$\frac{45}{45}$

MODERN ALGEBRA II.
Homework 8.

Seungmin Park
UNI: sp2723.

(1) Determine the degrees of the splitting fields of the following polynomials over $\mathbb{Q}$.

(a) $x^4 - 1$.

Sol. The unique factorization ($\mathbb{Q}[x]$ is UFD) is

$$x^4-1 = (x^2-1)(x^2+1) = (x-1)(x+1)(x-i)(x+i),$$

So the roots of this polynomial are $\pm 1, \pm i$. Then the splitting field is the smallest field extension of $\mathbb{Q}$ containing these roots, i.e. $\mathbb{Q}(-1, 1, -i, i) = \mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2+1)$

Hence the degree of the splitting field is

$$\deg_{\mathbb{Q}} \mathbb{Q}(i) = \deg (x^2+1) = 2 \checkmark$$

5

(b) x^4+1

Sol. The factorization is given by

$$x^4+1 = (x^2+i)(x^2-i)$$
$$= \left(x - \tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i\right)\left(x + \tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i\right)\left(x - \tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i\right)\left(x + \tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i\right)$$

Hence the splitting field is

$$\mathbb{Q}\left(-\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i,\ -\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i,\ \tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i,\ \tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i\right) = \mathbb{Q}(\sqrt{2}, i).$$

So the degree of it is:

$$\deg_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, i) = \underbrace{\deg_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})}_{\substack{=2\text{, as the} \\ \text{minimal poly is} \\ x^2-2 \text{ over } \mathbb{Q}}} \cdot \underbrace{\deg_{\mathbb{Q}(\sqrt{2})} \mathbb{Q}(\sqrt{2}, i)}_{\substack{=2 \text{ also, as the} \\ \text{min poly is} \\ x^2+1 \text{ over } \mathbb{Q}(\sqrt{2})}}$$

$$= 4 \checkmark$$

(2) Let $\omega = e^{2\pi i/3}$. Show that the extension $\mathbb{Q} \subset \mathbb{Q}(\omega, \sqrt[3]{2})$ is Galois and its Galois group is isomorphic to S_3.

Pf

Consider the polynomial x^3-2. Its roots are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ as $(\sqrt[3]{2})^3 = (\omega\sqrt[3]{2})^3 = (\omega^2\sqrt[3]{2})^3 = 2$, and since there can be at most three roots ($\because$ degree 3), these are all of the roots. Then it is split completely as $(x-\sqrt[3]{2})(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})$ over the splitting field

5

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) \quad (\because \omega^2\sqrt[3]{2} = (\omega\sqrt[3]{2})^2/\sqrt[3]{2}$$

$$= \mathbb{Q}(\omega, \sqrt[3]{2}).$$

So the extension field $\mathbb{Q} \subset \mathbb{Q}(\omega, \sqrt[3]{2})$ is a splitting field, hence Galois.

also need that the polynomial is separable

Now let $G = \mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}))$, and let us try to find out what group this is. First, $|G| = \deg(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}) = \deg(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \cdot \deg(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})) = 3 \cdot 2 = 6$ as it is Galois. Now consider the homomorphism $\sigma: K \to K$ that sends $\sqrt[3]{2} \rightsquigarrow \omega\sqrt[3]{2}$ and fixes ω, then σ is of order 3 as $\sigma^3 = \mathrm{id}$. Also, let τ denote the homomorphism $K \to K$ that sends $\omega \rightsquigarrow \omega^2$ and fixes $\sqrt[3]{2}$, then τ is of order 2 as $\tau^2 = \mathrm{id}$. Observe that $\tau\circ\sigma$ sends $\sqrt[3]{2} \rightsquigarrow \omega\sqrt[3]{2} \rightsquigarrow \omega^2\sqrt[3]{2}$, $\omega \rightsquigarrow \omega^2$, whereas $\sigma\circ\tau$ sends $\sqrt[3]{2} \rightsquigarrow \omega\sqrt[3]{2}$ and $\omega \rightsquigarrow \omega^2$, so $\tau\circ\sigma = (\sigma\circ\tau)^{-1}$. This gives a group of homomorphisms $\{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3$. There can be at most 6 homomorphisms since $\sqrt[3]{2}$ must be sent to one of the three roots of its minimal polynomial, $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, and ω must be sent to either ω or ω^2. Then these 6 are all of the homomorphisms $K \to K$, and since we know that there are 6 automorphisms, these 6 homomorphisms must in fact be those automorphisms. Thus

