EXERCISES GALOIS THEORY AND SOME SOLUTIONS

CARSTEN DIETZEL, SILVIA PROPERZI

1. Week 1

Exercise 1.1. Let $\sigma : K \to L$ be a field homomorphism, prove that σ is injective.

Solution. [*using ring theory*] We know that $\ker\sigma$ is an ideal of K. But K is a field so the only possibilities are that $\ker\sigma = \{0\}$ or $\ker\sigma = K$. As $\sigma(1) = 1 \neq 0$, we know that $1 \notin \ker\sigma$, hence $\ker\sigma = \{0\}$ which means that σ is injective. ■

Solution. [*by hands*] Let $a, b \in K$ such that $\sigma(a) = \sigma(b)$. Then

$$\sigma(a-b) = \sigma(a) - \sigma(b) = 0.$$

If we assume that $a \neq b$, then $a - b$ is a non-zero element in a field, hence it is invertible. Then

$$1 = \sigma(1) = \sigma((a-b)(a-b)^{-1}) = \sigma(a-b)\sigma((a-b)^{-1}) = 0,$$

which is a contradiction. Therefore $a = b$ and so σ is injective. ■

Exercise 1.2. Let K be a field, K_0 be its prime field and $\sigma : K \to K$ be a field homomorphism. Prove that $\sigma \in \mathrm{Hom}(K/K_0, K/K_0)$.

Exercise 1.3. Let $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$, $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}(i) = \{\frac{a+ib}{c+di} \mid a, b, c, d \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{2}) = \{\frac{a+\sqrt{2}b}{c+\sqrt{2}d} \mid a, b, c, d \in \mathbb{Q}\}$.

(i) Prove that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}(i) = \mathbb{Q}[i]$.
(ii) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are not isomorphic.

Solution.

(i) Clearly for every field extension L/K and every $\alpha \in L$ we have that $K[\sqrt{2}] \subseteq K(\alpha)$.

Vice versa take $\frac{a+\sqrt{2}b}{c+\sqrt{2}d} \in \mathbb{Q}(\sqrt{2})$, then we can write:

$$\frac{a+\sqrt{2}b}{c+\sqrt{2}d} = \frac{(a+\sqrt{2}b)(c-\sqrt{2}d)}{(c+\sqrt{2}d)(c-\sqrt{2}d)} = \frac{ac-2bd+(bc-ad)\sqrt{2}}{c^2-2d^2}.$$

Hence

$$\frac{a+\sqrt{2}b}{c+\sqrt{2}d} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

In a similar way, given $\frac{a+ib}{c+id} \in \mathbb{Q}(i)$, we can write it as

$$\frac{a+ib}{c+id} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \mathbb{Q}[i].$$

(ii) Assume that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ were isomorphic and let $\varphi : \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$ be a field isomorphism. Then

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1.$$

But $\varphi(i) \in \mathbb{Q}(\sqrt{2})$ and, using the previous part of the exercise, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ where every square is positive, a contradiction. ■

Exercise 1.4.

(i) Let $a = \sqrt{2}$ and $b = \sqrt[3]{3}$. Prove that ab is algebraic over $\mathbb{Q}$.
(ii) Show that $\sqrt{2} + i$ is algebraic over $\mathbb{Q}$ by finding a nonzero polynomial $f \in \mathbb{Q}[X]$ with $\deg(f) = 4$ such that $f(\sqrt{2} + i) = 0$. What are the other roots of f?

Solution.

(i) Observe that $ab^6 = \sqrt{2}^6 \sqrt[3]{3}^6 = 8 \cdot 9 = 72$. Therefore ab is a root of the polynomial $X^6 - 72 \in \mathbb{Q}[X]$.
(ii) let $\alpha = \sqrt{2} + i$. Then $\alpha^2 = 2 + 2\sqrt{2}i - 1 = 1 + 2\sqrt{2}i$ and $\alpha^2 - 1 = 2\sqrt{2}i$. Squaring both sides of the last equality we have that

$$\alpha^4 - 2\alpha^2 + 1 = (\alpha^2 - 1)^2 = (2\sqrt{2}i)^2 = -8.$$

Therefore the polynomial

$$f(X) = X^4 - 2X^2 + 1 + 8 = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$$

is such that $f(\alpha) = 0$.

Looking for other roots of f means to find all $x \in C$ such that $f(x) = 0$, i.e. $x^4 - 2x^2 + 9 = 0$. Going back to how we construct f, this equation can also be written as $(x^2 - 1)^2 = (2\sqrt{2}i)^2$. Therefore $x^2 - 1 = 2\sqrt{2}i$ or $x^2 - 1 = -2\sqrt{2}i$. So

$$x^2 = 2\sqrt{2}i + 1 = \alpha^2 \qquad \text{or} \qquad x^2 = -2\sqrt{2}i + 1 = \overline{\alpha^2} = \overline{\alpha}^2,$$

where $\overline{\alpha}$ indicates the complex conjugate of α. Thus $x = \pm\alpha$ or $x = \pm\overline{\alpha}$ and the 4 roots of f are

$$x_1 = \alpha = \sqrt{2} + i, x_2 = -\alpha = -\sqrt{2} - i,$$

$$x_3 = \overline{\alpha} = \sqrt{2} - i, x_4 = -\overline{\alpha} = -\sqrt{2} + i.$$

■

Exercise 1.5. Let p be a prime number. Denote by $\binom{n}{k}$ the binomial coefficient "n over k".

(i) Prove that p divides $\binom{p}{k}$ for $1 \leq k \leq p - 1$.
(ii) Let K be a field of characteristic p. Show that the map $\Phi : K \to K; x \mapsto x^p$ is a field endomorphism. This map is called the *Frobenius endomorphism* of K.

Solution.

(i) Note that $p \nmid i$ for $1 \leq i \leq p - 1$, therefore $p \nmid 1 \cdot 2 \ldots \cdot k = k!$ for $k \leq p$. If $k \geq 1$, then $p \nmid (p - k)!$ for the same reason.

We have $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ which can also be written as

$$p! = \binom{p}{k} \cdot k! \cdot (p - k)!$$

If $1 \leq k \leq p - 1$, then $p|p!$, so p has to divide at least one factor on the right side. As $p \nmid k!, (p - k)!$, it follows that $p|\binom{p}{k}$.
(ii) Clearly, $\Phi(1) = 1^p = 1$. As K is commutative under multiplication, we see for arbitrary $x, y \in K$ that

$$\Phi(xy) = (xy)^p = x^p y^p = \Phi(x)\Phi(y).$$

Furthermore,

$$\begin{aligned}\Phi(x+y) &= (x+y)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} x^p y^{p-k} \\ &= x^p + y^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{=0} x^k y^{p-k} \\ &= x^p + y^p = \Phi(x) + \Phi(y).\end{aligned}$$

Note that $\binom{p}{k} = 0$ for $1 \leq k \leq p-1$ follows from the divisibility $p|\binom{p}{k}$ proven in the previous part.

Therefore, Φ is a field homomorphism.

■

Exercise 1.6. Let L/K be a field extension and let M be a subring of L that contains K. Suppose that $\dim_K M < \infty$.

(i) Prove that for any $\alpha \in M$, there is a nonzero $f \in K[X]$ with $f(\alpha) = 0$.
Hint: The elements α^n $(n \geq 0)$ are linearly dependent.

(ii) Prove that M is a field.
Hint: For any $0 \neq \alpha \in K$, let $f \in \mathbb{Q}[X]$ be a nonzero polynomial with $f(\alpha) = 0$ whose degree is as small as possible. If $f = \sum_{i=0}^{\infty} a_i X^i$, prove that $a_0 \neq 0$ and use this to construct an inverse of α that lies in M.

Solution. (i) Let $n = \dim_K M$, then $\alpha^0, \alpha^1 \ldots, \alpha^n$ are linearly dependent over K, so there are $a_i \in K$ $(0 \leq i \leq n)$, not all $a_i = 0$, such that

$$\sum_{i=0}^{n} a_i \alpha^i = 0.$$

Using those a_i, define the polynomial $f = \sum_{i=0}^{n} a_i X^i$. By choice of the a_i's, we have $f \neq 0$ and

$$f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0.$$

(ii) Let $\alpha \neq 0$. We have to show that $\alpha^{-1} \in K$. Choose $0 \neq f \in K[X]$ with $f(\alpha) = 0$ such that $n = \deg f$ is as small as possible. Write $f = \sum_{i=0}^{n} a_i X^i$, then, by minimality of n, $a_n \neq 0$. We show that $a_0 \neq 0$: suppose otherwise, then

$$\begin{aligned} f = \sum_{i=1}^{n} a_i X^i &= X \cdot \sum_{i=0}^{n-1} a_{i+1} X^i =: X \cdot g \\ \Rightarrow 0 = f(\alpha) &= \alpha \cdot g(\alpha) \\ \overset{\alpha \neq 0}{\Rightarrow} g(\alpha) &= 0. \end{aligned}$$

But then $g(\alpha) = 0$, and $\deg g < \deg f$, contradicting the minimality of n!

Therefore, $a_0 \neq 0$, and we can rewrite

$$\begin{aligned} \sum_{i=0}^{n} a_i \alpha^i &= 0 \\ \Rightarrow \sum_{i=1}^{n} a_i \alpha^i &= -a_0 \\ \Rightarrow \alpha \cdot \sum_{i=0}^{n-1} a_{i+1} \alpha^i &= -a_0 \\ \Rightarrow \alpha^{-1} = -a_0^{-1} \cdot \sum_{i=0}^{n-1} a_{i+1} \alpha^i &\in M. \end{aligned}$$

The inclusion in M follows from the fact that M contains K and α and is closed under multiplication and addition.

■

Exercise 1.7. Let K be field.

(i) Prove that $K[X]$ is a PID.
(ii) Let $I \neq \{0\}$ be an ideal of $K[X]$, then there exists a unique monic polynomial that generates I as an ideal.

2. Week 2

Exercise 2.1. Let L/K be a field extension and let $\alpha, \beta \in L$ such that

$$[K(\alpha) : K] = [K(\beta) : K] = 2.$$

Assume that the characteristic of K is not 2.

(i) Prove that there is an $\alpha' \in L$ such that $K(\alpha') = K(\alpha)$ and $\alpha'^2 \in K$.
(ii) Assume that $\alpha, \beta \in L$ satisfy $\alpha^2, \beta^2 \in K$. Prove that $K(\alpha) = K(\beta)$ if and only if $\frac{\alpha^2}{\beta^2}$ is a square in K.
(iii) Prove that there is a bijective map

$$K^\times/(K^\times)^2 \longrightarrow \{L \mid L/K \text{ is a field extension with } [L : K] \leq 2\}.$$

Solution.

(i) Since $[K(\alpha) : K] = 2$, $\alpha \notin K$ and the 3 elements $1, \alpha, \alpha^2$ are linearly dependent over K. Thus there exist $a_0, a_1, a_2 \in K$ not all zero such that

$$a_0 + a_1\alpha + a_2\alpha^2 = 0.$$

If $a_2 = 0$, then $a_0 + a_1\alpha = 0$, hence either $a_1 = 0$ or $\alpha = -a_0/a_1$. If $a_1 = 0$, the also $a_0 = 0$. But this is not possible because $(a_0, a_1, a_2) \neq (0, 0, 0)$. On the other hand, if $\alpha = -a_0/a_1$, then $\alpha \in K$, a contradiction.

So we have that $a_2 \neq 0$ and we can divide by a_2, obtaining

$$b + a\alpha + \alpha^2 = 0, \text{ i.e. } \alpha^2 + a\alpha = -b,$$

where $a = a_2^{-1}a_1 \in K$ and $b = a_2^{-1}a_0 \in K$. Since we assumed that K has not characteristic two, we can also complete the square:

$$(\alpha + a/2)^2 = \alpha^2 + a\alpha + a^2/4 = -b + a^2/4 \in K.$$

Therefore $\alpha' = \alpha + a/2$ is such that $\alpha'^2 = -b + a^2/4 \in K$. Moreover $\alpha' = \alpha + a/2 \in K(\alpha)$, so $K(\alpha') \subseteq K(\alpha)$ and $\alpha = \alpha' - a/2 \in K(\alpha')$ so $K(\alpha) \subseteq K(\alpha.)$. Therefore $K(\alpha) = K(\alpha')$ and $\alpha'^2 \in K$.

(ii) Assume that $\frac{\alpha^2}{\beta^2}$ is a square in K, i.e. there is a $k \in K$ such that $\frac{\alpha^2}{\beta^2} = k^2$. (Note that $k \neq 0$ otherwise $\alpha = 0 \in K$ and $[K(\alpha) : K] = [K : K] = 1$.)

Then $\alpha = k^2\beta^2$, hence $\alpha = \pm k\beta \in K(\beta)$. So $K(\alpha) \subseteq K(\beta)$. On the other hand, $\beta^2 = \frac{\alpha^2}{k^2}$, hence $\beta = \pm\frac{\alpha}{k} \in K(\alpha)$. So $K(\beta) \subseteq K(\alpha)$. Having proved both inclusions we deduce that $K(\alpha) = K(\beta)$.

Vice versa, assume that $K(\alpha) = K(\beta)$. Knowing that $[K(\alpha) : K] = 2$, we have that $\{1, \alpha\}$ is a generating set of the K-vector space $K(\alpha) = K(\beta)$. Therefore there exist $a, b \in K$ such that $\beta = a + b\alpha$. Squaring both sides of the equality, we get $\beta^2 = a^2 + 2ab\alpha + \alpha^2$. So $2ab\alpha = \beta^2 - a^2 - \alpha^2$ is a sum of elements in K. Hence $2ab\alpha \in K$, but $\alpha \notin K$. Therefore the only possibility is that $2ab = 0$, i.e. (since we are not in characteristic 2) $ab = 0$. But $b \neq 0$, otherwise $\beta = a \in K$, which is not possible (otherwise and $[K(\beta) : K] = [K : K] = 1$). Thus $a = 0$, i.e. $\beta = b\alpha$ and so $\frac{\beta^2}{\alpha^2} = a^2$ is a square in K.

(iii) Let L/K be a field extension with $[L : K] = 2$. Take $\alpha \in L \setminus K$, then

$$1 < [K(\alpha) : K] \leq [L : K] = 2.$$

Hence $L = K(\alpha)$. Moreover, the first part of this exercise allows us to choose α such that $\alpha^2 \in K$. Now we can define the following map

$$\psi : \{L \mid L/K \text{ is a field extension with } [L : K] \leq 2\} \to K^\times/(K^\times)^2$$

as $\psi(K) = [1]$ and for $[L : K] = 2$ as $\psi(L) = [\alpha^2] \in K^\times/(K^\times)^2$, for $\alpha \in L \setminus K$ (so $L = K(\alpha)$) such that $\alpha^2 \in K$.

This map is well-defined: take L/K of degree 2 and $\alpha, \beta \in L\backslash K$ such that $\alpha^2 \in K$. Then, by the remark made at the beginning, $L = K(\alpha) = K(\beta)$ As shown in the second part of this exercise, this is equivalent to $\frac{\alpha^2}{\beta^2} \in (K^\times)^2$, so $[\alpha^2] = [\beta^2] \in K^\times/(K^\times)^2$. (Note also that $[\alpha^2] = [1]$ if and only if $\alpha^2 = k^2 \in K^2$, so $\alpha = \pm k \in K$ and $K(\alpha) = L$.)

Let now prove that ψ is injective. Assume that we have two extension L/K and L'/K of degree ≤ 2, such that $[\alpha^2] = \psi(L) = \psi(L') = [\beta^2]$.

If $[\beta^2] = [\alpha^2] = [1]$, then $L = K(\alpha) = K = K(\beta) = L'$.

Otherwise, $\beta^2/\alpha^2 \in (K^\times)^2$, so, by the previous part of this exercise, $L = K(\alpha) = K(\beta) = L'$.

Finally, for the subjectivity, let $x \in K^\times$. If $x \in (K^\times)^2$, then $x = \alpha^2$ for some $\alpha \in K^\times$ and so $L = K(\alpha)$ is an extension of K of degree ≤ 2 and $\psi(L) = [\alpha]$.

If $x \notin (K^\times)^2$, then we can find and extension $L = K(\alpha)$ such that $\alpha^2 = x \in K^\times$ and so $\psi(L) = [x] \in K^\times/(K^\times)^2$. To construct this extension consider the polynomial $f(X) = X^2 - x \in K[X]$. It has to be irreducible, otherwise $X^2 - x = (aX + b)(cX + d) = acX^2 + (ad + bc)X + bd$, for some $a, c \in K^\times$ and $b, d \in K$. So $1 = ac$, $0 = ad + bc$ and $-x = bd$, i.e. $c = a^{-1}$, $d = -a^{-1}bc = bc^2$ and $-x = bd = b^2c^2 \in (K^\times)^2$, a contradiction to the assumption $x \notin (K^\times)^2$. Then we can consider the field $L = K[X]/(X^2 - x)$ that contains K (it is a field because the ideal $(X^2 - x)$ is maximal, since it is generated by an irreducible polynomial). Defining α as the class of X in L we get that $L = K(\alpha)$ and $\alpha^2 = x \in K$. ■

Exercise 2.2. Let E/K be a field extension and a and b be algebraic over K.

(1) Assume that $[K(a) : K] = m$, $[K(b) : K] = n$. Prove that $K[a, b] \subseteq E$ is generated, as a vector space over K, by the elements $a^i b^j$ $(1 \leq i \leq m, 1 \leq j \leq n)$.
(2) Prove that $a + b$ and ab are algebraic over K. Can you estimate the quantities $[K(a + b) : K]$ and $[K(ab) : K]$?
(3) Find a polynomial $f \in \mathbb{Q}[X]$ such that $\deg(f) \leq 6$ and $f(\sqrt[3]{3} + \sqrt{5})$.

Solution.

(1) We know that $\{b^j \mid 1 \leq j \leq n\}$ is a K-basis of $K(b)$, so it also generates $K[a, b] = (K[a])[b] = (K(a))[b]$ as a $K(a)$-vector space. Now let $x \in K[a, b]$, then we can write it as

$$x = \sum_{j=1}^{n} \alpha_j b^j,$$

for some $\alpha_j \in K(a)$. Moreover $\{a^i \mid 1 \leq i \leq m\}$ is a K-basis of $K(a)$, hence for every j,

$$\alpha_j = \sum_{i=1}^{m} k_{i,j} a^i,$$

for some $k_{i,j} \in \mathbb{Q}$. Putting everything together we get

$$x = \sum_{j=1}^{n} \alpha_j b^j = \sum_{j=1}^{n} \sum_{i=1}^{m} k_{i,j} a^i b^j,$$

so $\{a^i b^j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ generates $K[a, b]$ as a K vector space.

(2) We know that $K(a)/K$ is finite and that $K(b)/K$ is finite, so also $K(a)(b)/K$ is finite. Therefore, considering the tower of extension $K \subseteq K(a) \subseteq K(a)(b) = K(a, b)$, we get that $K(a, b)/K$ is a finite extension, hence also algebraic. Therefore $a + b, ab \in K(a, b)$ are algebraic over K.

(3) Let $g(X) = X^3 - 3 \in \mathbb{Q}[X]$. Then $g(\sqrt[3]{3}) = 0$, hence we can use the "conjugation" trick and consider the polynomial $f(X) = g(X - \sqrt{5})g(X + \sqrt{5})$, which has degree 6 and $f(\sqrt[3]{3} + \sqrt{5}) = 0$.

$$\begin{aligned} f(X) =& g(X - \sqrt{5})g(X + \sqrt{5}) = ((X - \sqrt{5})^3 - 3)((X + \sqrt{5})^3 - 3) = \\ & (X - \sqrt{5})^3(X + \sqrt{5})^3 - 3((X - \sqrt{5})^3 + (X + \sqrt{5})^3) + 9 \end{aligned}$$

But we can compute

$$\begin{aligned} &(X-\sqrt{5})^3 + (X + \sqrt{5})^3 = \\ &(X - \sqrt{5} + X + \sqrt{5})((X - \sqrt{5})^2 - (X - \sqrt{5})(X + \sqrt{5}) + (X + \sqrt{5})^2) = \\ &2X((X - \sqrt{5})(X - \sqrt{5} - X - \sqrt{5}) + X^2 + 2\sqrt{5}X + 5) = \\ &2X(-2\sqrt{5}(X - \sqrt{5}) + X^2 + 2\sqrt{5}X + 5) = \\ &2X(10 + X^2 + 5) = 2X^3 + 30X. \end{aligned}$$

Therefore

$$\begin{aligned} f(X) =& (X^2 - 5)^3 - 3(2X^3 + 30X) + 9 = \\ & X^6 - 15X^4 + 75X^2 - 125 - 6X^3 - 90X + 9 = \\ & X^6 - 15X^4 - 6X^3 + 75X^2 - 90X - 116. \end{aligned}$$

■

The following lemma can be used, without proof, in the following exercise.

