (i+j)(a_i + b_j) \\ &= (k+1) \sum_{i+j=k+1} (a_i + b_j) \\ &= c_k\end{aligned}$$

Q3

$$\begin{aligned}a(x) &= a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \\ ka(x) &= ka_0 + ka_1x + ka_2x^2 + \cdots + ka_nx^n \\ [ka(x)]' &= ka_1 + k2a_2x + \cdots + kna_nx^{n-1}\end{aligned}$$

$$\begin{aligned}a'(x) &= a_1 + 2a_2x + \cdots + na_nx^{n-1} \\ ka'(x) &= ka_1 + k2a_2x + \cdots + kna_nx^{n-1}\end{aligned}$$

Q4

There does not exist an $n \in \mathbb{Z}$ such that $n \cdot 1 = 0$, so ka_kx^{k-1} for values of $k \geq 0$ can only be zero when $k = 0$.

Otherwise if the characteristic is nonzero then two positive values in the ring can be 0 and the above does not hold.

Q5

$$\begin{aligned}[x^6 + 2x^3 + x + 1]' &= x^6 + x^2 + 1 \\ [x^5 + 3x^2 + 1]' &= x \\ [x^15 + 3x^10 + 4x^5 + 1]' &= 0\end{aligned}$$

Q6

$\text{char}\, F = 0 \implies p \cdot 1 = 0 \implies \forall a \in F, p \cdot a = 0$. The derivative of $a'(x)$ consists of terms of the form $ka_k x^{k-1}$. So $a'(x) = 0 \implies a(x)$ consists of terms of the form $a_{mp} x^{mp}$.

J. Multiple Roots

Q1

$a(x) = (x-c)^m$ for some $m > 1 \implies a(x) = (x-c)^2[(x-c)^{m-2}q(x)] = (x-c)^2 q'(x)$. Since $c \in K$, thus $a(x) \in K[x]$.

Q2

$$\begin{aligned} a(x) &= (x^2 - 2cx + c^2)q(x) \\ &= x^2 q(x) - 2cxq(x) + c^2 q(x) \\ a'(x) &= 2xq(x) + x^2 q'(x) - 2cq(x) - 2cxq'(x) + c^2 q'(x) \end{aligned}$$

Q3

$$\begin{aligned} a'(x) &= 2q(x)(x-c) + q'(x)(x-c)^2 \\ &= (x-c)[2q(x) + q'(x)(x-c)] \end{aligned}$$

Thus $a(x)$ and $a'(x)$ share a common factor in $F[x]$.

Q4

$$\begin{aligned} \{(x-c_1)[(x-c_2)\cdots(x-c_n)]\}' &= (x-c_1)'[(x-c_2)\cdots(x-c_n)] + (x-c_1)[(x-c_2)\cdots(x-c_n)]' \\ &= (x-c_2)\cdots(x-c_n) + (x-c_1)[(x-c_2)'(x-c_3)\cdots(x-c_n) + (x-c_2)[(x-c_3)\cdots(x-c_n)]'] \\ &= (x-c_2)\cdots(x-c_n) + (x-c_1)(x-c_3)\cdots(x-c_n) + (x-c_1)(x-c_2)[(x-c_3)'(x-c_4)\cdots(x - \\ &= (x-c_2)\ cdots(x-c_n) + (x-c_1)(x-c_3)\cdots(x-c_n) + (x-c_1)(x-c_2)(x-c_4)\cdots(x-c_n) - \end{aligned}$$

Q5

$a(x)$ does not have multiple roots and no term in $a'(x)$ repeats.

Q6

No common roots, hence no common factors.

Q7

Using polynomial long division, we see the derivatives do not factor the equations:

$$(2x-8) \nmid (x^2 - 8x + 8)$$

$$(x+3) \nmid (x^2 + x + 1)$$

$$2x^{99} \nmid x^{100} - 1$$