Let K denote $\mathbb{Q}(\omega, \sqrt[3]{2})$

$$G = \mathrm{Gal}(\mathbb{Q}(\omega,\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3$$

$\square$

(3) Let $F \subset K$ be a splitting field of $p(x) \in F[x]$ and set $n = \deg(p(x))$. Show that $Gal(K/F)$ is a subgroup of S_n.

<u>Pf</u>.

We can write the irreducible factorization ($\because$ $F[x]$ UFD for F field)

$$p(x) = p_1(x) p_2(x) \cdots p_m(x)$$

where the degree of $p_i(x)$ is some $n_i \in \mathbb{N}$, such that $n_1 + n_2 + \cdots + n_m = n$.

5

Now consider an automorphism $\sigma \in Gal(K/F)$. If $p_i(x)$ is of degree 1, then its root is in F, hence σ must fix this root. If $p_i(x)$ is of degree $n_i > 1$, then σ must send one of the root to any of the d roots, so σ is a permutation of the n_i roots. Thus ✓

$$Gal(K/F) \subset S_{n_1} \times S_{n_2} \times \cdots \times S_{n_m} \underset{\uparrow}{\subset} S_n$$

($\because$ $n = n_1 + n_2 + \cdots + n_m$).

$\blacksquare$

(4) Let $F \subset K$ be finite fields where $|F| = p^m$ and $|K| = p^n$. Show that m divides n.

Pf

Since F, K are finite, they cannot have characteristic zero, and since the two are fields, they must have a prime characteristic. Then F, K must contain prime fields $\mathbb{F}_{p_1}, \mathbb{F}_{p_2}$, respectively, for some prime p_1, p_2. Since F, K are finite dimensional $\mathbb{F}_{p_i}$-vector space, $i = 1, 2$, respectively, p_1 divides p^m and p_2 divides p^n. So $p_1 = p_2 = p$.

5

Thus we have a tower of fields

$$\mathbb{F}_p \subset F \subset K,$$

hence by multiplication formula,

$$\deg_{\mathbb{F}_p} K = \deg_{\mathbb{F}_p} F \cdot \deg_F K,$$

where $\deg_{\mathbb{F}_p} K = n$ and $\deg_{\mathbb{F}_p} F = m$, because as K, F are $\mathbb{F}_p$-vector spaces, their order is p to the power of their respective degrees.

Thus, $n = m \cdot \deg_F K$, hence m divides n. ✓

□

(Alternatively, one can directly consider K as F-vector space of some finite degree k. Then the order of K is the k-th power of that of F, i.e.

$$|K| = (|F|)^k = (p^m)^k = p^{km}, \qquad k \in \mathbb{N}.$$

so $p^n = p^{km}$ thus $n = km$.)