Lemma (Gauss' Lemma)**.** *Let A be a unique factorization domain and K be its fraction field. A non-constant polynomial $f \in A[X]$ is irreducible if and only if is primitive and is irreducible in $K[X]$.*

Exercise 2.3 (Eisenstein's irreducibility criterion)**.** Let A be a unique factorization domain and K be its fraction field. Let $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ be a polynomial of degree $n > 0$. Assume that there exists a prime element $p \in A$ such that $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $K[X]$.

Exercise 2.4. Let $\zeta \in \mathbb{C}$ be a primitive cubic root of one. Set $E = \mathbb{Q}[\sqrt[3]{2}]$, $F = \mathbb{Q}(\zeta)$ and $L = \mathbb{Q}[i]$.

(i) Prove that $[E : \mathbb{Q}] = 3$ and $[F : \mathbb{Q}] = 2$ and compute the minimal polynomial of ζ over $\mathbb{Q}$ and over L.
(ii) Prove that $EF = \mathbb{Q}(\sqrt[3]{2}, \zeta)$.
(iii) Compute $[EF : \mathbb{Q}]$ and $[E \cap F : \mathbb{Q}]$.

Solution. See Exercise 3.4 ■

Exercise 2.5. Let E/K be a field extension and let L/K and M/K be subextensions.

(i) Prove that $[LM : K] \cdot [L \cap M : K] \leq [L : K] \cdot [M : K]$.
(ii) Can you find examples where $[LM : K] \cdot [L \cap M : K] < [L : K] \cdot [M : K]$? *Hint:* Use two different roots of the polynomial $X^3 - 2$.

Solution. See Exercise 3.5 ■

Exercise 2.6. Let E/K be a field extension and let $f \in K[X]$ be a polynomial such that f factorizes in $E[X]$ as $f = \prod_{i=1}^{n}(x - \alpha_i)$. Prove by induction that $[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] \leq n!$.

Solution. See Exercise 3.6 ■

3. Week 3

Exercise 3.1. For every polynomial $p(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ of degree n, define its *reciprocal polynomial* as

$$\widehat{p}(X) = \sum_{i=0}^{n} a_{n-i} X^i.$$

Let $p(X), q(X) \in K[X]$ be polynomials of degree n and m respectively such that $p(0) \neq 0$ and $q(0) \neq 0$. Prove that

(i) $\widehat{p}(X) = X^n p(1/X)$ in $K(X)$,
(ii) $\widehat{\widehat{p}}(X) = p(X)$,
(iii) $\widehat{pq}(X) = \widehat{p}(X)\widehat{q}(X)$,
(iv) $\widehat{p}(X)$ is irreducible if and only if $p(X)$ is irreducible.

Solution. Suppose that $p(X) = \sum_{i=0}^{n} a_i X^i$ has degree n and $q(X) = \sum_{i=0}^{m} b_i X^i$ has degree m.

(i) $X^n p(1/X) = X^n \sum_{i=0}^{n} a_i (1/X)^i = \sum_{i=0}^{n} a_i X^{n-i} = \sum_{j=0}^{n} a_{n-j} X^j = \widehat{p}(X)$

(ii) Since $p(0) \neq 0$, $a_0 \neq 0$, therefore $\deg(\widehat{p}) = \deg(p) = n$. Hence, using the previous part of this exercise,

$$\widehat{\widehat{p}}(X) = X^n \widehat{p}(1/X) = X^n (1/X)^n p(1/(1/X)) = p(X).$$

(iii) Since $p(0) \neq 0$ and $q(0) \neq 0$ we deduce that also $pq(0) \neq 0$. Hence we can apply the previous results for p, q and pq. So, using also that $pq(1/X) = p(1/X)q(1/X)$ and that $\deg pq = n + m$, we have that

$$\widehat{pq}(X) = X^{n+m} pq(1/X) = X^n p(1/X) X^m q(1/X) = \widehat{p}(X)\widehat{q}(X).$$

(iv) Suppose $\widehat{p}(X)$ is irreducible and let $p = q_1 q_2$ for $q_1(X), q_2(X) \in K[X]$. Note that $0 \neq p(0) = q_1(0)q_2(0)$ implies that both $q_1(0) \neq 0$ and $q_2(0) \neq 0$. Considering now the reciprocal polynomials and using the previous properties, $\widehat{p}(X) = \widehat{q_1}(X)\widehat{q_2}(X)$. Since $\widehat{p}(X)$ is irreducible, there is $i \in \{1, 2\}$ such that $\widehat{q_i}$ is a constant, i.e. $\deg q_i = \deg \widehat{q_i} = 0$. Thus, q_i is a constant too, and therefore $p(X)$ is irreducible.

Vice versa, assume that $p(X)$ is irreducible. Since we know that $p(X) = \widehat{\widehat{p}}$, by the property just proved, we obtain that $\widehat{p}$ is also irreducible. ∎

Exercise 3.2. Let E/K be a field extension and $x \in E$ be an algebraic element and let $f = f(x, K)$ is the minimal polynomial of x over K of degree $\deg(f) = n$.

(i) Prove that $[K(x) : K] = n$.
(ii) Prove that $\frac{1}{f(0)}\widehat{f}$ is the minimal polynomial of $1/x$ over K.
(iii) Write $f(X) = \sum_{i=0}^{n} a_i X^i = p(X^2) + Xd(X^2)$, where

$$p(X) = \sum_{j=0}^{\lfloor n/2 \rfloor} a_{2j} X^j \text{ and } d(X) = \sum_{j=0}^{\lfloor n/2 \rfloor} a_{2j+1} X^j.$$

Let $g(X) = p(X)^2 - Xd(X)^2$ and prove that
- if $d(x^2) = 0$, then the minimal polynomial of x^2 over K is $p(X)$,
- if $d(x^2) \neq 0$, then the minimal polynomial of x^2 over K is $(-1)^n g(X)$.

Solution.

(i) We will prove that $B = \{1, x, \ldots, x^{n-1}\}$ is a basis of $K(x)$ as a K vector space which implies that $[K(x) : K] = \dim_K(K(x)) = |B| = n$.
- *B is a generating set for $K(x)$ as a K vector space.*
To prove this recall that $K(x) = K[x]$, since x is algebraic over K. (Similar proof to 1) ⇒ 2) of Theorem 2.7 of the lecture notes.)

Let $z \in K(x) = K[x]$, say $z = h(x)$ for some $h \in K[X]$. Divide h by f to obtain polynomials $q, r \in K[X]$ such that $h = fq + r$, where $r = 0$ or $\deg r < \deg f = n$. This implies that

$$z = h(x) = f(x)q(x) + r(x) = r(x).$$

Moreover, we can write $r = \sum_{i=0}^{n-1} c_i X^i$ for some $c_0, \dots, c_{n-1} \in K$. Thus $z = \sum_{i=0}^{n-1} c_i x^i \in \langle 1, x, \dots, x^{n-1} \rangle$ and hence $K[x]$ is generated by $\{1, x, \dots, x^{n-1}\}$ as a K-vector space.

- *B is linearly independent over K.*
  If B is linearly dependent over K then there exists a linear combination $0 = \sum_{i=0}^{n-1} c_i x^i$ over K, with not all c_i equal to 0. Then the polynomial $h(X) = \sum_{i=0}^{n-1} c_i X^i$ is in $K[X] \setminus \{0\}$ and has x as a root. So

$$n - 1 = \deg(h) \leq \deg(f) = n,$$

  a contradiction.

(ii) Fist of all we note that $f(0) \neq 0$. Otherwise we can write $f(X) = Xg(X)$ for some $g(X) \in K[X]$, but f is monic and irreducible in $K[X]$, hence $g(X) = 1$ and $f(X) = X$. Evaluating f in x we obtain $0 = f(x) = x$, a contradiction with the hypothesis $x \neq 0$.

Since $f(0) \neq 0$, we can use the previous exercise and obtain that $\widehat{f}$ is also irreducible and $\widehat{f} = X^n f(1/X)$. Hence

$$\frac{1}{f(0)} \widehat{f}\,(1/x) = \frac{1}{f(0)} (1/x)^n f\left(\frac{1}{1/x}\right) = \frac{1}{f(0)x^n} f(x) = 0.$$

So we have that $\frac{1}{f(0)}\widehat{f}$ is an irreducible polynomial in $K[x]$ with $1/x$ as a root. To prove that $\frac{1}{f(0)}\widehat{f}$ is the minimal polynomial of $1/x$ over K it remains to prove that it is monic. Looking at the definition of $\widehat{f}$ we see that its leading coefficient is the constant term of f, i.e. $f(0)$. Therefore the leading coefficient of $\frac{1}{f(0)}\widehat{f}$ is $\frac{1}{f(0)} f(0) = 1$, hence $\frac{1}{f(0)}\widehat{f}$ is monic.

(iii) First of all note that

$$0 = f(x) = p(x^2) + xd(x^2), \tag{1}$$

therefore

$$g(x^2) = p(x^2)^2 - x^2 d(x^2)^2 = (p(x^2) + xd(x^2))(p(x^2) - xd(x^2)) = 0.$$

So x^2 is a root of g and the degree of g is

$$\begin{cases} 2\deg(p) & \text{if } n \text{ is even} \\ 1 + 2\deg(d) & \text{if } n \text{ is odd} \end{cases} = \begin{cases} 2\left\lfloor \frac{n}{2} \right\rfloor & \text{if } n \text{ is even} \\ 1 + 2\left\lfloor \frac{n}{2} \right\rfloor & \text{if } n \text{ is odd} \end{cases} = n.$$

Moreover, by the first point of this exercise and the fact that the degree is multiplicative

$$n = \deg(f) = [K(x) : K] = [K(x) : K(x^2)][K(x^2) : K].$$

Hence, to compute $[K(x^2) : K]$ (which is also the degree of $f(x^2, K)$, the minimal polynomial of x^2 over K), we need to know $[K(x) : K(x^2)]$. Observe that $X^2 - x^2$ is a polynomial in $K(x^2)[X]$ which has x has a root. Thus

$$[K(x^2) : K] = \deg(x, K(x^2)) \leq \deg(X^2 - x^2) = 2$$

Therefore

$$[K(x^2) : K] = \frac{[K(x) : K]}{[K(x) : K(x^2)]} \in \left\{n, \frac{n}{2}\right\}. \tag{2}$$

- If $d(x^2) = 0$, by Equation (1), also $p(x^2) = 0$ and $\deg(p) = \lfloor \frac{n}{2} \rfloor < n$. So

$$[K(x^2) : K] = \deg(f(x^2, K)) \leq \deg(p) < n,$$

thus, by (2), $[K(x^2) : K] = \frac{n}{2}$, which implies that n has to be even, $p(X)$ monic and

$$[K(x^2) : K] = \frac{n}{2} = \left\lfloor \frac{n}{2} \right\rfloor = \deg(p).$$

Therefore $p(X)$ is a monic polynomial in $K[X]$ which as x^2 as a root and of degree $[K(x^2) : K] = \deg(f(x^2, K))$, hence it is $\deg(f(x^2, K))$, the minimal polynomial of x^2 over K.

- If $d(x^2) \neq 0$, then, by Equation (1),

$$x = -\frac{p(x^2)}{d(x^2)} \in K(x^2).$$

Therefore $K(x) \subseteq K(x^2) \subseteq K(x)$ and so $K(x^2) = K(x)$, which means $[K(x) : K(x^2)] = 1$ and, by (2) ,

$$[K(x^2) : K] = \frac{[K(x) : K]}{[K(x) : K(x^2)]} = [K(x) : K] = n = \deg(g).$$

Moreover the leading coefficient of $g(X)$ is

$$\begin{cases} a_n & \text{if } n \text{ is even} \\ -a_n & \text{if } n \text{ is odd} \end{cases} = (-1)^n a_n = (-1)^n.$$

Therefore we have the monic polynomial $(-1)^n g(X) \in K[X]$ that vanishes in x^2, of degree $n = [K(x^2) : K] = \deg(f(x^2, K))$. Hence $(-1)^n g(X) = f(x^2, K)$. ∎

The following lemma can be used, without proof, in the following exercise.

Lemma (Gauss' Lemma)**.** *Let A be a unique factorization domain and K be its fraction field. A non-constant polynomial $f \in A[X]$ is irreducible if and only if it is primitive and irreducible in $K[X]$.*

Exercise 3.3 (Eisenstein's irreducibility criterion)**.** Let $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ be a polynomial of degree $n > 0$. Assume that there exists a prime p such that $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[X]$.

More general version
Let A be a unique factorization domain and K be its fraction field. Let $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ be a polynomial of degree $n > 0$. Assume that there exists a prime element $p \in A$ such that $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $K[X]$.

Exercise 3.4. Let $\zeta \in \mathbb{C}$ be a primitive cubic root of one. Set $E = \mathbb{Q}[\sqrt[3]{2}]$, $F = \mathbb{Q}(\zeta)$ and $L = \mathbb{Q}[i]$.

(i) Prove that $[E : \mathbb{Q}] = 3$ and $[F : \mathbb{Q}] = 2$ and compute the minimal polynomial of ζ over $\mathbb{Q}$ and over L.
(ii) Prove that $EF = \mathbb{Q}(\sqrt[3]{2}, \zeta)$.
(iii) Compute $[EF : \mathbb{Q}]$ and $[E \cap F : \mathbb{Q}]$.

Solution.

(i) We know that $[E:\mathbb{Q}]$ is the same as the degree of the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. Clearly $\sqrt[3]{2}$ is a root of $X^3-2 \in \mathbb{Q}[X]$. Moreover, by Eisenstein's criterion (Exercise 3.3) with $p=2$, we get that X^3-2 is irreducible in $\mathbb{Q}[X]$. Hence $f(\sqrt[3]{2},\mathbb{Q}) = X^3-2$ and $[E:\mathbb{Q}]=3$.

We also know that ξ is a (non-rational) root of $X^3-1=(X-1)(X^2+X+1)$. But X^2+X+1 has no rational roots and it has degree 2, so it is irreducible in $\mathbb{Q}[X]$ and it is the minimal polynomial of ξ over $\mathbb{Q}$. Therefore

$$[F:\mathbb{Q}] = \deg(f(\xi,\mathbb{Q}))\deg(X^2+X+1) = 2.$$

(ii) By definition $EF = \mathbb{Q}(E\cup F)$, which clearly EF contains $\mathbb{Q}$, $\sqrt[3]{2}$ and ξ, so $EF \supseteq \mathbb{Q}(\sqrt[3]{2},\xi)$. Moreover, every element x in $EF=\mathbb{Q}(E\cup F)$ is a $\mathbb{Q}$-linear combination

$$x = \sum_{i=0}^{n} a_i e_i + \sum_{j=0}^{m} b_j f_j,$$

where $a_i, b_j \in \mathbb{Q}$, $e_i \in E$ and $f_j \in F$ for all i,j. In addition, E is a $\mathbb{Q}$-vector space with basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, so for every i,

$$e_i = e_{i,1} + e_{i,2}\sqrt[3]{2} + e_{i,3}\sqrt[3]{4},$$

for some $e_{i,1}, e_{i,2}, e_{i,3} \in \mathbb{Q}$. On the other hand, F is $\mathbb{Q}$-vector space with basis $1, \xi, \xi^2$, so for every j,

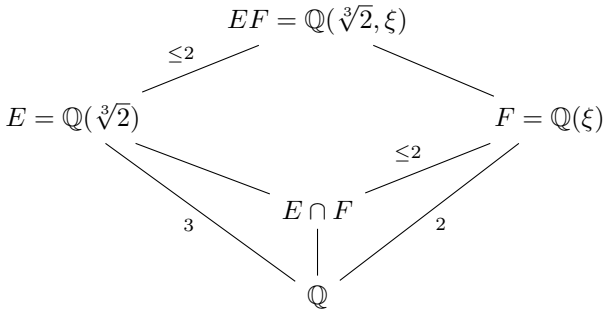
$$f_j = f_{j,1} + f_{j,2}\xi,$$

for some $f_{j,1}, f_{j,2} \in \mathbb{Q}$. Finally,

$$x = \sum_{i=0}^{n} a_i\big(e_{i,1} + e_{i,2}\sqrt[3]{2} + e_{i,3}\sqrt[3]{4}\big) + \sum_{j=0}^{m} b_j\big(f_{j,1} + f_{j,2}\xi\big) \in \mathbb{Q}(\sqrt[3]{2},\xi).$$

Thus we also have the other inclusion $EF \subseteq \mathbb{Q}(\sqrt[3]{2},\xi)$.

(iii) We are in the following situation:



so on the one hand we know that

$$[EF:\mathbb{Q}] = [EF:E][E:\mathbb{Q}] = [EF:E]2$$

and on the other hand, we know that

$$[EF:\mathbb{Q}] = [EF:F][F:\mathbb{Q}] = [EF:F]3 \leq 2\cdot 3 = 6.$$

Therefore 2 and 3 divide $[EF:\mathbb{Q}] \leq 6$. Hence the only possibility is that $[EF:\mathbb{Q}]=6$.

The intersection $E\cap F$ is contained in E, which is contained in $\mathbb{R}$, while $\xi \notin \mathbb{R}$. Therefore $[F:E\cap F] > 1$, since $\xi \in F \setminus E\cap F$ but we also know that $[F:E\cap F] \leq [F:\mathbb{Q}] = 2$. Hence $[F:E\cap F]=2$, which means that $E\cap F = \mathbb{Q}$ and so $[E\cap F:\mathbb{Q}]=1$. ■

Exercise 3.5. Let E/K be a field extension and let L/K and M/K be subextensions.

(i) Prove that $[LM : K] \cdot [L \cap M : K] \leq [L : K] \cdot [M : K]$.
(ii) Can you find examples where $[LM : K] \cdot [L \cap M : K] < [L : K] \cdot [M : K]$?
Hint: Use two different roots of the polynomial $X^3 - 2$.

Solution. (i) Considering the extensions $L/(L \cap M)$, $M/(L \cap M)$, Exercise 2.2 implies that

$$[LM : L \cap M] \leq [L : L \cap M] \cdot [M : L \cap M].$$

Multiplying by $[L \cap M : K]^2$, we get

$$[LM : L \cap M] \cdot [L \cap M : K] \cdot [L \cap M : K] \leq [L : L \cap M] \cdot [L \cap M : K] \cdot [M : L \cap M] \cdot [L \cap M : K]$$
$$\Rightarrow [LM : K] \cdot [L \cap M : K] \leq [L : K] \cdot [M : K].$$

(ii) We consider $\alpha = \sqrt[3]{2}$ and $\beta = \omega\sqrt[3]{2}$, where $\omega \neq 1$ is a primitive root of unity. α and β are different roots of the irreducible polynomial $X^3 - 2$. As $f(\alpha, \mathbb{Q}) = f(\beta, \mathbb{Q}) = 3$, it follows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.
Note that

$$E := \mathbb{Q}(\alpha) \cdot \mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\omega, \sqrt[3]{2}).$$

Expressing $\omega = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, we see that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. On the other hand, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. As $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}) \subseteq E$, it follows that $2, 3$ divide $[E : \mathbb{Q}]$ which implies that 6 divides $[E : \mathbb{Q}]$. On the other hand, as

$$[E : \mathbb{Q}] \leq [\mathbb{Q}(\omega) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6,$$

we infer that $[E : \mathbb{Q}] = 6$. Now considering $\mathbb{Q}(\alpha), \mathbb{Q}(\beta)$, we get $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$ as $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ and $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}]$ must be a proper divisor of $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and therefore be 1.
Putting everything together, we get:

$$[\mathbb{Q}(\alpha)\mathbb{Q}(\beta) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) : \mathbb{Q}] = 6 \cdot 1 < 3 \cdot 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}]. \quad \blacksquare$$

Exercise 3.6. Let E/K be a field extension and let $f \in K[X]$ be a polynomial such that f factorizes in $E[X]$ as $f = \prod_{i=1}^{n}(x - \alpha_i)$. Prove by induction that $[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] \leq n!$.

