Math 4108 HW5

Pengfei Zhu

February 8, 2024

Exercise 3.17 Let K be a field of characteristic 0, and suppose that $X^4 - 16X^2 + 4$ is irreducible over K. Let α be the element $X + \langle X^4 - 16X^2 + 4\rangle$ in the field $L = K[X]/\langle X^4 - 16X^2 + 4\rangle$. Determine the minimum polynomials of α^2, $\alpha^3 - 14\alpha$, and $\alpha^3 - 18\alpha$.

a) α^2

Since $\beta = \alpha^2$ does not belong to K, its minimum polynomial has degree at least 2. Then, since $\beta^2 - 16\beta + 4 = 0$ in K, the minimum polynomial of α^2 is $X^2 - 16X + 4$.

b) $\alpha^3 - 14\alpha$

$(\alpha^3 - 14\alpha)^2 = \alpha^6 - 28\alpha^4 + 196\alpha^2 = \alpha^2(\alpha^4 - 16\alpha^2 + 4) - 12(\alpha^4 - 16\alpha^2 + 4) + 48 = 48$, the minimum polynomial of $\alpha^3 - 14\alpha$ is $X^2 - 48$.

c) $\alpha^3 - 18\alpha$

$(\alpha^3 - 18\alpha)^2 = \alpha^6 - 36\alpha^4 + 324\alpha^2 = \alpha^2(\alpha^4 - 16\alpha^2 + 4) - 20(\alpha^4 - 16\alpha^2 + 4) + 80 = 80$, the minimum polynomial of $\alpha^3 - 18\alpha$ is $X^2 - 80$.

Exercise 6.1 Let f, g be polynomials over a field K, with $\partial(f) = m$, $\partial(g) = n$.
(i) Show that $D(f + g) = Df + Dg$.

Proof. We have $f = a_1 + 2a_2X + \cdots + ma_nX^{m-1}$ and $g = b_1 + 2b_2X + \cdots + nb_nX^{n-1}$ for some coefficients $a_m, b_n \in K$. Then, the sum $f + g$ is a polynomial of degree at most $\max(m, n)$.

The derivative of $f + g$ is

$$\begin{aligned} D(f+g) &= D(a_0 + a_1X + \cdots + a_mX^m + a_0 + b_1X + \cdots + b_nX^n) \\ &= a_1 + 2a_2X + \cdots + ma_mX^{m-1} + b_1 + 2b_2X + + \cdots + nb_nX^{n-1} \\ &= D(a_0 + a_1X + \cdots + a_mX^m) + D(b_1X + \cdots + b_nX^n) \\ &= Df + Dg. \end{aligned}$$

□

(ii) Show, by induction on $m + n$, that $D(fg) = (Df)g + f(Dg)$.

Proof. Prove by induction:
Base case (n = 0):
Both f and g are constants, and $D(fg) = 0 = (Df)g + f(Dg)$.
Inductive Hypothesis:
Assume the result holds for all pairs (f', g'), $\partial(f') + \partial(g') < m + n$.
Inductive Step: Suppose $m + n = k$;

$$\begin{aligned} D(fg) &= D(a_m b_0 X^m + a_m b_1 X^{m+1} + \cdots + a_m b_n X^{m+n}) \\ &= a_m(m b_0 X^{m-1} + (m+1) b_1 X^m + (m+2) b_2 X^{m+1} + \cdots + (m+n) b_n X^{m+n-1}) \\ &= m a_m X^{m-1}(b_0 + b_1 X + \cdots + b_n X^n) + a_m X^m (b_1 + 2 b_2 X + \cdots + n b_n X^{n-1}) \\ &= (Df)g + f(Dg). \end{aligned}$$

Here, we used the product rule for differentiation and applied the induction hypothesis to the terms involving derivatives.
$\therefore$ By the principle of induction, the claim holds for all polynomials that $\partial f + \partial g < k$ □

3. Let n be an integer which is not a perfect square. Prove that for any $a, b \in \mathbb{Q}$, if $a + b\sqrt{n}$ is a root of a polynomial $f(x) \in \mathbb{Q}[x]$, then $a - b\sqrt{n}$ is also a root of $f(x)$.

