UNIVERSITÀ DEGLI STUDI DI TRENTO

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea in Matematica

Elaborato Finale

Adjunction of n-th roots

Relatore:
Prof. Andrea Caranti

Laureanda:
Ester Dalvit

Anno accademico 2004–2005

Contents

Chapter 1

Introduction

We want to prove some elementary results in Galois theory, concerning in particular adjunction of roots.

First we shall prove a theorem which gives sufficient and necessary conditions for the irreducibility of pure polynomials, namely polynomials of the form $X^n - a$.

Then we shall use this result to prove that if an algebraic closure of a field has finite degree > 1 over the field, then it is equal to the field to which a square root of -1 is added.

These results can be found in the book by Serge Lang, *Algebra* [1].

Finally, we shall prove a theorem concerning the adjunction of n-th roots to the field of the rational numbers. We shall show that for each integer n the extension of $\mathbb{Q}$ through the n-th roots of k distinct primes has degree n^k over $\mathbb{Q}$.

This theorem is due to Ian Richards, and it is presented in the article *An application of Galois theory to elementary arithmetic*, [2].

In the first chapter we consider the pure polynomial

$$X^n - a \in K[X]$$

with coefficients in a field K, and study when it is irreducible.

Setting $a = 1$, we get the polynomial $X^n - 1 \in K[X]$. Its roots, which are the solutions of the equation

$$X^n = 1,$$

are called n-th roots of unity. They may or may not lie in the field K.

If an n-th root of unity has order n, then it is called primitive.

The roots of the pure polynomial $X^n - a$ have much to do with the n-th roots of unity. Let α be a root of $X^n - a$, i.e. $\alpha^n = a$, and let ε be a n-th root of unity, i.e. $\varepsilon^n = 1$; then

$$(\alpha\varepsilon)^n = \alpha^n\varepsilon^n = a \cdot 1 = a.$$

If the polynomial $X^n - a$ is irreducible over the field K, none of its roots lies in the field K. Consider the vector space

$$\{a + b\alpha : a, b \in K\},$$

constructed by adjunction of the root α to the field K. It is easy to note that its dimension over K is n, because this is the smallest integer $s > 1$ such that $\alpha^s \in K$. In this case we say that the degree of the field extension $K(\alpha)$ over K is n.

The Theorem proved in the first chapter claims that the pure polynomial $X^n - a$ is irreducible over the field K if and only if the following two conditions are verified:

- for any prime p dividing n, we have $a \notin K^p$;
- if 4 divides n, then $a \notin -4K^4$.

It is easy to prove that these conditions are sufficient, whereas the proof that they are also necessary involves some Galois theory. In the proof induction is used and the Theorem is reduced to the case where n is a prime power, distinguishing the cases where the characteristic of the field is 0 or a prime number.

In the same chapter a corollary, due to E. Artin, is also proved, in which the adjunction of a n-th root to a field is considered.

The algebraic closure of a field K is "the" smallest field which contains K and the roots of every polynomial whose coefficients lie in K.

The corollary claims that if the algebraic closure of a field K has finite degree greater than 1, then it coincides with the field obtained by adjunction of a square root of -1 to the field K. Furthermore, in this case the characteristic of the field is 0.

In the first part we studied the adjunction of one n-th root of an element a to a field K.

In the second chapter the field $K = \mathbb{Q}$ of the rational numbers is considered, and the adjunction of n-th roots of k distinct primes to $\mathbb{Q}$ is studied.

I. Richards proved that, for any integer $n > 1$, the adjunction to $\mathbb{Q}$ of the n-th roots of k distinct primes $\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}$, gives a field extension, whose degree is n^k. In other words, the powers from 1 to $n-1$ of the n-th roots that we are considering are linearly independent one of another. Thus the dimension of the vector space

$$\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$$

over $\mathbb{Q}$ is n^k.

This result is very easy for $n = 2$, but the general case is an elementary consequence of Galois theory. In the proof the cases where n is odd or even are considered separately, and the induction principle is used.

Chapter 2

Introduzione

In questo lavoro vengono presentati alcuni risultati elementari della teoria di Galois, che riguardano in particolare l'aggiunzione di radici.