Solution. For sake of simplicity, we assume that f is monic.
If $n = 1$, then f is a $X - \alpha$ with $\alpha \in K$. In this case, $K(\alpha) = K$ which implies

$$[K(\alpha) : K] = [K : K] = 1 = 1!.$$

Suppose now that the statement has been proven true over each field K' and each polynomial $g \in K'[X]$ with $\deg g = n$. Let now be $f \in K[X]$ with

$$f = \prod_{i=1}^{n+1(X-\alpha_i)}$$

and consider the extension $K(\alpha_{n+1})/K$. As $f(\alpha_{n+1}, K)$ divides f, we see that

$$[K(\alpha_{n+1}) : K] = \deg f(\alpha_{n+1}, K) \leq \deg f = n + 1.$$

Furthermore,

$$g = \prod_{i=1}^{n}(X - \alpha_i) = \frac{f}{X - \alpha_{n+1}} \in K(\alpha_{n+1})[X],$$

because both numerator as denominator are in $K(\alpha_{n+1})[X]$. As $\deg g = n$, the induction hypothesis tells us that

$$[K(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) : K(\alpha_{n+1})] = [K(\alpha_{n+1}(\alpha_1, \alpha_2, \ldots, \alpha_n)) : K(\alpha_{n+1})] \leq n!.$$

And it follows that

$$\begin{aligned}[K(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) : K] &= [K(\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) : K(\alpha_{n+1})] \cdot [K(\alpha_{n+1}) : K] \\ &\leq n! \cdot (n+1) = (n+1)!.\end{aligned}$$

This implies that the statement is also true in case that $\deg f = n + 1$. By the induction principle, the statement is proven in general. ■

4. Week 4

Exercise 4.1. Let K be a field. For a polynomial $f = \sum_{k=0}^{n} a_k X^k \in K[X]$, we define the *derivative* by

$$f' = \sum_{k=1}^{n} k a_k X^{k-1}.$$

(i) Let $\alpha \in K$ and $f, g \in K[X]$. Prove the following properties of the derivative
   (a) $(f+g)' = f' + g'$,
   (b) $(\alpha \cdot f)' = \alpha \cdot f'$,
   (c) $(f \cdot g)' = f' \cdot g + f \cdot g'$.

(ii) Let $f \in K[X]$ be a polynomial that factorizes as $f = \prod_{i=1}^{n}(X - \alpha_i)$. Prove that the roots $\alpha_1, \ldots, \alpha_n$ are pairwise different if and only if $\gcd(f, f') = 1$.

(iii) Let C be an algebraic closure of K and let $f \in K[X]$ be a polynomial with $\deg(f) \geq 1$ that is irreducible over K. Prove that f has repeated roots in C if and only if $f' = 0$. In particular, show that having such a polynomial f implies that $\mathrm{char}(K) = p > 0$ and $f(X) = g(X^p)$ for some irreducible polynomial $g \in K[X]$.

Solution.

(i) For sake of simplicity, write $f = \sum_{k=0}^{\infty} a_k X^k$ and $g = \sum_{k=0}^{\infty} b_k X^k$. Then

$$\begin{aligned}(f+g)' &= \left(\sum_{k=0}^{\infty}(a_k + b_k)X^k\right)' = \sum_{k=1}^{\infty} k(a_k + b_k)X^{k-1} \\ &= \sum_{k=1}^{\infty} k a_k X^{k-1} + \sum_{k=1}^{\infty} k b_k X^{k-1} = f' + g'.\end{aligned}$$

Hence we have proved (a). We can now prove also (b) as:

$$(\alpha \cdot f)' = \left(\sum_{k=0}^{\infty} \alpha a_k X^k\right) = \sum_{k=1}^{\infty} k\alpha a_k X^{k-1} = \alpha \cdot \sum_{k=1}^{\infty} k a_k X^{k-1} = \alpha \cdot f'.$$

To prove (c), we first check the equality for $f = X^k$ and $g = X^l$:

$$(f \cdot g)' = (X^{k+l})' = (k+l)X^{k+l-1} = kX^{k-1}X^l + X^k l X^{l-1} = f' \cdot g + f \cdot g'.$$

Using the already-established K-linearity (i.e. (a) and (b) of this exercise), we can now calculate

$$\begin{aligned}(f \cdot g)' &= \left(\sum_{k,l\geq 0} a_k b_l X^{k+l}\right)' = \sum_{k,l\geq 0} a_k b_l (X^{k+l})' \\ &= \sum_{k,l\geq 0} a_k b_l ((X^k)' X^l + X^k (X^l)') \\ &= \sum_{k,l\geq 0} a_k b_l (X^k)' X^l + \sum_{k,l\geq 0} a_k b_l X^k (X^l)' \\ &= \left(\sum_{k=0}^{\infty} a_k X^k\right) \cdot \left(\sum_{l=0}^{\infty} b_l (X^l)'\right) + \left(\sum_{k=0}^{\infty} a_k (X^k)'\right) \cdot \left(\sum_{l=0}^{\infty} b_l X^l\right) \\ &= f' \cdot g + f \cdot g'.\end{aligned}$$

(ii) Let α_i be one of the roots of f. Write $f = (X - \alpha_i) \cdot g$. By the (i) of this exercise,

$$f' = (X - \alpha_i)' \cdot g + (X - \alpha_i) \cdot g' = g + (X - \alpha_i) \cdot g'.$$

Therefore, $f'(\alpha_i) = g(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$. This implies that $f'(\alpha_i) = 0$ if and only if α_i is a repeated root of f which is the case if and only if $(X - \alpha_i)$ is a common divisor of f and f'.

As the linear factors $(X-\alpha_i)$ are prime elements of $K[X]$, it follows that f and f' have common divisors if and only if f has repeated roots.

(iii) Let f be irreducible in $K[X]$ with repeated roots in $C[X]$. By the previous exercise, $\gcd(f, f') \neq 1$. As f is irreducible and $\gcd(f, f') \in K[X]$, this implies $\gcd(f, f') = f$. Therefore, f divides f'. As $\deg(f') < \deg(f)$, this implies $f' = 0$.

In case that $f' = 0$, we write $f = \sum_{k=0}^{\infty} a_k X^k$ and consider that

$$f' = \sum_{k=1}^{\infty} k a_k X^{k-1} = 0.$$

Therefore, for all $k \geq 0$, we have $k = 0$ or $a_k = 0$. As there is at least one $k \geq 1$ with a_k we conclude that $k = 0$ holds in K for some nonzero k. This implies that $\mathrm{char}(K) = p > 0$ and that $a_k = 0$ whenever $p \nmid k$. We can therefore write

$$f = \sum_{l=0}^{\infty} a_{pl} X^{pl} = g(X^p)$$

with $g = \sum_{l=0}^{\infty} a_{pl} X^l$. For a decomposition $g = g_1 g_2$, we also get a decomposition $f(X) = g(X^p) = g_1(X^p) g_2(X^p)$ which implies that either $g_1(X^p)$ or $g_2(X^p)$ is in K, which amounts to saying that g_1 or g_2 is in K. Therefore, g has to be irreducible. ■

Exercise 4.2. Let L be a finite field.

(i) Show that L is not algebraically closed.
Hint: Consider the polynomial $f(X) = 1 + \prod_{l\in L}(X - l) \in L[X]$.

(ii) Show that L contains a subfield K isomorphic to $\mathbb{Z}/p$ (its ring of integers) and that $|L| = p^m$, where $m = [L : K]$.

Assume now that $K = \mathbb{Z}/p$ and let $f(X) = X^{p^m} - X \in K[X]$. Let C be an algebraic closure of K and set $L = \{\alpha \in C \mid f(\alpha) = 0\}$. Prove that

(iii) $|L| = p^m$
Hint: Use the previous exercise.

(iv) Recall that, since K has characteristic p, $\Phi : K \to K$; $x \mapsto x^p$ is a field endomorphism (the Frobenius endomorphism). Prove that L is a field and $K \subseteq L \subseteq C$.

Solution.

(i) The polynomial $f(X) \in L[X]$ doesn't have roots in L. In fact consider any $a \in L$, then

$$f(a) = 1 + \prod_{l\in L}(a - l) = 1 + (a - a) \prod_{l\in L\setminus\{a\}} (X - l) = 1 + 0 = 1 \neq 0.$$

(ii) Let K be the ring of integers of L. Since L is finite, K is finite too. Hence K is isomorphic to $\mathbb{Z}/p$ for some prime p. L is a vector space of dimension m over $K \cong \mathbb{Z}/p$. Let $\{x_1, x_2, \ldots, x_m\}$ is a basis of L over K, then every element of L can be written in a unique way as a linear combination $\sum_{i=1}^{m} a_i x_i$, with $a_i \in K$. So the number of elements of L is equal to the number of tuples $(a_1, \ldots, a_m) \in K^m$. Hence $|L| = |K|^m = p^m$.

(iii) If $f = X^{p^m} - X$, then $f' = p^m X^{p^m-1} - 1 = -1$. So, $\gcd(f, f') = 1$ and, by the previous exercise, we can conclude that f has p^m pairwise different roots in C, i.e. $|L| = p^m$.

(iv) Using the Frobenius endomorphism Φ of K, we can see that

$$L = \{\alpha \in C \mid \alpha^{p^m} = \alpha\} = \{\alpha \in C \mid \Phi^m(\alpha) = \alpha\}.$$

Since Φ is an endomorphism, Φ^m is also an endomorphism. Then for all $\alpha, \beta \in L$,

$$\Phi^m(\alpha + \beta) = \Phi^m(\alpha) + \Phi^m(\beta) = \alpha + \beta$$
$$\Phi^m(-\alpha) = -\Phi(\alpha) = -\alpha$$
$$\Phi^m(\alpha\beta) = \Phi^m(\alpha)\Phi^m(\beta) = \alpha\beta.$$
$$\Phi^m(\alpha^{-1}) = \big(\Phi^m(\alpha)\big)^{-1} = \alpha^{-1}.$$

So $\alpha + \beta, \alpha, \alpha\beta, \alpha^{-1} \in L$, i.e. L is a field. ■

Exercise 4.3. Let C/K be an algebraic field extension. Show that the following are equivalent:

(i) C is an algebraic closure of K.
(ii) For every algebraic extension L/K there is an extension homomorphism $\varphi \in \mathrm{Hom}(L/K, C/K)$.

Hint: For (i)⇒(ii) use Proposition 3.6 in the notes.

Exercise 4.4. Let $f \in K[X]$ be a polynomial of degree n. Let C be an algebraic closure of K and $A = \{\alpha_1, \dots \alpha_k\} \subseteq C$ be the distinct roots of f in C. We know that $E = K(\alpha_1, \dots, \alpha_k)$ is the decomposition field of f over K.

(i) Prove that $[E : K] \leq n!$.
(ii) Prove that there is an injective homomorphism $\mathrm{Gal}(E/K) \longrightarrow \mathbb{S}_A \cong \mathbb{S}_k$
Hint: Prove that $\sigma(A) = A$ for every $\sigma \in \mathrm{Gal}(E/K)$.
(iii) For $K = \mathbb{Z}/3$ and $f = X^3 - X - 1$, compute $[E : K]$ and $\mathrm{Gal}(E/K)$. (Observe that in this case $[E : K] < n!$.)

Solution. See Exercise 5.2 ■

Exercise 4.5. Let $f = X^4 - 5X^2 + 5 \in \mathbb{Q}[X]$ and E be a decomposition field of f over $\mathbb{Q}$. Prove that $[E : \mathbb{Q}] = 4$.
Hint: Given $\alpha, \beta \in \mathbb{C}$ two solutions of f such that $\beta \neq -\alpha$, compute $\alpha\beta$. Prove also that $E = \mathbb{Q}(\alpha)$.

Solution. See Exercise 5.3 ■

5. Week 5

Exercise 5.1. Let $\xi \in \mathbb{C}$ be a primitive cubic root of one. Prove that the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal and that $\mathbb{Q}(\sqrt[3]{2}, \xi)/\mathbb{Q}$ is normal.

Solution. Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \mathbb{Q}))$. By Proposition 4.10 of the lecture notes we know that $y \in O_G(\sqrt[3]{2})$ if and only if y and $\sqrt[3]{2}$ have the same minimal polynomial over $\mathbb{Q}$. So we need to compute the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.
First of all, note that $\sqrt[3]{2}$ is a root of the polynomial $f(X) = X^3 - 2$.
The roots of f are $\sqrt[3]{2}$, $\sqrt[3]{2}\xi$ and $\sqrt[3]{2}\xi^2$ which are all not in $\mathbb{Q}$. So, being of degree 3 and not having rational roots, f is irreducible over $\mathbb{Q}$.
Thus, by Proposition 4.10,

$$O_G\big(\sqrt[3]{2}\big) = \{\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}, \xi^2\}.$$

This implies that there exists $\sigma \in \mathrm{Hom}(\mathbb{C}/\mathbb{Q}, \mathbb{C}/\mathbb{Q})$ such that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\xi$. But $\sqrt[3]{2}\xi \notin \mathbb{Q}(\sqrt[3]{2})$ because $\sqrt[3]{2}\xi \in \mathbb{C} \setminus \mathbb{R}$ while $\sqrt[3]{2} \in \mathbb{R}$. Hence $\sigma(\mathbb{Q}(\sqrt[3]{2})) \not\subseteq \mathbb{Q}(\sqrt[3]{2})$ and so $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension.
To prove that $\mathbb{Q}(\sqrt[3]{2}, \xi)$ is a normal extension we use Proposition 5.10, so it is enough to prove that $\mathbb{Q}(\sqrt[3]{2}, \xi)$ is the decomposition field of f. We know that the decomposition field E of f over $\mathbb{Q}$ is $\mathbb{Q}$ extended with the roots of f, i.e. $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\xi, \sqrt[3]{2}\xi^2)$. But it's easy to see that actually

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

The inclusion $\subseteq$ is because $\sqrt[3]{2}, \xi = \frac{\sqrt[3]{2}\xi}{\sqrt[3]{2}} \in E$. Vice versa $\supseteq$ is due to the fact that the roots of f are products of $\sqrt[3]{2}$ and ξ, elements in $\mathbb{Q}(\sqrt[3]{2}, \xi)$. ■

Exercise 5.2. Let $f \in K[X]$ be a polynomial of degree n. Let C be an algebraic closure of K and $A = \{\alpha_1, \dots \alpha_k\} \subseteq C$ be the distinct roots of f in C. We know that $E = K(\alpha_1, \dots, \alpha_k)$ is the decomposition field of f over K.

(i) Prove that $[E : K] \leq n!$.
(ii) Prove that there is an injective homomorphism $\mathrm{Gal}(E/K) \longrightarrow \mathbb{S}_A \cong \mathbb{S}_k$
Hint: Prove that $\sigma(A) = A$ for every $\sigma \in \mathrm{Gal}(E/K)$.
(iii) For $K = \mathbb{Z}/3$ and $f = X^3 - X - 1$, compute $[E : K]$ and $\mathrm{Gal}(E/K)$. (Observe that in this case $[E : K] < n!$.)

Solution.

(i) If $n = 0$, the polynomial f is a nonzero constant. Therefore, $A = \emptyset$ and $E = K$. In this case, $[E : K] = [K : K] = 1 = 0!$.
Suppose that we have proven that $[F : L] \leq n!$ whenever F is the decomposition field of a polynomial $g \in L[X]$ with $\deg(g) = n$.
We assume now that $f \in K[X]$ has $\deg(f) = n + 1$. Denote the decomposition field of f over K by E. Let α be a root of f.
As $f(\alpha) = 0$ we know that $f(\alpha, K) | f$. Therefore,

$$[K(\alpha) : K] = \deg(f(\alpha, K)) \leq \deg(f) = n + 1.$$

As $\alpha \in K(\alpha)$, we conclude that $g = \frac{f}{X - \alpha} \in K(\alpha)[X]$. Furthermore, E is the decomposition field of g over K: if A is the set of roots of g, then $A \cup \{\alpha\}$ is the set of roots of f. Therefore, $E = K(A \cup \{\alpha\}) = K(\alpha)(A)$.
As $\deg(g) = n$, we can apply the inductive hypothesis and infer that

$$[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K] \leq (n + 1) \cdot n! = (n + 1)!.$$

(ii) Let $\alpha \in A$ and $\sigma \in \mathrm{Gal}(E/K)$, then

$$f(\sigma(\alpha)) = \overline{\sigma}(f)(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Therefore, $\sigma(\alpha) \in A$. As a consequence, $\sigma(A) = A$ for all $\sigma \in \mathrm{Gal}(E/K)$. Therefore the restriction

$$\begin{aligned} \gamma : \mathrm{Gal}(E/K) &\to \mathbb{S}_A \\ \sigma &\mapsto \sigma|_A \end{aligned}$$

is well-defined and, as the restriction of a group action, indeed a homomorphism. As E is generated by A over K, an automorphism $\sigma \in \mathrm{Gal}(E/K)$ is uniquely determined by its action on A. We conclude that γ is injective.

(iii) Let α be a root of f. As $f = X(X-1)(X+1)-1$, the fact that $\mathrm{char}(K) = 3$ implies that $\alpha + k$ is a root of f for any $k \in \mathbb{Z}/3$. Looking at the degree, this implies that these are in fact all roots of f.

Note that $f(k) = -1$ for all $k \in K$ which implies that f has no roots in K. A reducible polynomial of degree 3 over $K[X]$ always has roots in K, therefore f has to be irreducible.

It follows that $f = f(\alpha, K)$ and $[K(\alpha) : K] = 3$. As all roots of f are $\alpha + k \in K(\alpha)$ for $k \in K$, we conclude that $E = K(\alpha)$. Therefore $[E : K] = 3$.

By the same argument as in the proof of Theorem 4.10, there is for each $k \in K$ a unique $\phi \in \mathrm{Hom}(E/K, E/K)$ with $\phi(\alpha) = \phi(\alpha + k)$. This shows that $\mathrm{Gal}(E/K) \cong \mathbb{Z}/3$. ■

Exercise 5.3. Let $f = X^4 - 5X^2 + 5 \in \mathbb{Q}[X]$ and E be a decomposition field of f over $\mathbb{Q}$. Prove that $[E : \mathbb{Q}] = 4$.
Hint: Given $\alpha, \beta \in \mathbb{C}$ two solutions of f such that $\beta \neq -\alpha$, compute $\alpha\beta$. Prove also that $E = \mathbb{Q}(\alpha)$.

Solution. Note that, since f is an even polynomial if $\alpha \in \mathbb{C}$ is a root of f, then also $-\alpha$ is a root of f. Hence, given two roots $\alpha, \beta \in \mathbb{C}$ such that $\beta \neq -\alpha$, we have that $E = \mathbb{Q}(\alpha, -\alpha, \beta, -\beta)$. But $-\alpha, -\beta \in \mathbb{Q}(\alpha, \beta) \subseteq E$ and so

$$E = \mathbb{Q}(\alpha, -\alpha, \beta, -\beta) \subseteq \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha, -\alpha, \beta, -\beta) = E,$$

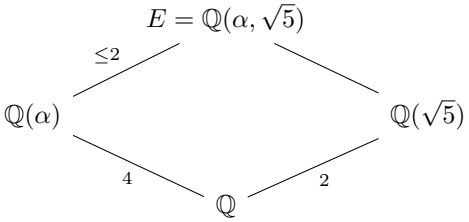
which means that $E = \mathbb{Q}(\alpha, \beta)$. Moreover we can decompose f in $\mathbb{C}[X]$ as

$$(X-\alpha)(X+\alpha)(X-\beta)(X+\beta) = (X^2-\alpha^2)(X^2-\beta^2) = X^4 - (\alpha^2+\beta^2)X^2 + \alpha^2\beta^2.$$

This implies in particular that $\alpha^2\beta^2 = 5$, hence $\beta = \pm\frac{\sqrt{5}}{\alpha} \in \mathbb{Q}(\alpha, \sqrt{5})$. Therefore $E = \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\alpha, \sqrt{5})$. On the other hand $\sqrt{5} = \pm\alpha\beta \in \mathbb{Q}(\alpha, \beta)$, hence $\mathbb{Q}(\alpha, \sqrt{5}) \subseteq \mathbb{Q}(\alpha, \beta) = E$. So we can conclude that $E = \mathbb{Q}(\alpha, \sqrt{5})$. Using the multiplicative of the degree of finite extension we get that

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

But $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial of α over $\mathbb{Q}$. Using Eisenstein criterion with $p = 5$, we have that f is irreducible (and monic), so it is the minimal polynomial of α over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$. It remains to compute $[E : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha, \sqrt{5}) : \mathbb{Q}(\alpha)]$. We have the following situation:



Observe that $\mathbb{Q}(\alpha, \sqrt{5})$ is equal to the composite of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{5})$. We can use the property of composite extension, $[LF : L] \leq [F : K]$, to deduce that

$$[\mathbb{Q}(\alpha, \sqrt{5}) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2.$$

The last equality is because $X^2 - 5$ is the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}$, as it is monic has $\sqrt{5}$ as a root and it's irreducible due to Eisenstein's criterion.