(5) Conversely, show that if m divides n, then the subset
$$\{x \in K \mid x^{p^m} = x\} \subset K$$
is a subfield of order p^m

Pf

Suppose $n = km$ for some $k \in \mathbb{N}$, and let us show that $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} = K$. Take any $\alpha \in \mathbb{F}_{p^m}$, then α is a root of the polynomial $x^{p^m} - x$, because $x^{p^m - 1} = 1$ for all $x \in \mathbb{F}_{p^m}^{\times}$ the multiplicative group. So $\alpha^{p^m} = \alpha$.
Now because $n = km$,

5

$$\alpha^{p^n} - \alpha = \alpha^{(p^m)^k} - \alpha = \alpha^{\overbrace{p^m \cdot p^m \cdots p^m}^{k \text{ times}}} - \alpha$$

$$= \underbrace{((\cdots(\underbrace{\underbrace{\alpha^{p^m}}_{\alpha})^{p^m}}_{=\alpha})\cdots)^{p^m}}_{\alpha} - \alpha \qquad (\because \alpha^{p^m} = \alpha).$$

$$= \alpha - \alpha$$

$$= 0$$

So α is a root of the polynomial $x^{p^n} - x = x^{p^{km}} - x$ as well, meaning that $\alpha \in \mathbb{F}_{p^n}$. ($\because$ Elements of $\mathbb{F}_{p^n}$ are the roots of $x^{p^n} - x$, as $x^{p^n - 1} = 1$ for all $x \in \mathbb{F}_{p^n}^{\times}$ and $x^{p^n} - x$ is separable as its "derivative" is a nonzero constant, so there are p^n distinct roots of $x^{p^n} - x$). Hence $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$. ✓

We know that $\{x \in K \mid x^{p^m} = x\} = \mathbb{F}_{p^m} \cap K$ (the roots of $x^{p^m} - x$ are elements of $\mathbb{F}_{p^m}$), and we showed that $\mathbb{F}_{p^m} \subset K$, so

$$\{x \in K \mid x^{p^m} = x\} = \mathbb{F}_{p^m} \cap K = \mathbb{F}_{p^m} \subset K, \qquad ✓$$

which thence is a subfield of order p^m. $\square$

(6) Let $F \subset K$ be finite fields where $|F| = p^m$ and $|K| = p^n$. Show that K/F is Galois, and $\mathrm{Gal}(K/F)$ is cyclic of order n/m, generated by the automorphism $x \rightsquigarrow x^{p^m}$.

Pf.

Consider the polynomial $x^{p^n} - x$. Since all of its roots are the distinct elements of $K = \mathbb{F}_{p^n}$, it splits completely over K and is separable, hence K/F is Galois. ✓

Now let σ denote the automorphism over K that sends $x \rightsquigarrow x^{p^m}$, for all $x \in K$. Then

5

σ sends $x \rightsquigarrow x^{p^m}$ ← This fixes all $x \in F$ since $x^{p^m} = x$ for all $x \in F$

σ^2 " $x \rightsquigarrow (x^{p^m})^{p^m} = x^{p^m p^m} = x^{p^{2m}}$

σ^3 " $x \rightsquigarrow x^{p^{3m}}$

$\vdots$

$\sigma^{n/m}$ sends $x \rightsquigarrow x^{p^{\frac{n}{m}\cdot m}} = x^{p^n} = x$ ✓

an integer because m divides n, from problem 4

($\because \mathbb{F}_{p^n}^\times$ is of order $p^n - 1$, so $x^{p^n-1} = 1$ for all x)

So $\sigma^{n/m}$ is the identity automorphism, hence we have the cyclic group of automorphisms generated by σ, of order n/m. ✓

Lastly, since K/F is Galois, $|\mathrm{Gal}(K/F)| = \deg(K/F)$ $= (\deg K/\mathbb{F}_p)/(\deg F/\mathbb{F}_p) = n/m$, so there is no other automorphisms. ✓

$\therefore \mathrm{Gal}(K/F) = \langle \sigma \rangle = \{ id, \sigma, \sigma^2, \ldots, \sigma^{n/m - 1} \}$.

where $\sigma \in \mathrm{Aut}(K/F)$ that sends $x \rightsquigarrow x^{p^m}$.

$\square$

(7) Let F be a field of characteristic p and $f(x) \in F[x]$ a polynomial. Show that $Df(x) = 0$ if and only if $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.