Innanzitutto viene enunciato e dimostrato un teorema che presenta condizioni necessarie e sufficienti per avere l'irriducibilità dei polinomi puri, cioè della forma $X^n - a$.

Questo risultato sarà usato per provare che se la chiusura algebrica di un campo K ha grado finito e maggiore di 1 su K, allora essa coincide con il campo che si ottiene aggiungendo a K una radice quadrata di -1.

Questi risultati si trovano nel libro di Lang, *Algebra* [1].

Infine, verrà dimostrato un teorema che tratta dell'aggiunzione di radici n-esime al campo dei razionali. Verrà provato che per ogni intero n maggiore di 1, estendendo $\mathbb{Q}$ con le radici n-esime di k primi distinti, si ottiene uno spazio vettoriale di dimensione n^k su $\mathbb{Q}$.

Questo teorema è stato dimostrato da Ian Richards, nell'articolo *An application of Galois theory to elementary arithmetic*, [2].

Nel primo capitolo viene caratterizzata l'irriducibilità del polinomio puro

$$X^n - a \in K[X]$$

a coefficienti in un campo K.

Ponendo $a = 1$, si ottiene il polinomio $X^n - 1 \in K[X]$, le cui radici, ovvero le soluzioni dell'equazione

$$X^n = 1$$

sono dette radici n-esime dell'unità. Esse possono appartenere o meno al campo K.

Una radice n-esima di periodo n viene detta primitiva.

Le radici del polinomio puro $X^n - a$ sono strettamente legate alle radici n-esime dell'unità: se α è una radice di $X^n - a$, cioè $\alpha^n = a$, e ε una radice dell'unità, cioè $\varepsilon^n = 1$, si ha

$$(\alpha\varepsilon)^n = \alpha^n\varepsilon^n = a \cdot 1 = a.$$

Se il polinomio $X^n - a$ è irriducibile sul campo K, ogni sua radice non appartiene a K. Si verifica facilmente che lo spazio vettoriale ottenuto dall'aggiunzione della radice α al campo K, ovvero lo spazio dato da

$$\{a + b\alpha : a, b \in K\}$$

ha dimensione n su K, poichè il minimo intero $s > 1$ tale che $\alpha^s \in K$ è n. In questo caso si dice che l'estensione $K(\alpha)$ su K ha grado n.

Il teorema enunciato e dimostrato nel primo capitolo afferma che il polinomio $X^n - a$ è irriducibile sul campo K se e solo se vengono soddisfatte le seguenti due condizioni:

- per ogni primo p che divide n, si deve avere $a \notin K^p$;
- se 4 divide n, allora deve essere $a \notin -4K^4$.

Si dimostra facilmente che queste condizioni sono sufficienti, mentre per provare che sono necessarie, ci si riconduce al caso in cui n sia potenza di un primo, si usa il principio di induzione e si distinguono i casi in cui la caratteristica del campo è 0 o un primo.

Nello stesso capitolo viene inoltre esposto un corollario, dovuto a E. Artin, che tratta l'aggiunzione di una radice n-esima ad un campo K.

La chiusura algebrica di un campo K è "il" più piccolo campo, unico a meno di isomorfismi, che contiene K e le radici di ogni polinomio a coefficienti nel campo K.

Il corollario presentato afferma che se la chiusura algebrica di un campo K ha grado finito e maggiore di 1, allora essa coincide con l'estensione del campo mediante una radice quadrata di -1. Inoltre in questo caso il campo ha caratteristica 0, ovvero contiene una copia isomorfa di $\mathbb{Q}$.

Nella prima parte si è studiata l'aggiunzione di una radice n-esima di un intero a ad un campo K.

Nel secondo capitolo viene considerato il caso $K = \mathbb{Q}$, il campo dei razionali, a cui si aggiungono le radici n-esime di k primi distinti.

I. Richards dimostra che, fissato un numero naturale $n > 1$, se si aggiungono al campo dei razionali $\mathbb{Q}$ le radici n-esime di numeri primi distinti $\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}$, si ottiene un'estensione di dimensione n^k. In altre parole le potenze fino alla $(n-1)$-esima delle radici considerate sono tutte linearmente indipendenti tra loro. Dunque

$$\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}),$$

visto come spazio vettoriale su $\mathbb{Q}$, ha dimensione n^k.