Finally, we want to understand whether $[\mathbb{Q}(\alpha, \sqrt{5}) : \mathbb{Q}(\alpha)]$ is 1 or 2. For this, we need to understand the relation between α and $\sqrt{5}$. Note that $\alpha^4 - 5\alpha^2 + 5 = 0$, so we can solve the equation for α^2 as it is a root of $X^2 - 5X + 5$, i.e.

$$\alpha^2 = \frac{5 \pm \sqrt{25 - 20}}{2} = \frac{5 \pm \sqrt{5}}{2},$$

hence $\sqrt{5} = \pm(2\alpha^2 - 5) \in \mathbb{Q}(\alpha)$. So $\mathbb{Q}(\alpha, \sqrt{5}) \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \sqrt{5})$, which means that $E = \mathbb{Q}(\alpha)$ and $[E : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. ■

Exercise 5.4. Let $\alpha = \sqrt[4]{7} + \sqrt{2} \in \mathbb{C}$

(i) Prove that $\sqrt{2} \in \mathbb{Q}(\alpha)$.
Hint: Use that $(\alpha - \sqrt{2})^4 = 7$ and compute $\sqrt{2}$ depending on α.
(ii) Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{7})$.
(iii) Prove that $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{7})$.
Hint: If $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{7})$, then the extension $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}(\sqrt{2})$ would be a quadratic extension. Therefore, there were $\beta, \gamma \in \mathbb{Q}(\sqrt{2})$ such that

$$\sqrt[4]{7}^2 + \beta\sqrt[4]{7} + \gamma = 0.$$

Produce a contradiction by showing that this would imply $\sqrt{7} \in \mathbb{Q}(\sqrt{2})$.
(iv) Compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$
(v) Prove that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not a normal extension.
Hint: $\sqrt[4]{7}$.

Solution.

(i) Note that $(\alpha - \sqrt{2})^4 - 7 = 0$. By expanding the left side, we get

$$\begin{aligned} 0 &= \alpha^4 - 4\sqrt{2}\alpha^3 + 12\alpha^2 - 8\sqrt{2}\alpha - 3 \\ &= (\alpha^4 + 12\alpha^2 - 3) - (4\alpha^3 + 8\alpha)\sqrt{2}. \end{aligned}$$

$$\rightarrow \quad \sqrt{2} = \frac{\alpha^4 + 12\alpha^2 - 3}{4\alpha^3 + 8\alpha} \in \mathbb{Q}(\sqrt{2}).$$

We are left with checking that $4\alpha^3 + 8\alpha \neq 0$. But this would only be possible for $\alpha \in \{0, \pm i\sqrt{2}\}$ which is not the case.

(ii) From the definition, it is immediate that $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[4]{7})$, therefore $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[4]{7})$.

On the other hand, the first part of the exercise shows that $\sqrt{2} \in \mathbb{Q}(\alpha)$. As $\sqrt[4]{7} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$, we also see that $\sqrt[4]{7} \in \mathbb{Q}(\alpha)$. It follows that $\mathbb{Q}(\sqrt{2}, \sqrt[4]{7}) \subseteq \mathbb{Q}(\alpha)$.

We conclude that $\mathbb{Q}(\sqrt{2}, \sqrt[4]{7}) = \mathbb{Q}(\alpha)$.

(iii) Suppose that $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{7})$. As $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ this would imply that $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}(\sqrt{2})] = 2$. Let therefore $f(\sqrt[4]{7}, \mathbb{Q}(\sqrt{2})) = X^2 + \beta X + \gamma$ with $\beta, \gamma \in \mathbb{Q}(\sqrt{2})$.

Evaluating f at $X = \sqrt[4]{7}$ would lead to $\sqrt{7} + \beta\sqrt[4]{7} + \gamma = 0$, hence

$$\beta^2\sqrt{7} = (-\sqrt{7} - \gamma)^2 = 7 + 2\gamma\sqrt{7} + \gamma^2$$

and so

$$\sqrt{7} = \frac{\gamma^2 + 7}{\beta^2 - 2\gamma} \in \mathbb{Q}(\sqrt{2}).$$

This is a contradiction, as soon as we have justified the last step by excluding $\gamma = \frac{\beta^2}{2}$. But $X^2 + \beta X + \frac{\beta^2}{2} = 0$ holds only for $X = \frac{\beta}{2}(-1 \pm i)$ which is clearly not in $\mathbb{Q}(\sqrt{2})$.

(iv) Recall that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{7})$. As $\sqrt{2} \notin \mathbb{Q}(\sqrt[4]{7})$, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[4]{7})] > 1$. On the other hand, $\sqrt{2}$ is a zero of $X^2 - 2 \in \mathbb{Q}(\sqrt[4]{7})[X]$, therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[4]{7})] \leq 2$, which proves that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[4]{7})] = 2$.

Therefore,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[4]{7})] \cdot [\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(v) We know that $\sqrt[4]{7} \in \mathbb{Q}(\alpha)$ which has minimal polynomial $f(\sqrt[4]{7}, \mathbb{Q}) = X^4 - 7$. One root of this polynomial is $i\sqrt[4]{7} \notin \mathbb{Q}(\alpha)$, therefore $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal. ■

6. Week 6

Exercise 6.1. Let F be a field, we denote by $F^\times$ the group $F \setminus \{0\}$ with the field multiplication. Every finite subgroup of $F^\times$ is a cyclic group.
Prove this statement using the following steps:

(i) Let G be a finite subgroup of $F^\times$. Being an abelian finite group we have that $G \cong \bigoplus_{i=1}^k \mathbb{Z}/p_i^{n_i}$, where p_i are not necessarily distinct primes. Take $m = \operatorname{lcm}(p_i^{n_i} \mid i \in \{1, \dots, k\})$. Prove that $x^m = 1$ for all $x \in G$.
(ii) Prove that $m = \prod_{i=1}^k p_i^{n_i}$.
Hint: Consider the polynomial $X^m - 1$. How many roots does it have?
(iii) Prove that G is cyclic.
Hint: Show that $p_i \neq p_j$ for all $i \neq j$.

Solution. We can assume that $G = \bigoplus_{i=1}^k \mathbb{Z}/p_i^{n_i}$.

(i) For every $x \in G$ we can write it as $x = (x_1, \dots, x_k)$, where $x_i \in \mathbb{Z}/{p_i}^{n_i}$ for every $i \in \{1, \dots, k\}$.. So $x_i^{p_i^{n_i}} = 1$ for every $i \in \{1, \dots, k\}$. Since m is also a multiple of $p_i^{n_i}$, we get that $x_i^m = 1$ for every $i \in \{1, \dots, k\}$. Therefore $x^m = (x_1, \dots, x_k)^m = 1_G$.
(ii) The polynomial $X^m - 1 \in K[X]$ has degree m, so it can have at most m roots. However, the previous point of this exercise shows that every element of G is a root. Thus $\prod_{i=1}^k p_i^{n_i} = |G| \leq m$. On the other hand, clearly $m = \operatorname{lcm}(p_i^{n_i} \mid i \in \{1, \dots, k\}) \leq \prod_{i=1}^k p_i^{n_i}$. Therefore $m = \prod_{i=1}^k p_i^{n_i}$.
(iii) Since we proved that $\operatorname{lcm}(p_i^{n_i} \mid i \in \{1, \dots, k\}) = \prod_{i=1}^k p_i^{n_i}$, we can deduce that $p_i^{n_i}$ and $p_j^{n_j}$ have to be coprime whenever $i \neq j$. Therefore $p_i \neq p_j$ for all $i \neq j$. Moreover, since $G \cong \bigoplus_{i=1}^k \mathbb{Z}/p_i^{n_i}$, we can deduce, using the Chinese remainder theorem, that $G \cong \mathbb{Z}/m$. ∎

Exercise 6.2. If C is an algebraic closure of K, $x \in C$ and $G = \operatorname{Gal}(C/K)$. Prove that the following statements are equivalent:

(i) x is separable over K.
(ii) Every $y \in O_G(x)$ is separable over K.
(iii) $\gamma(K(x)/K) = [K(x) : K] = \deg(f(x, K))$.

Solution. By Proposition 4.11 of the lecture notes, we know that

$$f(x, K) = \prod_{y \in O_G(x)} (X - y)^m$$

for some m. Moreover, by Proposition 4.10 of the lecture notes, $f(y, K) = f(x, K)$ for all $y \in O_G(x)$.

(i) $\iff$ (ii): x is separable over K if and only if x is a simple root of f, i.e. $m = 1$. Thus x is separable over K if and only if y is separable over K for all $y \in O_G(x)$.
(i) $\iff$ (iii): We know already that $[K(x) : K] = \deg(f(x, K))$. By Proposition 5.16 of the lecture notes, we also have that $\gamma(K(x)/K) = |O_G(x)|$. Thus

$$[K(x) : K] = \deg(f(x, K)) = m|O_G(x)| = \gamma(K(x)/K).$$

But x is separable over K if and only if $m = 1$, i.e.

$$[K(x) : K] = \deg(f(x, K)) = |O_G(x)| = \gamma(K(x)/K).$$ ∎

Recall the following property.

Proposition 1. *Let K be a field and C an algebraic closure of K. If a polynomial $f \in K[X]$ is irreducible and has repeated roots in C, then K has positive characteristic $p > 0$ and $f = g(X^p)$ for an irreducible polynomial $g \in K[X]$.*

Exercise 6.3. Let K be a field of positive characteristic p and let $K(t)$ be the field of rational functions over K. Prove that the extension $K(t)/K(t^p)$ is inseparable.
Hint: Use the Eisenstein criterion to prove that the polynomial $X^p - t^p$ is irreducible in $K(t^p)[X]$.

Solution. It is clear that $K(t^p)(t) = K(t)$ and that t is a root of the polynomial $f = X^p - t^p \in K(t^p)[X]$. We have to prove that $f = f(t, K(t^p))$ by showing that it is irreducible in $K(t^p)[X]$.
$K(t^p)$ is the field of fractions of the factorization domain $K[t^p]$ which we can identify with the ring $K[Y]$ by substituting $Y = t^p$. We apply Eisenstein with the prime $Y \in K[Y]$ to the monic polynomial $f = X^p - Y$: $Y | a_i$ for $i < p$ and $Y^2 \nmid Y = a_0$, hence f is irreducible in $K[Y, X]$ and, thus, also in $K(Y)[X] = K(t^p)[X]$.
Note that $f = X^p - t^p = (X - t)^p$ which implies that t is a repeated root of $f = f(t, K(t^p))$. This proves that $K(t)/K(t^p)$ is an inseparable extension. ■

Exercise 6.4. Let K be a field. Prove the equivalence of the following two statements:

(1) Each algebraic extension of K is separable.
(2) *Either* K has characteristic 0, *or* K has positive characteristic $p > 0$ and the Frobenius endomorphism $\Phi_K : K \to K$; $\Phi_K(x) = x^p$ is bijective.

Hint: The first statement is equivalent to the statement that each irreducible polynomial in $K[X]$ doesn't have repeated roots in an algebraic closure. Use the proposition to reduce the problem to the case that K has positive characteristic p.
In this case, use the fact that $(K[X])^p = \Phi_K(K)[X^p]$ to show that if $\Phi_K(K) = K$ then there are no irreducible polynomials of the form $g(X^p)$ in $K[X]$. On the other hand, if $\Phi_K(K) \neq K$, let $b \in K \setminus \Phi_K(K)$ and prove that the polynomial $X^p - b$ is irreducible in $K[X]$.

Solution. We have to show that K can only have inseparable extensions if and only if K has positive characteristic p and Φ_K isn't surjective.
The existence of inseparable extensions of K implies that there is an element $\alpha \in L$ for some extension L/K such that $f(\alpha, K)$ has repeated roots. We know that this is only possible if K has positive characteristic p and $f(\alpha, K) = g(X^p)$ for some irreducible polynomial $g \in K[X]$. Suppose that Φ_K is bijective and write

$$g = \sum_{i=0}^{n} a_i X^i$$

for some $a_i \in K$. Then

$$f = g(X^p) = \sum_{i=0}^{n} a_i X^{i \cdot p} = \sum_{i=0}^{n} (\Phi_K^{-1}(a_i))^p X^{i \cdot p} = \left(\underbrace{\Phi_K^{-1}(a_i)}_{=b_i} X^i \right)^p .$$

As all $b_i \in K$, this shows that f cannot be irreducible. Therefore, we have proven that inseparable extensions of K can only exist if Φ_K isn't bijective.
Suppose now that K has positive characteristic p and Φ_K isn't bijective. As a homomorphism of fields, Φ_K is always injective, therefore it is not surjective. Suppose that $a \notin \operatorname{im} \Phi_K$. This means that a is not a p-th power. Let α be a root of f in an algebraic closure $\overline{K}/K$. We claim that the extension $K(\alpha)/K$ is inseparable. As $\alpha^p = a$, we see that

$$f(\alpha, K) | X^p - a = X^p - \alpha^p = (X - \alpha)^p \Rightarrow f(\alpha, K) = (X - \alpha)^k \text{ for some } 2 \leq k \leq p.$$

Note that $\alpha \notin K$ as a is not a p-th power in K, so indeed $k \geq 2$. But this implies that α is a repeated root of $f(\alpha, K)$, so L/K is inseparable. ■

7. Week 7

Exercise 7.1. Let K be a field of characteristic different from 2.

(1) Let E/K be an extension of degree $[E:K]=2$, prove that E/K is Galois.
(2) Find a counterexample in characteristic 2.
Hint: Consider the field $E=\mathbb{Z}/2(X)$.

Solution.

(1) First of all, since the extension is finite we know that E/K is also algebraic. Let now $\alpha \in E \setminus K$. Then
$$1 < \deg(f(\alpha,K)) = [K(\alpha)] \leq [E:K] = 2,$$
so $\deg(f(\alpha,K))=2$. In particular, since $\alpha \in E$ is a root of $f(\alpha,K)$, a polynomial of degree 2, we deduce that $f(\alpha,K)$ decomposes linearly in $E[X]$. Hence E is a decomposition field of $f=f(\alpha,K)$. Moreover, we can write $f=X^2+aX+b$ for some $a,b\in K$. Hence $f'=2X+a$ is non-zero because K has characteristics different from 2, thus f is a separable polynomial (by the derivative criterion). Another way to prove the separability of f is that otherwise K would have characteristic $p>0$ and $f \neq g(X^p)$ for some $g\in K[X]$, a contradiction with $\deg(f)=2\neq p$. Therefore E is a decomposition field of $f(\alpha,K)$, which is a separable polynomial, i.e. E/K is Galois.
(2) Consider $E=\mathbb{Z}/2(X)$ and $K=\mathbb{Z}/2(X^2)$.
We can re-write E also as $E=K(X)$, so $[E:K]=\deg(f(X,K))$. Since the polynomial $Y^2-X^2\in K[Y]$ has X as a root in E, we know that $[E:K]\leq 2$. Moreover $\{1,X\}$ is a generating set of E as a K-vector space. On the other hand, $X\notin K$, otherwise $X=\frac{f(X^2)}{g(X^2)}$, for some polynomials $f,g\neq 0$ with coefficients in $\mathbb{Z}/2$. Thus X would satisfy $Xg(X^2)=f(X^2)$, but the degree as polynomials in X would be odd for $\deg(Xg(X^2))$ and even for $f(X^2)$, a contradiction. Therefore $[E:K]>1$, i.e. $[E:K]=2$. Moreover $\deg(f(X,K))[E:K]=2$, so $f(X,K)=Y^2-X^2$.
Finally, we prove that E/K is not a Galois extension, proving that it is not separable. In fact, the element $X\in E$ is not separable as its minimal polynomial is $f(X,K)=Y^2-X^2=(Y-X)^2\in E[Y]$, so X is a multiple root of it. ∎

Exercise 7.2. Let E/K be a separable extension and L/K be the normal closure of E in an algebraic closure C of K. Prove that L/K is a Galois extension.

Solution. Recall that, if $E=K(S)$ for a subset $S\subseteq E$ and C is an algebraic closure of K, the definition of L is $L=K(T)$, where
$$T=\{y\in C \mid y \text{ is a root of } f(x,K) \text{ for } x\in S\}$$
We know already that L/K is normal. Since for an extension being Galois is equivalent to being normal and separable, we are left to prove that L/K is separable. Moreover, to prove that L/K is separable it is enough to prove that every element in T is separable over K. So let $y\in T$, i.e. y is a root of $f(x,K)$ for some $x\in S$. But then $f(y,K)=f(x,K)$. We also know that $f(x,K)=\prod_{y\in O_G(x)}(X-y)^m$, but $x\in E$, so it is separable, hence $f(x,K)$ is also separable and therefore y is separable. ∎

Exercise 7.3. Let K be a field of characteristic $p>0$ and let L be an algebraic extension.

(i) Prove that for every $\alpha\in L$, there is an $n\in\mathbb{Z}_{\geq 0}$ such that α^{p^n} is separable.
Hint: Write $f(\alpha,K)=g(X^{p^n})$ with n as large as possible.

(ii) Recall that a field extension L/K is *purely inseparable* if and only if $f(\alpha, K)$ is not separable for all $\alpha \in L \setminus K$. Prove that assuming that L/K is finite, then it is purely inseparable if and only if $L^{p^\infty} = \bigcap_{n\geq 0} L^{p^n} \subseteq K$.

(iii) Let $M = KL^{p^\infty}$ and assume that L/K is finite. Prove that M/K is separable and L/M is purely inseparable.

Solution.

(i) Let $\alpha \in L$, and let $f = f(\alpha, K)$ be its minimal polynomial. We can write $f(\alpha, K) = g(X^{p^n})$ with n as large as possible. Moreover, g is irreducible (otherwise $f(\alpha, K)$ would be reducible, a contradiction) and, for the maximality of n, it is not of the form $h(X^p)$ for $h \in K[X]$. Therefore $g \in K[X]$ is a separable polynomial. But $g(\alpha^{p^n}) = 0$, so $g = f(\alpha^{p^n}, K)$ and α^{p^n} is a separable element over K.

(ii) Let L/K be a finite purely inseparable extension. Observe that the n found in the previous part of the exercise is bounded by $[L : K]$. Thus there exists $n \in \mathbb{N}$ such that α^{p^n} is separable for all $\alpha \in L$, hence $\alpha^{p^n} \in K$ (since L/K is purely inseparable). Thus $L^{p^n} \subseteq K$ and so $L^{p^\infty} \subseteq K$.

Vice versa assume that $L^{p^\infty} \subseteq K$. We want to prove that L/K is purely inseparable. Let $\alpha \in L \setminus K$. Then there is an $n \in \mathbb{N}$ such that $\beta = \alpha^{p^n} \in L^{p^\infty} \subseteq K$. So α is a root of $X^{p^n} - \beta \in K[X]$, hence $f(\alpha, K)$ divides $X^{p^n} - \beta$ in $K[X]$. But $X^{p^n} - \beta = (X - \alpha)^{p^n}$ in $C[X]$, for C an algebraic closure of K. Thus $f(\alpha, K) = (X - \alpha)^d$ for some $d \in \mathbb{N}$ and since $\alpha \notin K$ we have that $d > 1$. Therefore $f(\alpha, K)$ is not separable over K.

(iii) Since L/K is finite, there exists $n \in \mathbb{N}$ such that all elements in L^{p^n} are separable over K. Therefore all $\alpha \in L^{p^\infty}$ are separable over K, hence M/K is separable.

We know that $L^{p^\infty} \subseteq M$, so by the previous part of the exercise, we know that L/M is purely inseparable. ■

Exercise 7.4.