Proof. If $a + b\sqrt{n} \notin \mathbb{Q}$, then $\mathbb{Q}(a + b\sqrt{n})$ is an extension of $\mathbb{Q}$, and we have $[\mathbb{Q}(a+b\sqrt{n}) : \mathbb{Q}] \geq 2$. Now consider the polynomial $P = X^2 - 2aX + a^2 - b^2 n \in \mathbb{Q}[X]$. We have

$$P(a + b\sqrt{n}) = (a^2 + b^2 n + 2abn\sqrt{n}) - 2a^2 - 2abn\sqrt{n} + a^2 - b^2 n = 0$$

thus $a + bn\sqrt{n}$ is a root of P. Now, since we have $[\mathbb{Q}(a + b\sqrt{n}) : \mathbb{Q}] \geq 2$ and $\deg(P) = 2$, we get that P is the minimal polynomial of $a + bn\sqrt{n}$. Now, we also have

$$P(a - b\sqrt{n}) = (a^2 + b^2 n - 2abn\sqrt{n}) - 2a^2 + 2abn\sqrt{n} + a^2 - b^2 n = 0$$

so $a - b\sqrt{n}$ is also a root of P. □

4.

(a) Show that $f = X^3 + X + 1$ is irreducible over $\mathbb{Z}_2$.

Since the degree of this polynomial is 3, so it has no roots in $\mathbb{Z}_2$. f does not have any roots in $\mathbb{Z}_2$ with values of f at $X = 0$ and $X = 1$:

$$f(0) = 0^3 + 0 + 1 = 1 \neq 0$$

$$f(1) = 1^3 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0$$

so, f cannot be factored into linear factors over $\mathbb{Z}_2$. Therefore, f is irreducible over $\mathbb{Z}_2$.

(b) Write down the multiplication table for the splitting field K of f over $\mathbb{Z}_2$. What is the degree of K over $\mathbb{Z}_2$?

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

The degree of $\mathbb{K}$ over $\mathbb{Z}_2$ is 3 because f is of degree 3.

(c) Determine the linear factors of f in $K[X]$.

Since $f(x)$ is irreducible over $\mathbb{Z}_2$, all zeros of $f(x)$ must lie in an extension field of $\mathbb{Z}_2$. Let α be a zero of $f(x)$. $\mathbb{Z}_2(\alpha)$ can be described as $\alpha^4 = \alpha^2+\alpha$, $\alpha^5 = \alpha^2+\alpha+1$, $\alpha^6 = \alpha^2+1$, and $\alpha^7 = 1$. Higher powers of α repeat preceding powers. Therefore, $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2, \alpha+1, \alpha^2+1, \alpha^2+\alpha+1, \alpha^2+\alpha\} = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Z}_2\}$.

The three zeros of $f(x)$ are α, α^2, and $\alpha^2+\alpha$.

$$f(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^2+\alpha)$$

(d) Show that K^* is a cyclic group of order 7.

Let's check the orders of each non-zero element in K. Since K is small, we can simply compute the powers of each element until we find one with order 7.

The elements in K are $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. We'll check the orders of each:

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

(b) $\alpha^3 = \alpha^2 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2+\alpha$

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

(d) $\alpha^5 = \alpha^4 \cdot \alpha = (\alpha^2+\alpha+1)\cdot\alpha = \alpha^3+\alpha^2+\alpha = \alpha^2+1$

(e) $\alpha^6 = \alpha^5 \cdot \alpha = (\alpha^2+1)\cdot\alpha = \alpha^3+\alpha = \alpha+1$

(f) $\alpha^7 = \alpha^6 \cdot \alpha = (\alpha+1)\cdot\alpha = \alpha^2+\alpha$

So, we see that α has order 7, which means K^* is generated by α. Hence, K^* is cyclic of order 7.

5. Find the degrees of the splitting fields of the following polynomials over $\mathbb{Q}$.

(a) $x^3 - x^2 - x - 2$

By observation, $x = 2$ is a root of this polynomial. Then, we can factor it as $x^3 - x^2 - x - 2 = (x - 2)(x^2 + 1)$. The quadratic factor $x^2 + 1$ has no real roots, so it's irreducible over the rationals. The roots of $x^2 + 1$ are complex, namely i and $-i$. Thus, the splitting field of this polynomial over $\mathbb{Q}$ is $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$.

(b) $x^4 - 5$

Since $x^4 - 5 = (x^2 - \sqrt{5})(x^2 + \sqrt{5})$, the polynomial's roots are $\{\pm\sqrt[4]{5}, \pm\sqrt[4]{5}i\}$. So the splitting field of $x^4 - 5$ over $\mathbb{Q}$ is $F = \mathbb{Q}(\sqrt[4]{5}, i)$, which has degree 8 over $\mathbb{Q}$.