Questo risultato si ottiene facilmente per $n = 2$, mentre per interi più grandi è una conseguenza elementare della teoria di Galois. Nella dimostrazione vengono distinti i casi in cui n è pari o dispari, e si procede per induzione.

Una facile applicazione di questo teorema a espressioni quali

$$\sqrt[4]{3} + \sqrt[5]{4} + \sqrt[6]{72}$$

porta a concludere che esse non hanno mai valori razionali, a meno che i termini non si semplifichino in modo ovvio. Nell'esempio, ponendo $n = 60$ e considerando i primi $2, 3$, dal teorema sappiamo che una base di $\mathbb{Q}(\sqrt[60]{2}, \sqrt[60]{3})$ è

$$\left\{ \sqrt[60]{2^a 3^b} : 0 \leq a, b < 60 \right\}.$$

Ognuno dei termini nella nostra espressione ha questa forma, dunque essi sono linearmente indipendenti su $\mathbb{Q}$ e quindi non possono semplificarsi.

Chapter 3

The pure polynomial $X^n - a$

3.1 The result

In this chapter a theorem will be proved, which says when a pure polynomial is irreducible over a field.

Theorem 3.1.1. *Let K be a field, and $n \geq 2$ an integer. Let $a \in K$, $a \neq 0$. Then $X^n - a$ is irreducible in $K[X]$, if and only if:*

1. *for all primes p such that $p \mid n$ we have $a \notin K^p$ and*
2. *if $4 \mid n$, then $a \notin -4K^4$.*

Proof. We will organise the proof as follows: first, we prove that the conditions 1 and 2 are sufficient to let our polynomial be irreducible; then we prove that they are also necessary.

3.2 Proof that the conditions are sufficient

In this part of the proof, we shall reduce the theorem to the case when n is a prime power, proceeding by induction.

We proceed as follows:

1. we prove that if the theorem holds for prime powers $n = p^r$, then it is true for each integer $n > 0$;

2. we prove the result for $n = p$ prime; we distinguish the cases $\operatorname{char} K = p$ and $\operatorname{char} K \neq p$;

3. we prove our theorem for prime powers $n = p^r$, where p is a prime; again we distinguish the cases $\operatorname{char} K = p$ and $\operatorname{char} K \neq p$. In this latter case, we shall make another distinction, namely, letting α be root of $X^p - a$, we investigate what happens if α is or is not a p-th power in $K(\alpha)$.

3.2.1 If the theorem holds for prime powers, then it is true for each positive integer

Assume that the theorem is shown for prime powers, i.e. the polynomial $X^{p^r} - a$ over a field K is irreducible for each integer $r \geq 1$.

Write $n = p^r m$ where p is an odd prime relative prime to m.

By induction, we can assume that $X^m - a$ is irreducible over K. In fact we can consider the prime factorization of m, and

$$m = \underbrace{p_1^{r_1}}_{p_{(1)}^{r_{(1)}}} \underbrace{p_2^{r_2} \dots p_k^{r_k} 2^{r_0}}_{m_{(1)}}$$

Now we consider $m_{(1)} = p_2^{r_2} \dots p_k^{r_k} 2^{r_0}$, and

$$m_{(1)} = \underbrace{p_2^{r_2}}_{p_{(2)}^{r_{(2)}}} \underbrace{p_2^{r_2} \dots p_k^{r_k} 2^{r_0}}_{m_{(2)}}$$

And so on, till

$$m_{(k-1)} = \underbrace{p_k^{r_k}}_{p_{(k)}^{r_{(k)}}} \underbrace{2^{r_0}}_{m_{(k)}}$$

and the last step

$$m_{(k)} = \underbrace{2^{r_0}}_{p_{(k+1)}^{r_{(k+1)}}}$$

where $m_{(k+1)} = 1$. The induction basis is verified, because $X^{m_{(k+1)}} - a = X - a$ is irreducible.