Pf

Suppose first that $f(x) = g(x^p)$ for some $g(x) \in F[x]$. Then

$$Df(x) = D(g(x^p)) \underset{\because \text{ chain rule}}{=} Dg(x^p) \cdot D(x^p) = Dg(x^p) \cdot p x^{p-1} \underset{\because \text{ characteristic } p}{=} 0$$

5

hence $Df(x) = 0$. ✓

Conversely, suppose $Df(x) = 0$, and suppose $f(x) \neq g(x^p)$ for some $g(x) \in F[x]$. Then $f(x)$ contains a term of degree not divisible by p, say q, i.e.

$$f(x) = a \cdot x^q + (\text{all other terms of degree other than } q).$$

for some nonzero $a \in F$. Then $Df(x) = a \cdot q x^{q-1} + (\text{all other terms of degree other than } q-1)$.

Then p does not divide the coefficient aq, because $p \nmid a$, $p \nmid q$, and p is prime. Hence $aq x^{q-1} \neq 0$, and thus $Df(x) \neq 0$, a contradiction. So $f(x)$ must only contain terms with degree divisible by p, i.e. $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

✓ $\square$

(8) F is called perfect if the Frobenius homomorphism $F \to F$ given by $x \mapsto x^p$ is an isomorphism. Show that a finite field is perfect.

Pf.

Consider a finite field $\mathbb{F}_{p^n}$; p prime, $n \in \mathbb{N}$:

① Take any $a, b \in \mathbb{F}_{p^n}$. Then

$$\mathrm{Frob}(a+b) = (a+b)^p \underset{\uparrow}{=} a^p + b^p = \mathrm{Frob}(a) + \mathrm{Frob}(b)$$

($\because$ characteristic p).

5

$$\mathrm{Frob}(ab) = (ab)^p = a^p \cdot b^p = \mathrm{Frob}(a) \cdot \mathrm{Frob}(b) \checkmark$$

$\therefore$ The Frobenius function is indeed a homomorphism.

② Since $\mathbb{F}_{p^n}$ is a field, $\ker(\mathrm{Frob}) = \{0\}$ or $\mathbb{F}_{p^n}$ as the kernel is an ideal. But it cannot be the whole field as $\mathrm{Frob}(1) = 1^p = 1 \neq 0$. So $\ker(\mathrm{Frob}) = \{0\}$, hence Frob is injective. This implies Frob is surjective as it maps onto the same finite field. ✓

$\therefore$ Frob is an isomorphism.

$\Rightarrow \mathbb{F}_{p^n}$ is perfect.

$\square$

(9) Let F be a perfect field and $f(x) \in F[x]$ an irreducible polynomial. Show that $f(x)$ is separable.

Pf.

Case 1) F is of characteristic 0

Then $\gcd(f(x), Df(x)) = 1$ since $f(x)$ is irreducible and $Df(x) \neq 0$, hence separable. ✓

Case 2) F is of characteristic p, p prime.

Suppose $f(x)$ is not separable, i.e. $\gcd(f(x), Df(x)) \neq 1$. We know that $f(x)$ is irreducible, so it must be that $Df(x) = 0$. From Problem (7), this implies that $f(x) = g(x^p)$ for some $g(x) \in F[x]$, that is,

$$f(x) = a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots + a_1 x^p + a_0 \checkmark$$

for some $a_0, \cdots, a_n \in F$ and $n \in N$. Here, since F is perfect, $a_i = b_i^p$ for some $b_i \in F$, for all i. Thus

$$f(x) = b_n^p (x^n)^p + b_{n-1}^p (x^{n-1})^p + \cdots + b_1^p x^p + b_0^p$$

$$= (b_n x_n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)^p, \checkmark$$

where the last equality is due to the fact that F is of characteristic p. Then $f(x)$ is not irreducible, a contradiction.

$\therefore$ $f(x)$ is separable. ✓

$\square$

5