(c) $x^6 + x^3 + 1$

Because $(x^6 + x^3 + 1)(x^3 - 1) = x^9 - 1$, $\mathbb{Q}(e^{2\pi i/9})$ is the splitting field. The polynomial $x^6 + x^3 + 1$ is irreducible over $\mathbb{Q}$ (plug in $x + 1$ for x) with root $e^{2\pi i/9}$. Since $e^{2\pi i/9}$ generates all the roots of $x^9 - 1$, it must generate all the roots of $x^6 + x^3 + 1$. So the degree of the extension is 6.

6. Let n be an integer ≥ 3 and let $\omega = e^{\frac{2\pi i}{n}}$.

(a) Prove that $\mathbb{Q}(\omega)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

We need to check 2 conditions:

(a) Every root of $x^n - 1$ is in $\mathbb{Q}(\omega)$.
Every root of $x^n - 1$ is of the form ω^k, where $0 \leq k \leq n - 1$. This is because ω is a primitive nth root of unity, meaning $\omega^n = 1$ and its powers generate all n distinct roots of unity. Since $\mathbb{Q}(\omega)$ contains all powers of ω, it contains all the roots of $x^n - 1$.

(b) $\mathbb{Q}(\omega)$ is the smallest field extension of $\mathbb{Q}$ containing all the roots of $x^n - 1$.
We observe that $\mathbb{Q}(\omega)$ is generated by ω, and therefore contains all powers of ω. Any other field containing all roots must contain ω, hence it must contain $\mathbb{Q}(\omega)$.

Therefore, $\mathbb{Q}(\omega)$ is indeed the splitting field of $x^n - 1$ over $\mathbb{Q}$.

(b) Find its degree for $n = 3, 4, 5, 6, 7, 8$.

$n = 3$: $x^3 - 1 = (x - 1)(x^2 + x + 1)$. The roots are 1 and $\frac{-1 \pm i\sqrt{3}}{2}$. The splitting field has degree 2.

$n = 4$: $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$. The roots are 1, -1, i, and $-i$. The splitting field has degree 2.

$n = 5$: $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$. Since the second polynomial is irreducible over $\mathbb{Q}$ by the eisenstein criterion. By setting $y = x +$

$\frac{1}{x}$, we obtain a quadratic for y and solve it to see that the roots are 1, $\frac{-1+\sqrt{5}\pm i\sqrt{10+2\sqrt{5}}}{4}$ and $\frac{-1-\sqrt{5}\pm i\sqrt{10-2\sqrt{5}}}{4}$. The splitting field has degree 4.

$n = 6$: $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$. The roots are 1, -1, and $\frac{\pm 1 \pm i\sqrt{3}}{2}$ for all four possible choices of the $\pm$ signs. The splitting field has degree 2.

$n = 7$: $x^7 - 1 = (x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$. Again, it turns out that the second factor is irreducible by the eisenstein criterion, so the splitting field has degree 6.

$n = 8$: $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$. The roots are 1, -1, $\pm i$, and $\pm(1 \pm i\sqrt{2})$, for all four choices of sign. The splitting field is $\mathbb{Q}(i, \sqrt{2})$ and has degree 4.

So, summarizing:

1. For $n = 3, 4, 6$, the degree of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is 2.
2. For $n = 5, 8$, the degree is 4.
3. For $n = 7$, the degree is 6.

7.

(a) Find the minimum polynomial of $\cos\left(\frac{2\pi}{5}\right)$. (You might find the identities $\cos(2\theta) = 2\cos^2\theta - 1$ and $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$ helpful.)

Let $x = \cos\left(\frac{2\pi}{5}\right)$. We know that $\cos\left(\frac{2\pi}{5}\right)$ is a root of the equation $x^5 - 1 = 0$ because $\cos\left(\frac{2\pi}{5}\right)$ represents the cosine of a regular pentagon's interior angle. Thus, the minimal polynomial of $\cos\left(\frac{2\pi}{5}\right)$ divides $x^5 - 1$.

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

So we have that $x^4 + x^3 + x^2 + x + 1 = 0$.

$$0 = 1 + x + x^2 + x^3 + x^4 = 1 + (x + x^4) + (x^2 + x^3)$$
$$= 1 + 2x + 2(2x^2 - 1) = 4x^2 + 2x - 1.$$

So the minimal polynomial for $\cos\left(\frac{2\pi}{5}\right)$ is $4x^2 + 2x - 1$.

(b) Prove that a regular pentagon is constructible.

From the fact that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Now we see that α lies in the extension field of degree $4 = 2^2$, and hence, α is constructible.

Also, by the quadratic equation and the fact that $\alpha = \cos(\frac{2\pi}{5}) > 0$, we get

$$\alpha = \frac{-1 + \sqrt{5}}{4}.$$

Hence, α is constructible over $\mathbb{Q}$.