Let

$$X^m - a \quad = \quad \prod_{\nu=1}^{m}(X - \alpha_\nu) \quad \in K[X]$$

be the factorization of $X^m - a$ in an algebraic closure $\overline{K}$ of the field K, and let $\alpha = \alpha_1$; then $\alpha^m = a$.

Substituting X^{p^r} for X we have:

$$X^n - a \quad = \quad X^{p^r m} - a \quad = \quad \prod_{\nu=1}^{m}(X^{p^r} - \alpha_\nu).$$

Claim: α is not a p-th power in $K(\alpha)$.

Suppose it is. Then there is an element $\beta \in K(\alpha)$ such that $\alpha = \beta^p$.

Let $N = N_{K(\alpha)|K}$ be the norm from $K(\alpha)$ to K.

$X^m - a = m_{K,\alpha}$ is the minimum polynomial of α over K, because it is irreducible, monic and α is a root.

Then:

$$(-1)^m(-a) = N(\alpha) = N(\beta^p) = N(\beta)^p$$

since $N : K(\alpha)^* \to K^*$ is a homomorphism of groups.

If m is odd, then

$$a = N(\beta)^p \in K^p.$$

If m is even, then p is odd, because they are coprime, and

$$a = -N(\beta)^p = N(-\beta)^p \in K^p.$$

In both cases the element a is p-th power in K, which is a contradiction to Assumption 1.

Hence α is not a p-th power in $K(\alpha)$.

We assumed that the theorem holds for prime powers; then, since p is odd and $\alpha \notin K(\alpha)^p$, the polynomial $X^{p^r} - \alpha$ is irreducible over $K(\alpha)$.

Let A be a root of the polynomial $X^{p^r} - \alpha \in K(\alpha)$. Then

$$K \subset K(\alpha) \subset K(A)$$

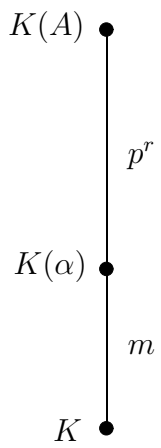

Figure 3.1: The tower of fields considered in the proof.

is a tower of fields, with:

$$[K(\alpha) : K] = \deg(m_{K,\alpha}) = \deg(X^m - a) = m,$$

because $X^m - a$, irreducible over K, is the minimum polynomial of α over K and has degree m. Furthermore

$$[K(A) : K(\alpha)] = \deg(m_{K(\alpha),A}) = \deg(X^{p^r} - \alpha) = p^r,$$

because A is a root of $X^{p^r} - \alpha$, irreducible over $K(\alpha)$, and so this is the minimum polynomial of A over $K(\alpha)$.

By multiplicativity of degrees (Proposition A.1.1), it is

$$[K(A) : K] = [K(A) : K(\alpha)][K(\alpha) : K] = p^r m = n$$

Then $\deg(m_{K,A}) = [K(A) : K] = n$. A is root of $X^{p^r} - \alpha$, and this polynomial divides $X^n - a$, hence A is root of the polynom $X^n - a$, which has degree n. Thus $X^n - a$ is the minimum polynomial of A over K, hence irreducible.

3.2.2 Proof for n prime

Now we want to prove the theorem for prime powers, proceeding by induction over r. For the rest of the proof let $n = p^r$, where p is prime.

The induction starts with $r = 1$, i.e. $n = p$ a prime.
Let α be a root of $f = X^p - a \in K[X]$.

If the characteristic of K is $\mathrm{char}(K) = p$, then

$$X^p - a = X^p - \alpha^p = (X - \alpha)^p \in K[X].$$

Assume f reducible. Then there is a proper divisor $g \in K[X]$ of f, i.e.

$$g = (X - \alpha)^s \in K[X],$$

where $1 \leq s \leq p - 1$. Then

$$g = X^s - s\alpha X^{s-1} + \cdots + (-1)^s \alpha^s \in K[X].$$

In particular $s\alpha \in K$. Since $s < p$, we have $s \cdot 1_K \neq 0_K$, and $\alpha = \dfrac{(s \cdot 1_K)\alpha}{s \cdot 1_K} \in K$.