(i) Let L/K be a finite Galois extension and let M/K be a subextension. For $\sigma \in \mathrm{Gal}(L/K)$ prove that $\mathrm{Gal}({}^\sigma M/K) = {}^\sigma \mathrm{Gal}(M/K)$, where the latter upperscript-σ denotes conjugation by σ in $\mathrm{Gal}(L/K)$.

(ii) Let E/K be a finite Galois extension and $F_1, \dots, F_n$ fields such that $K \subseteq F_i \subseteq E$ for all $i \in \{1, \dots, n\}$. For every i let $S_i = \mathrm{Gal}(E/F_i)$. Then

$$\mathrm{Gal}\left(E/\bigcap_{i=1}^n F_i\right) = \left\langle \bigcup_{i=1}^n S_i \right\rangle, \quad \mathrm{Gal}\left(E/\prod_{i=1}^n F_i\right) = \bigcap_{i=1}^n S_i.$$

Hint: Determine the subfield fixed by $\langle \bigcup_{i=1}^n S_i \rangle$ and the subgroup of $\mathrm{Gal}(E/K)$ that fixes $\prod_{i=1}^n F_i$.

Solution. See Exercise 8.1. ■

Exercise 7.5. For infinite extensions, the Galois correspondence is not always true (more precisely β is not always injective).
Let $p_1, p_2, \dots$ be the ordered list of prime numbers, let $S_k = \{\sqrt{p_i} \mid 1 \leq i \leq k\}$ and $S = \cup_{k\in\mathbb{N}} S_k$. Consider the field extensions $E_k = \mathbb{Q}(S_k)$ and $E = \mathbb{Q}(S)$, let $G = \mathrm{Gal}(E/\mathbb{Q})$ and for every $\sigma \in G$ denote $m(\sigma) = \{x \in P \mid \sigma(x) \neq x\}$.
Let $H = \{\sigma \in G \mid m(\sigma) \text{ is finite}\}$.

(i) Prove by induction on k that $\sqrt{m} \notin E_k$ for every $m \in \mathbb{N}$ such that $\gcd(m, p_i) = 1$ for all $1 \leq i \leq k$.

(ii) H is a proper subgroup of G.

(iii) ${}^H E = \mathbb{Q}$.

Solution. See Exercise 8.2. ■

8. Week 8

Exercise 8.1.

(i) Let L/K be a finite Galois extension and let M/K be a subextension. For $\sigma \in \mathrm{Gal}(L/K)$ prove that $\mathrm{Gal}(\sigma(M)/K) = \sigma \,\mathrm{Gal}(M/K)\sigma^{-1}$.

(ii) Let E/K be a finite Galois extension and $F_1, \dots, F_n$ fields such that $K \subseteq F_i \subseteq E$ for all $i \in \{1, \dots, n\}$. For every i let $S_i = \mathrm{Gal}(E/F_i)$. Then

$$\mathrm{Gal}\left(E/\bigcap_{i=1}^{n} F_i\right) = \left\langle \bigcup_{i=1}^{n} S_i \right\rangle, \quad \mathrm{Gal}\left(E/\prod_{i=1}^{n} F_i\right) = \bigcap_{i=1}^{n} S_i.$$

Hint: Determine the subfield fixed by $\langle \bigcup_{i=1}^{n} S_i \rangle$ and the subgroup of $\mathrm{Gal}(E/K)$ that fixes $\prod_{i=1}^{n} F_i$.

Solution.

(i) By definition an element in $\mathrm{Gal}(\sigma(M)/K)$ is a field automorphism $\varphi : \sigma(M) \to \sigma(M)$ such that $\varphi|_K = id$. Given $\psi \in \mathrm{Gal}(M/K)$, then $\sigma\psi\sigma^{-1}$ is bijective and $\sigma\psi\sigma^{-1}(\sigma(M)) = \sigma(M)$, so $\sigma\psi\sigma^{-1} \in \mathrm{Gal}(\sigma(M)/K)$. On the other hand, if $\varphi \in \mathrm{Gal}(\sigma(M)/K)$, then $\varphi = \sigma\psi\sigma^{-1}$, where $\psi = \sigma^{-1}\varphi\sigma \in \mathrm{Gal}(M/K)$.

(ii) Let $S = \langle \bigcup_{i=1}^{n} S_i \rangle$, we want to prove that $\bigcap_{i=1}^{n} F_i = {}^{S}L$.

($\subseteq$) let $x \in \bigcap_{i=1}^{n} F_i$. For every $\varphi \in \bigcup_{i=1}^{n} S_i$, there is $j \in \{1, \dots, n\}$ such that $\varphi \in S_j = \mathrm{Gal}(E/F_j)$, so $\varphi(x) = x$ since $x \in \bigcap_{i=1}^{n} F_i \subseteq F_j$. Hence $\varphi(x) = x$ also for every $\varphi \in S = \langle \bigcup_{i=1}^{n} S_i \rangle$.

($\supseteq$) Vice versa, $S_i \leq S$, for every $i \in \{1 \dots, n\}$. So, since the Galois correspondence reverses inclusions, ${}^{S_i}E \supseteq {}^{S}E$. But, by the correspondence, we also know that ${}^{S_i}E = F_i$. Therefore $F_i \supseteq {}^{H}E$ for all $i \in \{1, \dots, n\}$, hence $\bigcap_{i=1}^{n} F_i \supseteq {}^{S}E$.

So we proved that $\bigcap_{i=1}^{n} F_i = {}^{S}E$, so, using again the Galois correspondence, we get that

$$\mathrm{Gal}\left(E/\bigcap_{i=1}^{n} F_i\right) = \mathrm{Gal}\left(E/{}^{H}E\right) = S = \left\langle \bigcup_{i=1}^{n} S_i \right\rangle.$$

Let $F = \prod_{i=1}^{n} F_i$, we want to prove that $\mathrm{Gal}(E/F) = \bigcap_{i=1}^{n} S_i$.

($\subseteq$) Let $\sigma \in \mathrm{Gal}(E/F)$, then $\sigma|_{F_i} = id$ for all i, so $\sigma \in \mathrm{Gal}(E/F_i) = S_i$ for all i. Therefore $\bigcap_{i=1}^{n} S_i \supseteq \mathrm{Gal}(E/F)$.

($\supseteq$) Since $F_i \subseteq \prod_{i=1}^{n} F_i = F$ for all i, then $S_i = \mathrm{Gal}(E/F_i) \geq \mathrm{Gal}(E/F)$ for all i. So $\bigcap_{i=1}^{n} S_i \subseteq \mathrm{Gal}(E/F)$. ∎

Exercise 8.2. For infinite extensions, the Galois correspondence is not always true (more precisely β is not always injective).
Let $p_1, p_2, \dots$ be the ordered list of prime numbers, let $S_k = \{\sqrt{p_i} \mid 1 \leq i \leq k\}$ and $S = \cup_{k \in \mathbb{N}} S_k$. Consider the field extensions $E_k = \mathbb{Q}(S_k)$ and $E = \mathbb{Q}(S)$, let $G = \mathrm{Gal}(E/\mathbb{Q})$ and for every $\sigma \in G$ denote $m(\sigma) = \{x \in S \mid \sigma(x) \neq x\}$.
Let $H = \{\sigma \in G \mid m(\sigma) \text{ is finite}\}$. Prove that

(i) For every n such that $\gcd(n, p_i) = 1$ for all $1 \leq i \leq k$, we have $\sqrt{n} \notin E_k$.
Hint: Use induction on k.

(ii) H is a proper subgroup of G.

(iii) ${}^{H}E = \mathbb{Q}$.

Solution.

(i) If $k = 1$, $E_k = \mathbb{Q}(\sqrt{p_1})$ and if $\sqrt{n} \in E_k$, then we can write $\sqrt{n} = a + b\sqrt{p_1}$, for some $a, b \in \mathbb{Q}$. So $n = a^2 + b^2 p_1 + 2ab\sqrt{p_1}$ which would imply that $\sqrt{p_1} \in \mathbb{Q}$, which is not the case.

Assume now that the thesis is true for $k \geq 1$ and consider integer n coprime with every p_i for $1 \leq i \leq k+1$. By inductive hypothesis, we know that $p_{k+1} \notin E_k$, so $E_{k+1} = E_k(\sqrt{p_{k+1}})$ is an extension of degree 2 of E_k. If $\sqrt{n} \in E_{k+1}$, then we can write $\sqrt{n} = a + b\sqrt{p_{k+1}}$, for some $a, b \in E_k$. So $n = a^2 + b^2 p_1 + 2ab\sqrt{p_{k+1}}$ which would imply that $\sqrt{p_{k+1}} \in E_k$, which is not the case. Therefore, we have the thesis.

(ii) To prove that H is a proper subgroup we can show that there is an element σ in G such that $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$ for all $i \geq 1$. In order to construct this element σ we can proceed again by induction showing that there is $\sigma_k \in \mathrm{Hom}(E_k/\mathbb{Q}, E_k/\mathbb{Q})$ such that $\sigma_k(\sqrt{p_i}) = -\sqrt{p_i}$ for all $1 \leq i \leq k$.

If $k = 1$ this is clear. Let now $k \geq 1$. By the previous part of the exercise $E_{k+1} = E_k(\sqrt{p_k})$ is an extension of degree 2 of E_k. Hence, given σ_k, we know that there exists an extension σ_{k+1} of σ_k to $\mathrm{Hom}(E_{k+1}/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma_{k+1}(\sqrt{p_{k+1}}) = -\sqrt{p_{k+1}}$. So we can construct the desired $\sigma \in G \setminus H$.

(iii) Obviously $\mathbb{Q} \subseteq {}^H E$. On the other hand, let $x \in {}^H E$. In particular $x \in E = \mathbb{Q}(S)$, but x can be written as a finite $\mathbb{Q}$-combination of elements in S. If we assume that $x \notin \mathbb{Q}$ then there exists a positive integer k such that $x \in E_k \setminus E_{k-1}$. Thanks to the first part of this exercise, can then consider the homomorphism $\tau : E_k \to E_k$ that extends the identity of E_k and such that $\tau(\sqrt{p_k}) = -\sqrt{p_k}$. Clearly, this extends again to an element of G such that

$$\overline{\tau}\left(\sqrt{p_j}\right) = \begin{cases} \sqrt{p_j} & \text{if } j \neq k \\ -\sqrt{p_i} & \text{if } j = k \end{cases}.$$

But actually $\overline{\tau} \in H$, so $\tau(x) = x$, which implies that $x \in E_{k-1}$, a contradiction. ■

Exercise 8.3. Let $n \geq 1$ and let $\mathbb{S}_n$ be the symmetric group over $\{1, 2, \ldots, n\}$. For $1 \leq i \leq n$, define the subgroups

$$S_i = \{\pi \in \mathbb{S}_n : \pi(i) = i\}.$$

(i) For $\pi \in \mathbb{S}_n$, and $1 \leq i \leq n$ prove that $S_{\pi(i)} = \pi S_i \pi^{-1}$. Show also that

$$\bigcap_{\pi \in \mathbb{S}_n} \pi S_1 \pi^{-1} = \{\mathrm{id}\}.$$

(ii) Let L/K be a finite Galois extension with $\mathrm{Gal}(L/K) \cong \mathbb{S}_n$. Prove that there is an intermediate extension E/K with $[E : K] = n$ and $\prod_{\pi \in \mathbb{S}_n} \pi(E) = L$.

(iii) Let L/K and E/K be as in the previous item. There is an element $x \in E$ such that $E = K(x)$. Let $f = f(x, K)$ be its minimal polynomial. Prove that L is the decomposition field of f over K. In particular, every $\mathbb{S}_n$-extension of K is the decomposition field of a polynomial of degree n over K.

Solution. See Exercise 9.1. ■

Exercise 8.4. Let p be a prime and let L be a field with p^n elements. We know that L contains $K = \mathbb{Z}/p$.

(i) Prove that every element in L is a root of the polynomial $X^{p^n} - X$. Deduce that L is separable over K and that the Frobenius endomorphism $\Phi(x) = x^p$ is an automorphism.

(ii) Recall that L^* is a cyclic group of order $p^n - 1$. Show that

$$\mathrm{Gal}(L/K) = \{\Phi^i : 0 \leq i \leq n-1\} \cong C_n.$$

(iii) Let $|L| = p^6$. Use the previous exercise to count the number of elements $x \in L$ with $K(x) = L$.
Hint: Use the Galois correspondence to determine the number of elements that are not contained in a proper subfield of L.

Solution. See Exercise 9.2. ■

9. Week 9

Exercise 9.1. Let $n \geq 1$ and let $\mathbb{S}_n$ be the symmetric group over $\{1, 2, \ldots, n\}$. For $1 \leq i \leq n$, define the subgroups

$$S_i = \{\pi \in \mathbb{S}_n : \pi(i) = i\}.$$

(i) For $\pi \in \mathbb{S}_n$, and $1 \leq i \leq n$ prove that $S_{\pi(i)} = \pi S_i \pi^{-1}$. Show also that

$$\bigcap_{\pi \in \mathbb{S}_n} \pi S_1 \pi^{-1} = \{\mathrm{id}\}.$$

(ii) Let L/K be a finite Galois extension with $\mathrm{Gal}(L/K) \cong \mathbb{S}_n$. Prove that there is an intermediate extension E/K with $[E : K] = n$ and $\prod_{\pi \in \mathbb{S}_n} \pi(E) = L$.

(iii) Let L/K and E/K be as in the previous item. There is an element $x \in E$ such that $E = K(x)$. Let $f = f(x, K)$ be its minimal polynomial. Prove that L is the decomposition field of f over K. In particular, every $\mathbb{S}_n$-extension of K is the decomposition field of a polynomial of degree n over K.

Solution. We calculate

$$\begin{aligned} S_i &= \{\rho \in \mathbb{S}_n : \rho(i) = i\} \\ &= \{\rho \in \mathbb{S}_n : (\rho\pi^{-1})(i) = \pi^{-1}(i)\} \\ &= \{\rho \in \mathbb{S}_n : (\pi\rho\pi^{-1})(i) = i\}. \end{aligned}$$

This shows that $\pi S_i \pi^{-1} = S_{\pi(i)}$. Using this, we see that

$$\bigcap_{\pi \in \mathbb{S}_n} \pi S_1 \pi^{-1} = \bigcap_{\pi \in \mathbb{S}_n} S_{\pi(1)} = \bigcap_{i=1}^{n} S_i = \{\rho \in \mathbb{S}_n : \forall 1 \leq i \leq n : \rho(i) = i\} = \{\mathrm{id}\}.$$

It is easy to see that $S_1 \cong \mathbb{S}_{n-1}$, therefore $|S_1| = (n-1)!$ and $[\mathbb{S}_n : S_1] = n$.

Combining this knowledge with that gained from the previous exercise, we see that $\mathrm{Gal}(L/K)$ contains a subgroup H with $[\mathrm{Gal}(L/K) : H] = n$ and $\bigcap_{\pi \in \mathrm{Gal}(L/K)} \pi H \pi^{-1} = 1$. Let $E = {}^{H}L$ be the corresponding intermediate field. By the Galois correspondence, we see that

$$[E : K] = [\mathrm{Gal}(L/K) : H] = n$$

and

$$\mathrm{Gal}\left(L/\prod_{\pi \in \mathrm{Gal}(L/K)} \pi(E)\right) = \bigcap_{\pi \in \mathbb{S}_n} \pi \,\mathrm{Gal}(L/E)\pi^{-1} = \bigcap_{\pi \in \mathbb{S}_n} \pi H \pi^{-1} = 1.$$

This implies $\prod_{\pi \in \mathrm{Gal}(L/K)} \pi(E) = L$.

(ii) We know that $\mathcal{O}_{\mathrm{Gal}(L/K)}(x)$ is the set of roots of $f(x, K)$. If $y = \pi(x) \in \mathcal{O}_{\mathrm{Gal}(L/K)}(x)$, then $K(y) = \pi(K(x))$. Let M be the decomposition field of f, then

$$\begin{aligned} M &= K\left(y : y \in \mathcal{O}_{\mathrm{Gal}(L/K)}(x)\right) \\ &= \prod_{y \in \mathcal{O}_{\mathrm{Gal}(L/K)}(x)} K(y) \\ &= \prod_{\pi \in \mathrm{Gal}(L/K)} \pi(K(x)) \\ &= \prod_{\pi \in \mathrm{Gal}(L/K)} \pi(E) = L. \end{aligned}$$

■

Exercise 9.2. Let L/K be an extension of finite fields where $|K| = q$ and $[L : K] = n$.

(i) Let $\sigma(x) = x^q$ be the Frobenius automorphism. Prove that σ has order n and that $\mathrm{Gal}(L/K) = \langle\sigma\rangle \cong C_n$.

(ii) Let $n \in \{3, 4, 6\}$. Count the number of elements $x \in L$ with $K(x) = L$. What does this tell you about the number of irreducible polynomials $f \in K[X]$ with $\deg f = n$?
Hint: Use the Galois correspondence to determine the number of elements that are not contained in a proper subfield of L.

Solution. (i) We already know that σ is an automorphism. We show that σ has exactly order n:

Note that $|L| = |K|^{[L:K]} = q^n$. By Lagrange's theorem, we see that for all $x \in L^\times$,

$$1 = x^{|L^\times|} = x^{q^n-1} \Rightarrow x = x \cdot x^{q^n-1} = x^{q^n} = \sigma^n(x)$$

which shows $\sigma^n = \mathrm{id}_L$.

$L^\times$ is a cyclic group, therefore $L^\times \cong C_{q^n-1} = \langle x\rangle$ for some $x \in L^\times$ with $o(x) = q^n - 1$. For $0 < i < p$, we see that for such an x,

$$\sigma^i(x) = x^{q^i} \neq x$$

because $1 < q^i < q^n - 1$. Therefore $\sigma^i \neq \mathrm{id}_L$ for $0 < i < n$ which proves that $o(\sigma) = n$. Therefore,

$$n = |\langle\sigma\rangle| \leq |\mathrm{Gal}(L/K)| \leq [L : K] = n.$$

This shows that $\mathrm{Gal}(L/K) = \langle\sigma\rangle \cong C_n$. Furthermore, as the inequalities force the equality $|\mathrm{Gal}(L/K)| = [L : K]$, we conclude that L/K is a Galois extension.

(ii) Note that a cyclic group C_n has a unique subgroup of index d for each positive $d|n$. By the Galois correspondence, this shows that L/K has a unique intermediate extension L_d/K for any $d|[L : K] = n$. Observe that $L_n = L$ and $L_1 = K$.

We first determine the number of elements in L that are not contained in any intermediate field of L/K:

$n = 3$: We have to calculate $|L_3 \setminus L_1| = q^3 - q^1 = q^3 - q$.

$n = 4$: Note that $L_1 \subseteq L_2$, therefore the desired quantity is

$$|L_4 \setminus L_2| = q^4 - q^2.$$

$n = 6$: We first determine

$$|L_2 \cup L_3| = |L_3| + |L_2| - |L_2 \cap L_3| = |L_3| + |L_2| - |L_1| = q^2 + q^3 - q.$$

As $L_1 \subseteq L_2, L_3$, the number of elements not contained in any intermediate fields is given by

$$|L_6 \setminus (L_2 \cup L_3)| = q^6 - q^3 - q^2 + q.$$

We know that each root α of an irreducible polynomial $f \in K[X]$ with $\deg f = n$ generates an extension M/K with $[M : K] = n$ and therefore satisfies $\alpha^{q^n} = \alpha$. It follows that $f|X^{q^n} - X$.

As $X^{q^n} - X$ has q^n distinct roots in L, we conclude that each irreducible polynomial f has n distinct roots in M. These roots can not lie in a proper intermediate field of L/K. On the other hand, each $\alpha \in L$ that does not lie in a proper intermediate field of L/K, satisfies $K(\alpha) = L$ and therefore $\deg f(\alpha, K) = [L : K] = n$.

Therefore, the number $\mathcal{P}_{q,n}$ of irreducible (monic) $f \in K[X]$ with $\deg f = n$ is $\mathcal{P}_{q,n} = \frac{\mathcal{A}_{q,n}}{n}$ where we denote by $\mathcal{A}_{q,n}$ the number of elements in an extension L/K with $[L:K]$ that are not in a proper intermediate field. We conclude that the number of irreducible monic polynomials in the considered cases is

$$\mathcal{P}_{q,3} = \frac{q^3 - q}{3},$$
$$\mathcal{P}_{q,4} = \frac{q^4 - q^2}{4},$$
$$\mathcal{P}_{q,6} = \frac{q^6 - q^3 - q^2 + q}{6}.$$

Remark: For $|K| = q$, the general formula for the number of irreducible monic polynomials $f \in K[X]$ with $\deg f = n$ is

$$\mathcal{P}_{q,n} = \frac{\sum_{d|n} \mu(n/d) q^d}{n}$$

where μ is the *Moebius function*.