But $a = \alpha^p$, thus $a \in K^p$, which contradicts Assumption 1.
Then f is irreducible over K when $\mathrm{char}(K) = p$.

When $\mathrm{char}(K) \neq p$, we have $\mathrm{char}(K) \nmid p$, because p is prime. Hence there is (in an algebraic closure of K) a primitive p-th root of unity ε over K.

$\alpha, \alpha\varepsilon, \alpha\varepsilon^2, \ldots, \alpha\varepsilon^{p-1}$ are distinct roots of f, because ε has order p, and these are all the roots, because f has degree p. Then

$$f = \prod_{i=0}^{p-1} (X - \varepsilon^i \alpha) \in K[X].$$

Assume that f is reducible.
Then there is a proper divisor g of f, which means there is an integer $1 \leq s \leq p - 1$ such that

$$g = \prod_{i=1}^{s} \left(X - \varepsilon^{t_i} \alpha\right) \in K,$$

where $1 \leq t_i \leq p - 1$ for each t_i and the elements t_i are all distinct.
In particular the constant term of g is in the field K,

$$\varepsilon^k \alpha^s \in K,$$

for some $1 \leq k \leq p$.

Then

$$K^p \ni (\varepsilon^k \alpha^s)^p = \varepsilon^{pk} \alpha^{ps} = a^s,$$

i.e. there is $b \in K$ such that $b^p = a^s$.

Since p is prime and $s < p$, $\gcd(s, p) = 1$. Using the euclidean algorithm we can find $x, y \in \mathbb{Z}$ such that $xp + ys = 1$. It follows that

$$b^{py} = a^{sy} = a^{1-xp} = aa^{-xp};$$

hence we obtain

$$a = b^{py} a^{xp} = (b^y a^x)^p \in K^p.$$

This is a contradiction to Assumption 1, hence is f irreducible over K.

3.2.3 Proof for prime powers

Now we shall prove the induction step. Let $n = p^r$, with p prime and $r \geq 2$.

By induction, we may assume that the theorem is proved for each polynomial $X^{p^s} - a$, where $s < r$; we must show the result for the polynomial $X^{p^r} - a$.

- Case 1: Assume that $\mathrm{char}(K) = p$.

  α is a root of $X^p - a$, hence $\alpha^p = a$, and

  $$(X - \alpha)^p = X^p - \alpha^p = X^p - a \in K[X]$$

  is the minumum polynomial of α over K.

  It follows that

  $$X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p \in K[X].$$

  Claim: α is not a p-th power in $K(\alpha)$.

  Assume that α is a p-th power in $K(\alpha)$; then there exists an element $\beta \in K(\alpha)$ such that $\beta^p = \alpha$.

  Let $N = N_{K(\alpha)|K}$ be the norm from $K(\alpha)$ to K. The minimum polynomial of α over K is $X^p - a$, because it is irreducible and α is one of its roots. Thus

  $$(-1)^p(-a) = N(\alpha) = N(\beta^p) = N(\beta)^p.$$

If p is odd, $a = N(\beta)^p \in K^p$, contradiction to Assumption 1.

If $p = 2$, let $b = N(\beta) \in K$. Hence $b^2 = -a$. Since $\alpha^2 = a$, $\alpha^2 = -b^2$,

$$0 = \alpha^2 + b^2 = (\alpha + b)^2.$$

Therefore $\alpha = -b$; but $\alpha \notin K$ (because $X^p - \alpha$ is irreducible), and $-b \in K$, contradiction.

Thus the claim is proved.

The polynomial $X^{p^{r-1}} - \alpha \in K(\alpha)[X]$ is irreducible over $K(\alpha)$ by induction hypothesis: its degree is less than p^r and we can apply the theorem because we have just proved condition 1, and

$$\alpha \notin -4K(\alpha)^4 = 0,$$

so condition 2 is also satisfied.

Hence the polynomial $X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p$ is irreducible over K, by unique factorization.