■

Exercise 9.3. Give an explicit description of $\mathrm{norm}_{L/K}$ and $\mathrm{trace}_{L/K}$ for the following field extensions:

(i) $\mathbb{C}/\mathbb{R}$,

(ii) $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, d squarefree,

(iii) $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$

Hint: Represent an element of $\mathbb{Q}[\sqrt[3]{2}]$ as $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, argue that

$$\mathrm{norm}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(x) = (a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot (a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}) \cdot (a + b\xi^2\sqrt[3]{2} + c\xi\sqrt[3]{4})$$

where $\xi \neq 1$ is a third root of unity. Multiplying this out would give you 27 summands - you only need those which do not contain a rational power of $\sqrt[3]{2}$ (why?). Then sum everything up by using the fact that $\xi + \xi^2 = -1$.

(iv) $K(t)/K(t^p)$, where $\mathrm{char}\ K = p > 0$.

Solution. See Exercise 10.3. ■

Exercise 9.4.

(i) Let L/K be a finite extension of fields. Prove that $\mathrm{trace}_{L/K} \neq 0$ if and only if L/K is separable.
Hint: Theorem 5.13.

(ii) Let L/K be a cyclic field extension and let $\mathrm{Gal}(L/K) = \langle\tau\rangle$. For an element $a \in L$, prove the equivalence

$$\mathrm{trace}_{L/K}(a) = 0 \Leftrightarrow \exists c \in L : a = c - \tau c.$$

Hint: Determine $\dim_K \ker(c \mapsto c - \tau c)$ and $\dim_K \ker(\mathrm{trace}_{L/K})$ in order to prove that $\mathrm{im}(c \mapsto c - \tau c) = \ker(\mathrm{trace}_{L/K})$.

Solution. See Exercise 10.4. ■

Exercise 9.5. Let L/K be an extension with $[L:K] = 2$ and $\mathrm{char}\ K \neq 2$. Express $\mathrm{norm}_{L/K}(x)$ in terms of $\mathrm{trace}_{L/K}(x)$ and $\mathrm{trace}_{L/K}(x^2)$.

Solution. See Exercise 10.5. ■

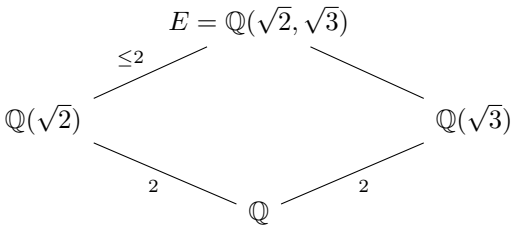
10. Week 10

Exercise 10.1. Let $f(X) = X^4 - 5X^2 + 6$.

(i) Let E be the decomposition field of f over $\mathbb{Q}$. Compute the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.
(ii) Find all the intermediate extensions of E/K.
(iii) Prove that for every prime number p, the polynomial $g(X) = f(X)(X^2-6)$ has always a root in $\mathbb{Z}/p$.

Solution.

(i) Observe that $f(X) = (X^2-2)(X^2-3)$, so its solutions are $\pm\sqrt{2}, \pm\sqrt{3}$. Hence $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and we have the following situation:



But $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, Otherwise $\sqrt{3} = a + b\sqrt{2}$, for some $a, b \in \mathbb{Q}$ and so $3 = a^2 + 2b^2 + 2ab\sqrt{2}$, which would mean that $\sqrt{2} \in \mathbb{Q}$, a contradiction. Therefore $[E : \mathbb{Q}(\sqrt{2})] = 2$ and $[E : \mathbb{Q}] = 4$, so $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.

Hence

$$\mathrm{Gal}(E/K) \cong \mathrm{Gal}(E/\mathbb{Q}(\sqrt{2})) \times \mathrm{Gal}(E/\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Every $\sigma \in \mathrm{Gal}(E/K)$ is completely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Moreover $\sigma(\sqrt{2})$ has to be a root of the minimal polynomial $f(\sqrt{2}, \mathbb{Q}) = X^2 - 2$, which are $\pm\sqrt{2}$. Similarly $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Therefore the 4 elements of $\mathrm{Gal}(E/K)$ are precisely $\sigma_0 = id$ and

$$\sigma_1 : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2} \\ \sqrt{3} & \mapsto \sqrt{3} \end{cases}, \quad \sigma_2 : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2}, \\ \sqrt{3} & \mapsto \sqrt{3} \end{cases}, \quad \sigma_3 : \begin{cases} \sqrt{2} & \mapsto -\sqrt{2}, \\ \sqrt{3} & \mapsto -\sqrt{3} \end{cases}.$$

(ii) $G = \mathrm{Gal}(E/K) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ has 5 subgroups:

$$\{id\}, H_1 = \langle \sigma_1 \rangle, H_2 = \langle \sigma_2 \rangle, H_3 = \langle \sigma_3 \rangle \text{ and } G.$$

The corresponding fixed fields are

$${}^{\{id\}}E = E, {}^{H_1}E = \mathbb{Q}(\sqrt{3}), {}^{H_2}E = \mathbb{Q}(\sqrt{2}), {}^{H_3}E = \mathbb{Q}(\sqrt{6}) \text{ and } {}^{G}E = \mathbb{Q}.$$

(iii) For $p = 2$ and $p = 3$ it is easy to see that 0 is a root of g.

Suppose now that $p > 3$ and that f has no roots in $\mathbb{Z}/p$. Then 2 and 3 are not squares in $\mathbb{Z}/p$. We need to prove that $X^2 - 6$ has a root in $\mathbb{Z}/p$, which means that 6 is a square in $\mathbb{Z}/p$. Take the subgroup $S = \{x^2 \mid x \in (\mathbb{Z}/p)^\times\}$ of squares of $(\mathbb{Z}/p)^\times$. Recall that $(\mathbb{Z}/p)^\times$ is the group of units of a field. Hence it is a cyclic group, say $(\mathbb{Z}/p)^\times = \langle \gamma \rangle$ and $S = \langle \gamma^2 \rangle$. Since $p-1$ is even, the order of γ^2 is $\frac{p-1}{2}$ and S is a subgroup of $(\mathbb{Z}/p)^\times$ of index 2. Therefore if $a, b \notin S$ then, since $S \ \ ab \in S$, otherwise

a product of two elements of $(\mathbb{Z}/p)^\times$ that are not in Sq has to be an element of S. ∎

Exercise 10.2. Let K be a field, $n \geq 1$ and let $E = K(x_1, \ldots, x_n)$ be the rational function field in n indeterminates.

(i) Let G be the subgroup of $\mathrm{Aut}(E/K)$ given by automorphisms of the form

$$\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} \mapsto \frac{f(x_{\pi(1)}, \ldots, x_{\pi(n)})}{g(x_{\pi(1)}, \ldots, x_{\pi(n)})}$$

for some $\pi \in \mathbb{S}_n$. Let $F = {}^G E$. Prove that $\mathrm{Gal}(E/F) = G \cong \mathbb{S}_n$.

(ii) Recall Cayley's theorem. Use it, together with the previous part of the exercise, to prove that every finite group is the Galois group of some Galois extension.

Can you give an explicit description of such an extension for every finite group?

Solution.

(i) Let $\sigma : S_n \to G$ the map $\sigma(\pi) = \sigma_\pi$ such that

$$\sigma_\pi(q(x_1, \dots, x_n) \mapsto q(x_{\pi(1)}, \dots, x_{\pi(n)}),$$

for all $q(x_1, \dots, x_n) \in K(x_1, \dots, x_n)$. First of all, we want to prove that σ is a group homomorphism:

$$\begin{aligned}\sigma_\rho\sigma_\pi(q(x_1, \dots, x_n)) =& \sigma_\rho(q(x_{\pi(1)}, \dots, x_{\pi(n)})) = \\ & q(x_{\rho\pi(1)}, \dots, x_{\rho\pi(n)}) = \sigma_{\rho\pi}(q(x_1, \dots, x_n))\end{aligned}$$

Moreover, by definition of G, σ is surjective. Finally, σ is also injective, i.e $\ker\sigma = \{id\}$. Indeed if $\pi \neq id$, there exists $i \in \{1, \dots, n\}$ such that $\sigma(i) \neq i$. Hence $\sigma_\pi(x_i) = x_{\pi(i)} \neq x_i$.

Now, by Artin's theorem, we know that $\mathrm{Gal}(E/F) = G \cong S_n$, in particular, E/F is a Galois extension.

(ii) Cayley's Theorem states that each finite group is isomorphic to a subgroup of S_n for some n. So take a finite group H, we can assume that H is a subgroup of S_n for some n. By the previous part of the exercise we have that $\mathrm{Gal}(E/F) \cong S_n$. By the Galois correspondence, H corresponds to the intermediate field ${}^H E$ and $\mathrm{Gal}(E/{}^H E) \cong H$.

More precisely, the Cayley embedding is given by

$$\lambda : G \to S_G \quad \lambda(g) = \lambda_g : h \mapsto gh.$$

We can then write $E = K((x_g)_{g\in G})$ and $\sigma : G \to \mathrm{Aut}(E/K)$ given by $\sigma(h) = \sigma_h : q((x_g)_{g\in G}) \mapsto q((x_{hg})_{g\in G})$. ■

Exercise 10.3. Give an explicit description of $\mathrm{norm}_{L/K}$ and $\mathrm{trace}_{L/K}$ for the following field extensions:

(i) $\mathbb{C}/\mathbb{R}$,

(ii) $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$, d squarefree,

(iii) $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$

Hint: Represent an element of $\mathbb{Q}[\sqrt[3]{2}]$ as $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, argue that

$$\begin{aligned}\mathrm{norm}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(x) = (a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot (a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}) \\ \cdot (a + b\xi^2\sqrt[3]{2} + c\xi\sqrt[3]{4})\end{aligned}$$

where $\xi \neq 1$ is a third root of unity. Multiplying this out would give you 27 summands - you only need those which do not contain a rational power of $\sqrt[3]{2}$ (why?). Then sum everything up by using the fact that $\xi + \xi^2 = -1$.

(iv) $K(t)/K(t^p)$, where $\mathrm{char}\, K = p > 0$.

Solution.

(i) $\mathrm{Hom}(\mathbb{C}/\mathbb{R}, \mathbb{C}/\mathbb{R}) = \{id, \sigma\}$, where $\sigma(a + ib) = a - ib$. Hence

$$\mathrm{norm}_{\mathbb{C}/\mathbb{R}}(a + ib) = (a + ib)\sigma(a + ib) = (a + ib)(a - ib) = a^2 + b^2 = |a + ib|^2.$$

$$\mathrm{trace}_{\mathbb{C}/\mathbb{R}}(a + ib) = (a + ib) + \sigma(a + ib) = (a + ib) + (a - ib) = 2a = 2Re(a + ib).$$

(ii) $\mathrm{Hom}(\mathbb{Q}[\sqrt{d}]/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{id, \sigma\}$, where $\sigma(a + \sqrt{d}b) = a - \sqrt{d}b$. Hence

$$\mathrm{norm}_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(a + ib) = (a + \sqrt{d}b)\sigma(a + \sqrt{d}b) = (a + \sqrt{d}b)(a - \sqrt{d}b) = a^2 - db^2.$$

$$\mathrm{trace}_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(a + \sqrt{d}b) = (a + \sqrt{d}b) + \sigma(a + \sqrt{d}b) = (a + ib) + (a - \sqrt{d}b) = 2a.$$

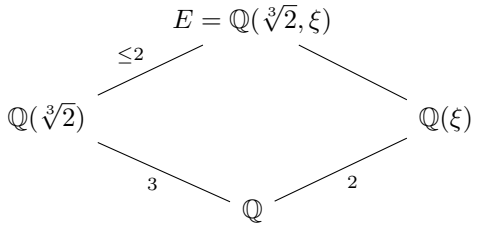
(iii) The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $f(\sqrt[3]{2},\mathbb{Q}) = X^3 - 2$, as it is irreducible (using Eisenstein for $p = 2$). Moreover, his roots in $\mathbb{C}$ are

$$\sqrt[3]{2},\ \sqrt[3]{2}\xi \text{ and } \sqrt[3]{2}\xi^2,$$

where ξ is a primitive third root of unit over $\mathbb{Q}$. So if $\tau \in \mathrm{Hom}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q})$, then $\tau(\sqrt[3]{2}) = \sqrt[3]{2}\xi^i$ for some $i \in \{0,1,2\}$. More precisely,

$$\mathrm{Hom}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}, \overline{\mathbb{Q}}/\mathbb{Q}) = \{id, \sigma, \sigma^2\},\ \text{where } \sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi.$$

Now we want to prove that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ are linearly independent over $\mathbb{Q}(\xi)$. To prove this it is enough to show that $[\mathbb{Q}(\sqrt[3]{2},\xi) : \mathbb{Q}(\xi)] = 3$. So we have the following situation:



And we know that $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$ because $\xi \notin \mathbb{Q}$ and is a root of

$$X^3 - 1 = (X-1)(X^2 + x = 1),$$

so ξ has degree 2 over $\mathbb{Q}$.

Therefore, denoting $E = \mathbb{Q}(\sqrt[3]{2},\xi)$,

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\xi)][\mathbb{Q}(\xi) : \mathbb{Q}] = [E : \mathbb{Q}(\xi)]2$$

but also

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})]3.$$

So the only possibility is that $[E : \mathbb{Q}] = 6$ and $[E : \mathbb{Q}(\sqrt[3]{2})] = 3$.

In particular $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a basis of E over $\mathbb{Q}(\xi)$. Hence

$$\begin{aligned}
&\mathrm{trace}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = \\
&\quad (a + b\sqrt[3]{2} + c\sqrt[3]{4}) + \sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) + \sigma^2(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = \\
&\quad (a + b\sqrt[3]{2} + c\sqrt[3]{4}) + (a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}) + (a + b\xi^2\sqrt[3]{2} + c\xi^4\sqrt[3]{4}) = \\
&\quad 3a + b\sqrt[3]{2}(1 + \xi + \xi^2) + c\sqrt[3]{4}(1 + \xi + \xi^2)
\end{aligned}$$

and

$$\begin{aligned}
&\mathrm{norm}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \\
&\quad = (a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot \sigma(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot \sigma^2(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \\
&\quad = (a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot (a + b\xi\sqrt[3]{2} + c\xi^2\sqrt[3]{4}) \cdot (a + b\xi^2\sqrt[3]{2} + c\xi\sqrt[3]{4}) = \ldots
\end{aligned}$$

As $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ are linearly independent over $\mathbb{Q}(\xi)$ and the norm of an element in $\mathbb{Q}[\sqrt[3]{2}]$ is in $\mathbb{Q}$, we can ignore products that involve a rational multiple of $\sqrt[3]{2}$ resp. $\sqrt[3]{4}$. Note also that $\xi + \xi^2 = -1$.

$$\begin{aligned}
\ldots &= a^3 + 2b^2 + 4c^3 + 2abc(\xi \cdot \xi + \xi^2 \cdot \xi^2 + \xi + \xi^2 + \xi + \xi^2) \\
&= a^3 + 2b^2 + 4c^3 - 6abc.
\end{aligned}$$

(iv) The extension $K(t)/K(t^p)$ is generated by the primitive element t, i.e. $K(t) = K(t^p)(t)$. Furthermore, $f(t, K(t^p)) = X^p - t^p = (X-t)^p$. This proves that $K(t)/K(t^p)$ is purely inseparable. In particular, there is only one embedding into an algebraic closure of $K(t^p)$ which can be taken to be the identity of $K(t)$.

Therefore,

$$\operatorname{trace}_{K(t)/K(t^p)}(x) = [K(t) : K(t^p)]_{\text{ins}} \cdot x = px = 0.$$

Furthermore,

$$\operatorname{norm}_{K(t)/K(t^p)}(x) = x^{[K(t):K(t^p)]_{\text{ins}}} = x^p$$

is the Frobenius endomorphism of $K(t)$. ■

Exercise 10.4.

(i) Let L/K be a finite extension of fields. Prove that $\operatorname{trace}_{L/K} \neq 0$ if and only if L/K is separable.
Hint: Theorem 5.13.

(ii) Let L/K be a cyclic field extension and let $\operatorname{Gal}(L/K) = \langle\tau\rangle$. For an element $a \in L$, prove the equivalence

$$\operatorname{trace}_{L/K}(a) \Leftrightarrow \exists c \in L : a = c - \tau c.$$

Hint: Determine $\dim_K \ker(c \mapsto c - \tau c)$ and $\dim_K \ker(\operatorname{trace}_{L/K})$ in order to prove that $\operatorname{im}(c \mapsto c - \tau c) = \ker(\operatorname{trace}_{L/K})$.

Solution. (i) Suppose that L/K is inseparable. Then K has characteristic p for some prime p and and $[L : K]_{\text{ins}} = p^n$ for some $n > 0$. But then, for all $x \in L$,

$$\begin{aligned}\operatorname{trace}_{L/K}(x) &= [L : K]_{\text{ins}} \cdot \sum_{\sigma \in \operatorname{Hom}(L/K, \bar{L}/K)} \sigma(x) \\ &= \underbrace{p^n}_{=0} \cdot \sum_{\sigma \in \operatorname{Hom}(L/K, \bar{L}/K)} \sigma(x) = 0.\end{aligned}$$

On the other hand, suppose that L/K is separable. Then, by Theorem 5.13, the set $\operatorname{Hom}(L/K, \bar{L}/K)$ is linearly independent. Furthermore, as L/K is separable, $[L : K]_{\text{ins}} = 1$. This implies that

$$\operatorname{trace}_{L/K} = \sum_{\sigma \in \operatorname{Hom}(L/K, \bar{L}/K)} \sigma \not\equiv 0.$$

(ii) Let $\gamma : L \to L;\ c \mapsto c - \tau c$. Our goal is to show that $\operatorname{im}\gamma = \ker \operatorname{trace}_{L/K}$.

First of all, $\operatorname{im}\gamma \subseteq \ker \operatorname{trace}_{L/K}$, as for all $x \in L$,

$$\begin{aligned}\operatorname{trace}_{L/K}(\gamma(x)) &= \operatorname{trace}_{L/K}(x - \tau x) \\ &= \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma(x) - \tau(x) \\ &= \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma(x) - \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma\tau(x) \\ &= \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma(x) - \sum_{\sigma' \in \operatorname{Gal}(L/K)} \sigma'(x) \quad (\sigma' = \sigma\tau) \\ &= 0.\end{aligned}$$

Let us now have a look at the dimensions! We know that

$$\ker\gamma = \{x \in L : \gamma x = 0\} = \{x \in L : \tau x = x\} = {}^{\langle\tau\rangle}L = {}^{\operatorname{Gal}(L/K)}L = K.$$

Therefore $\dim_K \ker \gamma = 1$ which implies that

$$\dim \operatorname{im} \gamma = \dim_K L - \dim_K \ker \gamma = \dim_K L - 1.$$

On the other hand, we have shown that $\operatorname{trace}_{L/K} \neq 0$, therefore $\operatorname{im} \operatorname{trace}_{L/K} = K$, i.e. $\dim_K \operatorname{trace}_{L/K} = 1$ which tells us that

$$\dim_K \ker \operatorname{trace}_{L/K} = \dim_K L - \dim_K \operatorname{im} \operatorname{trace}_{L/K} = \dim_K L - 1.$$

To conclude, we have shown that

$$\dim \operatorname{im} \gamma = \dim_K L - 1 = \dim_K \ker \operatorname{trace}_{L/K}.$$

As $\operatorname{im} \gamma \subseteq \ker \operatorname{trace}_{L/K}$, this shows that $\operatorname{im} \gamma = \ker \operatorname{trace}_{L/K}$. ■

Exercise 10.5. Let L/K be an extension with $[L : K] = 2$ and $\operatorname{char} K \neq 2$. Express $\operatorname{norm}_{L/K}(x)$ in terms of $\operatorname{trace}_{L/K}(x)$ and $\operatorname{trace}_{L/K}(x^2)$.

Solution. Note first that L/K is separable, as $2 \nmid [L : K]$. Therefore $\operatorname{Hom}(L/K, \overline{L}/K)$ has two elements, call them σ, τ. Then

$$\begin{aligned} \operatorname{norm}_{L/K}(x) &= \sigma(x)\tau(x), \\ \operatorname{trace}_{L/K}(x) &= \sigma(x) + \tau(x) \\ \operatorname{trace}_{L/K}(x^2) &= \sigma(x^2) + \tau(x^2) \\ &= \sigma(x)^2 + \tau(x)^2. \end{aligned}$$

From this we derive

$$\begin{aligned} (\operatorname{trace}_{L/K}(x))^2 &= \sigma(x)^2 + \tau(x)^2 + 2\sigma(x)\tau(x) \\ &= \operatorname{trace}_{L/K}(x^2) + 2\operatorname{norm}_{L/K}(x) \\ \Rightarrow\ (\operatorname{trace}_{L/K}(x))^2 - \operatorname{trace}_{L/K}(x^2) &= 2\operatorname{norm}_{L/K}(x) \\ \Rightarrow\ \frac{1}{2}\left((\operatorname{trace}_{L/K}(x))^2 - \operatorname{trace}_{L/K}(x^2)\right) &= \operatorname{norm}_{L/K}(x). \end{aligned}$$

■

11. Week 11

Exercise 11.1. Prove that $f(X) = X^4 - aX^2 + b \in \mathbb{Q}[X]$ is solvable by radicals and determine a radical tower for $R/\mathbb{Q}$, where R contains a decomposition field of f over $\mathbb{Q}$.

Solution. We first solve the equation $f(X) = 0$ by substituting $Y = X^2$. The resulting equation is

$$Y^2 - aY + b = 0$$

whose solutions are $y_{1,2} = \frac{a}{2} \pm \sqrt{\left(\frac{a}{2}\right) - b}$.
Let $K_0 = \mathbb{Q}$. We see that

$$K_1 = K_0(y_1, y_2) = \mathbb{Q}\left(\sqrt{\left(\frac{a}{2}\right)^2 - b}\right).$$

Note that the solutions of $f(X) = 0$ are the solutions of $X^2 = y_1$ resp. $X^2 = y_2$. Let $x_{1,2}$ be the solutions of $X^2 = y_1$, then $x_{1,2} = \pm\sqrt{\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}}$. Similarly, the solutions of $X^2 = y_2$ are $\pm\sqrt{\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}}$.
We therefore get

$$K_2 = K_1(x_1, x_2) = K_1\left(\sqrt{\frac{a}{2} + \sqrt{\left(\frac{a}{2}\right)^2 - b}}\right)$$

and

$$K_3 = K_2(x_3, x_4) = K_2\left(\sqrt{\frac{a}{2} - \sqrt{\left(\frac{a}{2}\right)^2 - b}}\right).$$

It is clear from the construction that $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_3$ is a radical tower and that $K(x_1, \ldots, x_4) \subseteq K_3$. ∎

Exercise 11.2. Let p be prime and suppose that $a \in \mathbb{Q}$ is *not* a p-th power in $\mathbb{Q}$. Let E be the decomposition field of $f = X^p - a \in \mathbb{Q}[X]$. Describe $\mathrm{Gal}(E/\mathbb{Q})$ - does it look familiar to you?
Hint: Observe first that $E = \mathbb{Q}(\omega, \sqrt[p]{a})$ where ω is a p-th root of unity. An element $\varphi \in \mathrm{Gal}(E/\mathbb{Q})$ can now be constructed by extending an element in $\mathbb{Q}(\omega)/\mathbb{Q} \cong (\mathbb{Z}/p)^\times$ by assigning a value for $\varphi(\sqrt[p]{a})$.

Solution. Note that the solutions of $f(X) = X^p - a = 0$ are given by $\omega^i \sqrt[p]{a}$ where ω is a primitive p-th root of unity. It is easily checked that the decomposition field of f is $E = \mathbb{Q}(\omega, \sqrt[p]{a})$.
We first show that $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$. If $p = 2$, this is clear from the fact that a is not a square in $\mathbb{Q}$, so let us assume $p > 2$. We have to show that $f(\sqrt[p]{a}, \mathbb{Q}) = X^p - a$ which amounts to showing that $X^p - a$ is irreducible. Let $h \in \mathbb{Q}[X]$ be a polynomial with $h | X^p - a$, then

$$h = \prod_{j=0}^{\deg h - 1} (X - \omega^{i_j} \sqrt[p]{a})$$

for some - distinct - indices $0 \leq i_j \leq p - 1$. Then

$$|h(0)| = \prod_{j=0}^{\deg h - 1} |-\omega^{i_j} \sqrt[p]{a}| = \sqrt[p]{|a|}^{\deg h} =: c \in \mathbb{Q}.$$

In particular, $c^p = |a|^{\deg h}$ is a p-th power in $\mathbb{Q}$. Suppose that $0 < \deg h < p$, then we can choose integers m, n such that $m \deg h + np = 1$. Therefore $|a|^{(\deg h) \cdot m} \cdot |a|^{pn} =$

$|a|$ would also be a p-th power in $\mathbb{Q}$ which, if $p > 2$, contradicts our assumption that a is not a p-th power in $\mathbb{Q}$. We have therefore shown that $f(\sqrt[p]{a}) = X^p - a$ and $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$.
Note that $\mathbb{Q}(\omega)/\mathbb{Q}$ is a normal extension. We claim that $f(\omega, \mathbb{Q}) = g = \frac{X^p-1}{X-1}$. We calculate

$$g(\omega) = \frac{\omega^p - 1}{\omega - 1} = \frac{1-1}{\omega - 1} = 0$$

but we also have to show that g is irreducible. This is the case if and only if $g(X+1)$ is irreducible. We calculate

$$g(X+1) = \frac{(X+1)^p - 1}{X} = \frac{\sum_{k=1}^{p} \binom{p}{k} X^k}{X} \overset{l=k-1}{=} X^p + \sum_{l=0}^{p-2} \binom{p}{l+1} X^l.$$

Note that $g(X+1)$ is monic, and $p \mid \binom{p}{l+1}$ $(0 \leq l \leq p-2)$. Its constant coefficient is $\binom{p}{1} = p$ which, however, is not divisible by p^2. By the Eisenstein criterion for the prime p, $g(X+1)$ is irreducible and so is g.
Therefore, $\deg f(\omega, \mathbb{Q}) = p - 1 = \varphi(p-1)$ which implies that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}/p) = (\mathbb{Z}/p)^\times$. We make this action more explicit: if $\alpha \in (\mathbb{Z}/p)^\times$ then the element $\varphi_\alpha \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ acts by $\varphi_\alpha(\omega) = \omega^\alpha$. More generally, $\varphi_\alpha(\omega^i) = \omega^{\alpha i}$, where in the exponents, we calculate mod p.
Note that $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ and $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$. As E is the compositum of $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\sqrt[p]{a})$, we deduce that $[E : \mathbb{Q}] \leq p(p-1)$. On the other hand, $[\mathbb{Q}(\omega) : \mathbb{Q}]$ and $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}]$ are coprime and have to divide $[E : \mathbb{Q}]$, so $p(p-1) \leq [E : \mathbb{Q}]$. It follows that $[E : \mathbb{Q}] = p(p-1)$.
If $\varphi \in \mathrm{Gal}(E/\mathbb{Q})$, then $\varphi(\omega) = \omega^\alpha$ for some $\alpha \in (\mathbb{Z}/p)^\times$. Furthermore $\varphi(\sqrt[p]{a}) = \omega^\beta \sqrt[p]{a}$ for some $\beta \in \mathbb{Z}/p$. There are p possible values for $\varphi(\sqrt[p]{a})$ and $p-1$ possible values for $\varphi(\omega)$. As there are $p(p-1)$ possible combinations and $|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = p(p-1)$, we conclude that each combination defines an element of $\mathrm{Gal}(E/\mathbb{Q})$. We can therefore say that

$$\mathrm{Gal}(E/\mathbb{Q}) = \{\varphi_{\alpha,\beta} : \alpha \in (\mathbb{Z}/p)^\times, \beta \in \mathbb{Z}/p\}$$

where $\varphi_{\alpha,\beta} = \omega^\alpha$, $\varphi_{\alpha,\beta}(\sqrt[p]{a}) = \omega^\beta \sqrt[p]{a}$. Let now $\varphi_{\alpha,\beta}, \varphi_{\gamma,\delta} \in \mathrm{Gal}(E/\mathbb{Q})$, then

$$\begin{aligned}
(\varphi_{\alpha,\beta}\varphi_{\gamma,\delta})(\omega) &= \varphi_{\alpha,\beta}(\omega^\gamma) = \omega^{\alpha\gamma}, \\
(\varphi_{\alpha,\beta}\varphi_{\gamma,\delta})(\varphi_{\alpha,\beta}\varphi_{\gamma,\delta})(\sqrt[p]{a}) &= \varphi_{\alpha,\beta}(\omega^\delta \sqrt[p]{a}) \\
&= \omega^{\alpha\delta} \cdot \omega^\beta \sqrt[p]{a} \\
&= \omega^{\alpha\delta+\beta} \sqrt[p]{a}.
\end{aligned}$$

This implies that $\varphi_{\alpha,\beta}\varphi_{\gamma,\delta} = \varphi_{\alpha\gamma,\alpha\delta+\beta}$ which shows that

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} : \alpha \in (\mathbb{Z}/p)^\times, \beta \in \mathbb{Z}/p \right\} \cong \mathbb{Z}/p \rtimes (\mathbb{Z}/p)^\times \cong \mathrm{AGL}(p, 1),$$

the latter being the group of affine transformations of the $\mathbb{Z}/p$-vector space $\mathbb{Z}/p$. ■

Exercise 11.3. Let $p > 2$ be a prime and ω a p-th root of unity. In this exercise, we consider the cyclotomic field extension $\mathbb{Q}(\omega)/\mathbb{Q}$.

(i) What is $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$?
(ii) Prove that there is a unique quadratic intermediate extension $L/\mathbb{Q} = \mathbb{Q}(\sqrt{m})/\mathbb{Q}$ for some $m \in \mathbb{Q}$. When is $L/\mathbb{Q} \subseteq \mathbb{R}$?
Hint: -1 is a square in $(\mathbb{Z}/p)^\times$ if and only if $p = 4k+1$ for some k.
(iii) Define the element

$$\gamma = \sum_{k=0}^{p-1} \omega^{k^2} \in \mathbb{Q}(\omega).$$

Compute $|\gamma|^2 = \gamma \cdot \bar{\gamma}$.

Hint: Note that $\overline{\omega^l} = \omega^{-l}$ and multiply everything out.

(iv) Prove that $\gamma \in L$ and $\gamma^2 \in \mathbb{Z}$. Use this information to determine L!

Solution. (i) We first show that $\deg(f(\omega, \mathbb{Q})) = p - 1$. Let $f = X^{p-1} + \ldots + X + 1 = \frac{X^p - 1}{X - 1}$, then $f(\omega) = \frac{\omega^p - 1}{\omega - 1} = \frac{0}{\omega - 1} = 0$, therefore $g = \frac{X^p - 1}{X - 1} | f(\omega, \mathbb{Q})$. We show that g is irreducible by showing that $g(X + 1)$ is irreducible. We calculate

$$\begin{aligned} g(X+1) &= \frac{(X+1)^p - 1}{(X+1) - 1} \\ &= \frac{\left(\sum_{k=0}^{p} \binom{p}{k} X^k\right) - 1}{X} \\ &= \frac{\sum_{k=1}^{p} \binom{p}{k} X^k}{X} \\ &= X^{p-1} + \sum_{l=0}^{p-2} \binom{p}{l+1} X^l \quad (l = k - 1) \\ &= X^{p-1} + \left(\sum_{l=1}^{p-2} \binom{p}{l+1} X^l\right) + p. \end{aligned}$$

As $p \mid \binom{p}{l}$ for $1 \leq k \leq k$ and $p^2 \nmid p$, we see by the Eisenstein criterion that $g(X + 1)$ is irreducible. Therefore, g is also irreducible.

As $\deg(f(\omega, \mathbb{Q})) = \varphi(p - 1)$, we see that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}/p) = (\mathbb{Z}/p)^\times$ where $\alpha \in (\mathbb{Z}/p)^\times$ acts as the element $\varphi_\alpha \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ with $\varphi_\alpha(\omega) = \omega^\alpha$.

(ii) $\mathbb{Z}/p$ is a field, therefore $(\mathbb{Z}/p)^\times$ is cyclic of order $p - 1$. As $2 \mid p - 1$, we see that $(\mathbb{Z}/p)^\times \cong \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ has a unique subgroup of index 2 which corresponds to the unique quadratic intermediate field $L/\mathbb{Q}$ of $\mathbb{Q}(\omega)/\mathbb{Q}$. This one is given by $\{\varphi^2 : \varphi \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\} \cong ((\mathbb{Z}/p)^\times)^2$. We note that, by the Galois correspondence,

$$L = \{x \in \mathbb{Q}(\omega) : \forall \alpha \in (\mathbb{Z}/p)^\times : \varphi_{\alpha^2}(x) = x\}$$

Let $\psi \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}$ be defined by $\psi(x) = \overline{x}$, the complex conjugation. This is well-defined since $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal. As $\psi(\omega) = \overline{\omega} = \omega^{-1}$, we conclude that $\psi = \varphi_{-1}$.

We conclude that

$$\begin{aligned} L \subseteq \mathbb{R} &\Leftrightarrow \forall x \in L : \psi(x) = x \\ &\Leftrightarrow \forall x \in L : \varphi_{-1}(x) = x \\ &\Leftrightarrow \varphi_{-1} \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ &\Leftrightarrow -1 \in ((\mathbb{Z}/p)^\times)^2 \\ &\Leftrightarrow p \equiv 1 \ (4), \end{aligned}$$

the last step being justified by the hint.

(iii) Note that $\omega^{-1} = \bar{\omega}$. Furthermore, the number ω^k only depends on the class of k modulo p, so we might assume that k comes from $\mathbb{Z}/p$. Using this, we

calculate

$$\begin{aligned}|\gamma|^2 = \gamma\cdot\bar{\gamma} &= \left(\sum_{k\in\mathbb{Z}/p}\omega^{k^2}\right)\cdot\left(\overline{\sum_{l\in\mathbb{Z}/p}\omega^{l^2}}\right)\\ &= \left(\sum_{k\in\mathbb{Z}/p}\omega^{k^2}\right)\cdot\left(\sum_{l\in\mathbb{Z}/p}\omega^{-l^2}\right)\\ &= \sum_{k,l\in\mathbb{Z}/p}\omega^{k^2-l^2}\\ &= \sum_{k,l\in\mathbb{Z}/p}\omega^{(k+l)(k-l)}\end{aligned}$$

We now substitute $k=\frac{a+b}{2}$ and $l=\frac{a-b}{2}$ $(a,b\in\mathbb{Z}/p)$. This is possible since p is odd.

$$\begin{aligned}\ldots, &= \sum_{a,b\in\mathbb{Z}/p}\omega^{ab}\\ &= \sum_{a,b\in\mathbb{Z}/p;\ ab=0}\omega^0 + \sum_{a,b\in\mathbb{Z}/p;\ ab\neq 0}\omega^{ab}\\ &= |\{(a,b)\in\mathbb{Z}/p^2 : ab=0\}| + \sum_{c\in(\mathbb{Z}/p)^\times}\ \sum_{a,b\in\mathbb{Z}/p^2;\ ab=c}\omega^c\\ &= |\{(a,b)\in\mathbb{Z}/p^2 : a=0\vee b=0\}| + \sum_{c\in(\mathbb{Z}/p)^\times}|\{(a,b)\in\mathbb{Z}/p^2 : ab=c\}|\cdot\omega^c\\ &= 2p-1+\sum_{c\in(\mathbb{Z}/p)^\times}|\{(a,a^{-1}c)\in\mathbb{Z}/p^2 : a\neq 0\}|\cdot\omega^c\\ &= p+p-1+\sum_{c\in(\mathbb{Z}/p)^\times}(p-1)\omega^c\\ &= p+(p-1)\cdot\sum_{c\in\mathbb{Z}/p}\omega^c\\ &= p+(p-1)\cdot\sum_{m=0}^{p-1}\omega^m\\ &= p+(p-1)\cdot\frac{1-\omega^p}{1-\omega}\\ &= p+(p-1)\cdot 0 = p.\end{aligned}$$

(iv) We first show that $\gamma\subseteq L$. L is the field fixed by all φ_{α^2} $(\alpha\in(\mathbb{Z}/p)^\times)$, so we check that γ is indeed fixed by all these elements:

$$\begin{aligned}\varphi_{\alpha^2}(\gamma) &= \varphi_{\alpha^2}\left(\sum_{a\in\mathbb{Z}/p}\omega^{a^2}\right)\\ &= \sum_{a\in\mathbb{Z}/p}\omega^{(\alpha a)^2}\\ &\overset{b=\alpha a}{=} \sum_{b\in\mathbb{Z}/p}\omega^{b^2}=\gamma.\end{aligned}$$

Therefore, $\gamma\in L$.

If $p \equiv 1\ (4)$, we have seen in part (ii) that $L \subseteq \mathbb{R}$. Therefore, $\gamma \in \mathbb{R}$ which shows that

$$p = |\gamma|^2 = \gamma^2 \Rightarrow \gamma \in \{\pm\sqrt{p}\}.$$

Therefore $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\gamma) \subseteq L$. As $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = [L : \mathbb{Q}] = 2$, this shows $L = \mathbb{Q}(\sqrt{p})$.

The case $p \equiv 1\ (3)$ is slightly harder. Write $Q = ((\mathbb{Z}/p)^\times)^2$, then $-1 \notin Q$ and, as $[(\mathbb{Z}/p)^\times : Q] = 2$, we see that $(\mathbb{Z}/p)^\times = Q \sqcup -Q$. Furthermore,

$$\gamma = 1 + 2 \cdot \sum_{a \in Q} \omega^a,$$

as each nonzero square in $(\mathbb{Z}/p)^\times$ is representable as a square of exactly two different elements. As $\overline{\gamma} = \varphi_{-1}(\gamma)$, we see that

$$\overline{\gamma} = 1 + 2 \cdot \sum_{a \in Q} \omega^{-a} = 1 + 2 \cdot \sum_{a' \in -Q} \omega'.$$

Now we calculate

$$\begin{aligned}
\gamma + \overline{\gamma} &= 1 + 2 \cdot \sum_{a \in Q} \omega^a + 1 + 2 \cdot \sum_{a \in -Q} \omega^a \\
&= 2 + 2 \cdot \sum_{a \in Q \sqcup -Q} \omega^a \\
&= 2\omega^0 + 2 \cdot \sum_{a \in (\mathbb{Z}/p)^\times} \omega^a \\
&= 2 \cdot \sum_{a \in \mathbb{Z}/p} \omega^a \\
&= 2 \cdot \sum_{m=0}^{p-1} \omega^m = 0
\end{aligned}$$

where the last step is the evaluation of the same geometric sum as in the previous part of the exercise. We conclude that $\overline{\gamma} = -\gamma$. Therefore,

$$p = |\gamma|^2 = \gamma \cdot \overline{\gamma} = \gamma \cdot (-\gamma) = -\gamma^2.$$

This implies $\gamma \in \{\pm i\sqrt{p}\}$. As in the other case, we conclude that $L = \mathbb{Q}(i\sqrt{p})$.

Remark: getting the correct sign of γ is extremely (!) difficult. However, for this exercise, it is sufficient to determine γ up to a potential sign. One can prove, for example using complex analysis, that

$$\gamma = \begin{cases} \sqrt{p} & p \equiv 1\ (4) \\ i\sqrt{p} & p \equiv 3\ (4). \end{cases}$$

■

Exercise 11.4. Let ω be an 8-th root of unity.

(i) What is $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$?
(ii) Prove that $\mathbb{Q}(\omega)/\mathbb{Q}$ has exactly *three* quadratic intermediate extensions. Determine them!
Hint: Compute ω^2 and $(\omega + \omega^{-1})^2$.

Solution. (i) We first show that $\deg f(\omega, \mathbb{Q}) = 4 = \varphi(8)$. As ω is a primitive 8-th root of unity, we see that $(\omega^4)^2 = \omega^8 = 1$ but $\omega^4 \neq 1$, therefore $\omega^4 = -1$ which shows that $f(\omega, \mathbb{Q}) | X^4 + 1$. Now, $g = X^4 + 1$ is irreducible if $g(X+1)$ is irreducible. We calculate

$$g(X+1) = (X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 1 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

Using the Eisenstein criterion with $p = 2$ proves the irreducibility of $g(X+1)$ and therefore of g. $f(\omega, \mathbb{Q}) = X^4 + 1$ has degree $4 = \varphi(8)$ which implies $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathcal{U}(\mathbb{Z}/8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

It is easily checked that $x^2 = \bar{1}$ for all $x \in \mathcal{U}(\mathbb{Z}/8)$. Therefore, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is a Klein Four Group!

(ii) The subgroups of $\mathcal{U}(\mathbb{Z}/8)$ are $\{\bar{1}\}$, $\{\bar{1}, \bar{3}\}$, $\{\bar{1}, \bar{5}\}$, $\{\bar{1}, \bar{7}\}$ and $\mathcal{U}(\mathbb{Z}/8)$ itself. Those subgroups of index 2 correspond two quadratic intermediate extensions. As there are three subgroups of index 2, there are three intermediate extensions.

As $\omega^4 = -1$ (see the previous part), we see that $(\omega^2)^2 = -1$. Therefore, $\omega^2 = \pm i$, depending on the choice of ω. This shows that $\mathbb{Q}(i) \subseteq \mathbb{Q}(\omega)$.

On the other hand,

$$(\omega + \omega^{-1})^2 = \omega^2 + \omega^{-2} + 2\omega\omega^{-1} = i + i^{-1} + 2 = i - i + 2 = 2,$$

which shows that $\omega + \omega^{-1} = \pm\sqrt{2}$, again depending on the choice of ω. Thus, $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\omega)$. As $i, \sqrt{2} \in \mathbb{Q}(\omega)$, we also find that $i\sqrt{2} \in \mathbb{Q}(\omega)$ which proves that $\mathbb{Q}(i\sqrt{2}) \subseteq \mathbb{Q}(\omega)$. ■

12. Week 12

Exercise 12.1. Let $a \in \mathbb{Z}_{>0}$ and $K = \mathbb{Q}(i\sqrt{a})$. Then $K/\mathbb{Q}$ cannot be an intermediate extension of a cyclic extension of degree multiple of 4.
Hint: Suppose there was a cyclic Galois extension $L/\mathbb{Q}$ with $K \subseteq L$ and $[L : K] = 4d$. Use the Galois correspondence to restrict the problem to an intermediate extension $L'/\mathbb{Q}$ with $[L' : \mathbb{Q}] = 4$ and $K \subseteq L'$. Now show that complex conjugation restricts to a nontrivial automorphism of $L'/\mathbb{Q}$. What can you say about its fixed field?

Solution. Assume that there exists a cyclic extension $L/\mathbb{Q}$ of degree $4d$ for some $d \geq 1$. Then $G = \mathrm{Gal}(L/\mathbb{Q})$ is a cyclic group of order $4d$. So there exists a unique subgroup H G of index 4. Since the subgroup of a cyclic group are ordered by divisibility of the order, we get $H \subseteq \mathrm{Gal}(K/\mathbb{Q})$. Hence, using Galois correspondence, $L' = {}^{H} \supseteq K$ and $L'/\mathbb{Q}$ is a cyclic extension of degree 4.
Consider now the complex conjugation $\sigma : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$. It's restriction to L' is an element of $G' = \mathrm{Gal}(L'/\mathbb{Q})$ which is not the identity, as $\sigma(i\sqrt{a}) = -i\sqrt{a}$.
Therefore we have a subgroup of G' $J = \langle \sigma|_{L'} \rangle$ of order 2. Thus, by uniqueness of subgroup of order 2 in a cyclic group, $J = \mathrm{Gal}(L'/K)$. On the other hand, the fixed field of $\mathrm{Gal}(L'/K)$ is $K = \mathbb{Q}(i\sqrt{a})$, while the one fixed by J is

$$ {}^{J}L' = \{z \in L' \mid \bar{z} = z\} = L' \cap \mathbb{R}.$$

But K is not contained in $\mathbb{R}$ since $i\sqrt{a}$ is not real. ■

Exercise 12.2. Compute the Galois group of $f(X) = X^{104} - 1$ over $\mathbb{Z}/13$.
Hint: 104 is divisible by 13.

Solution. First of all note that $104 = 13 \cdot 8$, so

$$X^{104} - 1 = (X^8)^{13} - 1 = (X^8 - 1)^{13}.$$

Thus the Galois group of f is the same as the Galois group of $g = X^8 - 1$.
Note that K is the decomposition field of $g = X^8 - 1$ if and only if K is as small as possible while containing 8 elements such that $\alpha^8 = 1$. For $n > 0$, let F_n be the field with 13^n elements, then $F_n^\times$ is cyclic of order $13^n - 1$. Therefore, $F_n^\times$ contains a subgroup of size 8 if and only if $8|13^n - 1$. One quickly finds that $n = 2$ is the smallest $n > 0$ with that property. Therefore, $K = F_2$. As this implies that $[K : \mathbb{Z}/13] = 2$, we get that $\mathrm{Gal}(K/\mathbb{Z}/13 \cong C_2$. The generator of $\mathrm{Gal}(K/\mathbb{Z}/13)$ is the Frobenius automorphism $\Phi(x) = x^{13}$.
Another way to determine the degree is the following: first decompose

$$X^8 - 1 = (X^4 + 1)(X^2 + 1)(X + 1)(X - 1).$$

Clearly, the factors $X + 1$ and $X - 1$ do not contribute new elements and therefore can be discarded. Note that the element $-1 \in \mathbb{Z}/13$ is a square as $-1 = 5^2 = 8^2$. Therefore, $X^2 + 1 = (X - 5)(X - 8)$ can also be discarded! Furthermore, this allows us to factorize

$$X^4 + 1 = (X^2 - 5)(X^2 - 8).$$

Trying out elements, we find that -5 is *not* a square in $\mathbb{Z}/13$. Let $\alpha \notin \mathbb{Z}/13$ be an element with $\alpha^2 = 5$, then $(5\alpha)^2 = 5^2\alpha^2 = -5 = 8$. Therefore, we can factorize

$$X^4 + 1 = (X - \alpha)(X + \alpha)(X - 5\alpha)(X + 5\alpha).$$

It turns out that $K = \mathbb{Z}/13(\alpha)$ with $f(\alpha, \mathbb{Z}/13) = X^2 - 5$. Therefore, $[K : \mathbb{Z}/13] = 2$ and we can finish as before. ■

Exercise 12.3. Let $f = X^5 - 5 \in \mathbb{Q}[X]$, E be a decomposition field of f over $\mathbb{Q}$ and $G = \mathrm{Gal}(E/\mathbb{Q})$.

(i) Determine $[E : \mathbb{Q}]$.

(ii) Prove (using Sylow's Theorems) that G has a unique subgroup of order 5 and that $G \cong \mathbb{Z}/5 \rtimes \mathbb{Z}/4$.
(iii) Find all intermediate extensions of $E/\mathbb{Q}$, specifying which ones are normal.

Solution. (i) It is easy to see that $E = \mathbb{Q}(\omega, \sqrt[5]{5})$ where ω is a primitive fifth root of unity. We have already shown on the last sheet that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ with $\mathrm{Gal}(\mathbb{Q}(\omega) : \mathbb{Q}) \cong \mathbb{Z}/5^\times$. Furthermore, $f(\sqrt[5]{5}, \mathbb{Q}) = X^5 - 5$, as the latter is irreducible as an Eisenstein polynomial for $p = 5$. This shows $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$.

Note that $E = \mathbb{Q}(\omega)\mathbb{Q}(\sqrt[5]{5})$, therefore

$$[E : \mathbb{Q}] \leq [\mathbb{Q}(\omega) : \mathbb{Q}][\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5 \cdot 4 = 20.$$

We also have $4 = [\mathbb{Q}(\omega) : \mathbb{Q}]|[E : \mathbb{Q}]$ and $5 = [\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}]|[E : \mathbb{Q}]$. Therefore, $20 = \mathrm{lcm}(4, 5)|[E : \mathbb{Q}]$ which proves $[E : \mathbb{Q} = 20$.

(ii) We have shown in the last session that

$$\mathrm{Gal}([E : \mathbb{Q}]) = \{\varphi_{a,b} : a \in \mathbb{Z}/p, b \in (\mathbb{Z}/p)^\times\} \cong \mathbb{Z}/5 \rtimes \mathbb{Z}/5^\times \cong \mathbb{Z}/5 \rtimes \mathbb{Z}/4.$$

Here, $\varphi_{a,b}(\omega) = \omega^b$, $\varphi_{a,b}(\sqrt[5]{5}) = \omega^a \sqrt[5]{5}$.

Furthermore, note that the multiplication rule on $\mathbb{Z}/5 \rtimes \mathbb{Z}/5^\times$ is given by

$$(a, b)(c, d) = (a + bc, bd).$$

One can show the unicity of the subgroup of index 5 as follows:

Let n_5 be the number of 5-Sylow subgroups of $\mathrm{Gal}(E/\mathbb{Q})$ which is of order 20. Then the Sylow theorems tell us that

$$\begin{aligned} &n_5 \geq 1, \\ &n_5|20, \\ &n_5 \equiv 1 \mod 5. \end{aligned}$$

This proves that $n_5 = 1$, i.e. there is a unique 5-Sylow subgroup in $\mathrm{Gal}(E/\mathbb{Q})$ (this can also be derived from the fact that $\mathbb{Z}/5$ is a normal 5-Sylow subgroup in $\mathbb{Z}/5 \rtimes \mathbb{Z}/5^\times$ and therefore the only 5-Sylow subgroup).

(iii) Abbreviate $G = \mathrm{Gal}(E/\mathbb{Q})$, then the possible subgroups are of order 1, 2, 4, 5, 10, 20. Those of order 1 and 20 are obviously 1 and G itself. These correspond to the intermediate fields E resp. $\mathbb{Q}$.

Furthermore, we have seen that there is a unique subgroup of size 5 which is $\langle\varphi_{1,1}\rangle$. The corresponding intermediate field is the unique extension of degree 4, i.e. $\mathbb{Q}(\omega)$.

A subgroup of order 10 has to contain $\langle\varphi_{1,1}\rangle$, the unique subgroup of size 5. Furthermore, it must contain one of the elements of order 2, say $\varphi_{0,-1}$. But then it contains $\varphi_{1,1}^a\varphi_{0,-1} = \varphi_{a,-1}$ as well. Therefore, there is a unique subgroup of order 10 which is given by $\langle\varphi_{1,1}, \varphi_{0,-1}\rangle$. The Galois correspondent is the unique subfield of degree 2 in $\mathbb{Q}(\omega)$ which is $\mathbb{Q}(\sqrt{5})$, as we have seen in the last session.

The 2-Sylow subgroups are of size 4 and one of them is $\langle\varphi_{0,2}\rangle$ which is cyclic. The other 2-Sylows of G are conjugates of this group which are $\langle\varphi_{a,2}\rangle$ ($a \in \mathbb{Z}/5$). The 5 corresponding intermediate fields are of degree 5 and are given by $\mathbb{Q}(\omega^a \sqrt[5]{5})$ ($a \in\in \mathbb{Z}/5$) (note that the a's do not necessarily correspond in subgroups and subfields)

Squaring the generators $\varphi_{a,2}$, one finds that the elements of order 2 in G are the elements $\varphi_{a,2}^2 = \varphi_{(a,2)^2} = \varphi_{3a,-1}$ which can also also be parametrized as $\varphi_{a,-1}$ ($a \in \mathbb{Z}/p$). Therefore, the subgroups of order 2 are

$\langle\varphi_{a,-1}\rangle$ $(a \in \mathbb{Z}/p)$. The 5 Galois correspondents have degree 10 and are given by $\mathbb{Q}(\sqrt{5}, \omega^a \sqrt[5]{5})$ $(a \in \mathbb{Z}/p)$

We list the subgroups and subfields:

Order	Subgroup(s)	Degree	Subfield(s)
1	1	20	E
2	$\langle\varphi_{a,-1}\rangle$ $(a \in \mathbb{Z}/p)$	10	$\mathbb{Q}(\sqrt{5}, \omega^a \sqrt[5]{5})$ $(a \in \mathbb{Z}/p)$
4	$\langle\varphi_{a,2}\rangle$ $(a \in \mathbb{Z}/5)$	5	$\mathbb{Q}(\omega^a \sqrt[5]{5})$ $(a \in \mathbb{Z}/5)$
5	$\langle\varphi_{1,1}\rangle$	4	$\mathbb{Q}(\omega)$
10	$\langle\varphi_{1,1}, \varphi_{0,-1}\rangle$	2	$\mathbb{Q}(\sqrt{5})$
20	E	1	$\mathbb{Q}$

■

Exercise 12.4. Let G be a finite group and M a G-module. Prove the following statements:

(i) If M is finite and $\gcd(|M|, |G|) = 1$ then $H^1(G, M) = 0$.
(ii) If M is finitely generated then $H^1(G, M)$ is finite.

Solution. For both parts of the exercise, we will use the fact that $|G| \cdot H^1(G, M) = 0$ (Theorem 12.14).

(i) For each $x \in M$, we have $|M| \cdot x = 0$. By construction of $H^1(G, M)$, it becomes clear that also $|M| \cdot \alpha = 0$ for each $\alpha \in H^1(G, M)$. As $\gcd(|M|, |G|) = 1$, we can write $1 = a|M| + b|G|$, therefore for all $\alpha \in H^1(G, M)$:

$$\alpha = 1 \cdot \alpha = a \cdot |M| \cdot \alpha + b \cdot |G| \cdot \alpha = 0 + 0 = 0.$$

Therefore, $H^1(G, M) = 0$.

(ii) By construction, $H^1(G, M)$ is finitely generated. Let $\alpha_1, \ldots, \alpha_k$ be generators. As $|G| \cdot \alpha_i = 0$ for all $1 \leq i \leq k$, we deduce that every element of $H^1(G, M)$ is of the form $\sum_{i=1}^k n_i \alpha_i$ with $0 \leq n_i < |G|$ for all i. Therefore $|H^1(G, M)| \leq |G|^k$. In particular, $H^1(G, M)$ is finite. ■

Exercise 12.5. Let K be a field that contains all n-th roots of unity, i.e. the set $\mu_n = \{\zeta \in K : \zeta^n = 1\}$ has n elements. Furthermore, let L/K be a Galois extension.

(i) Denote by $(L^\times)^n$ the group of n-th powers in $L^\times$. Check the exactness of the sequence

$$1 \longrightarrow \mu_n \xrightarrow{\iota} L^\times \xrightarrow{\varepsilon} (L^\times)^n \to 1$$

where $\iota(\zeta) = \zeta$ and $\varepsilon(x) = x^n$. Furthermore, check that this is an exact sequence of G-modules.

(ii) Write down the exact sequence from Theorem 12.3 and prove the existence of an isomorphism

$$((L^\times)^n \cap K)/(K^\times)^n \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n).$$

(iii) Suppose that $n = p$ is prime. What does the previous part of the exercise tell you about intermediate Galois extensions M/K of degree $[M : K] = p$?

Solution. (i) Exactness at μ_n is clear: as ι is an injection: therefore, $\ker \iota = 1 = \mathrm{im}\ (1 \to \mu_n)$.

By construction, ε is a surjection, which implies $\mathrm{im}\ \varepsilon = (L^\times)^n = \ker((L^\times)^n \to 1)$. It follows that the sequence is exact at $(L^\times)^n$.

Finally,

$$\ker \varepsilon = \{x \in L^\times : x^n = 1\} = \mu_n = \mathrm{im}\ \iota$$

as all n-th roots of unity are already contained in K. Therefore, the given sequence is indeed exact.

We have to show compatibility with the Galois action: let $\sigma \in \mathrm{Gal}(L/K)$ and $\zeta \in \mu_n$, then

$$\iota(\sigma(\zeta)) = \sigma(\zeta) = \sigma(\iota(\zeta)),$$

therefore ι is a homomorphism of $\mathrm{Gal}(L/K)$-modules. If $x \in L^\times$, then

$$\sigma(\varepsilon(x)) = \sigma(x^n) = \sigma(x)^n = \varepsilon(\sigma(x))$$

which shows that also ε is a homomorphism of $\mathrm{Gal}(L/K)$-modules.

(ii) Write $G = \mathrm{Gal}(L/K)$. The exact cohomology sequence is given by

$$1 \to H^0(G,\mu_n) \xrightarrow{\iota^0} H^0(G,L^\times) \xrightarrow{\varepsilon^0} H^0(G,(L^\times)^n) \xrightarrow{\delta} H^1(G,\mu_n) \xrightarrow{\iota^1} H^1(G,L^\times) \xrightarrow{\varepsilon^1} H^1(G,(L^\times)^n).$$

We ignore the last term in this sequence. By Hilbert's theorem 90, we have $H^1(G,L^\times) = 1$. Furthermore, $H^0(G,-)$ associates with a G-module its fixed elements, which implies $H^0(G,M) = M \cap K$ for each subgroup $M \leq L^\times$. This shows that $H^0(G,\mu_n) = \mu_n$, $H^0(G,L^\times) = K^\times$ and $H^0(G,(L^\times)^n) = (L^\times)^n \cap K$.

Furthermore, $\mu_n \leq K^\times$, therefore μ_n is a trivial G-module which implies $H^1(G,\mu_n) \cong \mathrm{Hom}(G,\mu_n)$ (see Example 12.10). The first terms of our sequence are therefore

$$1 \to \mu_n \xrightarrow{\iota^0} K^\times \xrightarrow{\varepsilon^0} (L^\times)^n \cap K \xrightarrow{\delta} \mathrm{Hom}(G,\mu_n) \to 1$$

Where ι^0, ε^0 are given by restriction of ι resp. ε.

As $\mathrm{im}\ \varepsilon^0 = (K^\times)^n$, the exactness of this sequence tells us that

$$\mathrm{Hom}(G,\mu_n) \cong ((L^\times)^n \cap K)/\mathrm{im}\ \varepsilon^0 = ((L^\times)^n \cap K)/(K^\times)^n.$$

Using the construction of δ in Theorem 12.13, we can make this isomorphism explicit: take an element $[x] \in ((L^\times)^n \cap K)/(K^\times)^n$, represented by $x \in (L^\times)^n \cap K$. Take an $\alpha \in L^\times$ with $x = \alpha^n$, then $\delta(x) : G \to \mu_n$ is the map given by

$$(\delta(x))(\sigma) = \frac{\sigma(\alpha)}{\alpha}.$$

This induces the isomorphism $\bar{\delta} : ((L^\times)^n \cap K)/(K^\times)^n \to \mathrm{Hom}(G,\mu_n)$; $[x] \mapsto \delta(x)$.

(iii) Let $[x] \in ((L^\times)^p \cap K)/(K^\times)^p$ be a nontrivial class, then $\alpha^p = x \in K$ for some $x \in L^\times$. Consider the extension $[K(\alpha) : K]$ which is of degree p. We remark that

$$\begin{aligned}\mathrm{Gal}(L/K(\alpha)) &= \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) = \alpha\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) : \frac{\sigma(\alpha)}{\alpha}\} \\ &= \ker \bar{\delta}([x]).\end{aligned}$$

Each normal subgroup $N \trianglelefteq \mathrm{Gal}(L/K)$ with $[\mathrm{Gal}(L/K) : N] = p$ is the kernel of some homomorphism $\varphi : \mathrm{Gal}(L/K) \to \mu_p$. The surjectivity of $\bar{\delta}$, together with the previous calculation, shows that each such subgroup N is of the form $\mathrm{Gal}(L/K(\alpha))$ for some $\alpha \in L^\times$ with $\alpha^n \in K$. This is Lemma 11.12.

A more careful inspection shows that there is a $1-1$ correspondence between subgroups of $H \leq ((L^\times)^p \cap K)/(K^\times)^p$ with $|H| = p$ and subgroups of $J \leq \mathrm{Hom}(\mathrm{Gal}(L/K),\mu_p)$ with $|J| = p$. ∎

(Carsten Dietzel) Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium
Email address: Carsten.Dietzel@vub.be

(Silvia Properzi) Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium
Email address: Silvia.Properzi@vub.be