- Case 2: $\mathrm{char}(K) \neq p$

  Let

  $$X^p - a = \prod_{\nu=1}^{p} (X - \alpha_\nu)$$

  be the factorization of $X^p - a$. Then substituting X^{p^r} for X we get

  $$X^{p^r} - a = \prod_{\nu=1}^{p} \left(X^{p^{r-1}} - \alpha_\nu \right);$$

  let $\alpha = \alpha_1$.

  Now we distinguish the cases where α is or is not a p-th power in $K(\alpha)$.

  Suppose that α is not a p-th power in $K(\alpha)$, and let A be a root of $X^{p^{r-1}} - \alpha$.

If p is odd, by induction hypothesis we can apply the theorem to the polynomial $X^{p^{r-1}} - \alpha$, because $\alpha \notin K(\alpha)^p$ and $4 \nmid p^{r-1}$, since p is odd. Thus $X^{p^{r-1}} - \alpha$ is irreducible over $K(\alpha)$. Then

$$[K(A) : K(\alpha)] = \deg(m_{K(\alpha),A}) = \deg(X^{p^{r-1}} - \alpha) = p^{r-1}$$

It is $X^p - a = m_{K,\alpha}$ (because it is irreducible and α is a root); then by multiplicativity of degrees:

$$\begin{aligned} \deg(m_{K,A}) &= [K(A) : K] = \\ &= [K(A) : K(\alpha)][K(\alpha) : K] = \\ &= p^{r-1}p = \\ &= p^r. \end{aligned}$$

A is a root of $X^{p^{r-1}} - \alpha$ and this polynomial divides $X^{p^r} - a$. Hence $X^{p^r} - a$ is the minimum polynomial of A over K. Hence it it irreducible over K.

Consider now the case where $p = 2$.

Assume that $\alpha = -4\beta^4$ for an element $\beta \in K(\alpha)$.

Let $N = N_{K(\alpha)|K}$ be the norm; then $X^2 - a = m_{K,\alpha}$ and:

$$-a = (-1)^2(-a) = N(\alpha) = N(-4\beta^4) = 16N(\beta)^4$$

Let $b = 4N(\beta)^2 \in K$. We have

$$(X + \alpha)(X - \alpha) = X^2 - a = X^2 + b^2 = (X + ib)(X - ib)$$

Comparing the two sides, one gets $\pm ib = \alpha \in K(\alpha)$.

But $b \in K$, hence $K(\alpha) = K(i)$, and $\alpha = (2i\beta^2)^2 \in K(\alpha)^2$, contradiction. It follows that $\alpha \notin -4K(\alpha)^4$.

Then, since by induction $X^{2^{r-1}} - \alpha$ is irreducible over $K(\alpha)$, it follows that $X^{2^r} - a$ is irreducible over K.

Now, suppose that α is a p-th power in $K(\alpha)$. Then there is an element $\beta \in K(\alpha)$ such that $\alpha = \beta^p$.

Let $N = N_{K(\alpha)|K}$ be the norm. Since $X^p - a = m_{K,\alpha}$, it follows that:

$$(-1)^p(-a) = N(\alpha) = N(\beta^p) = N(\beta)^p.$$

If p is odd, then $a = N(\beta)^p \in K^p$, contradiction to Assumption 1.

If $p = 2$, then $-a = N(\beta)^2 \in K^2$. Let $b = \pm N(\beta)$, then $-a = b^2$ for an element $b \in K$. By Assumption 1, a is not a square in K. Since

$$K^2 \ni a = (-1)(-a)$$

and

$$-a \in K^2,$$

it follows that -1 is not a square in K.

Let $i^2 = -1 \notin K^2$. Over $K(i)$ it is:

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib),$$

where both factors have degree 2^{r-1}.

If $X^{2^{r-1}} \pm ib$ is irreducible over $K(i)$, we have finished, because in this case $X^{2^r} + b$ is also irreducible over K, by unique factorization.

Hence, supppose that $X^{2^{r-1}} \pm ib$ is reducible over $K(i)$, then, by induction-assumption, $\pm ib$ is a square in $K(i)$ or $\pm ib \in -4K(i)^4$. In the latter case, there is a $c \in K(i)$ such that $\pm ib = -4c^4 = (2ic^2)^2 \in K(i)^2$.

Then in both cases $\pm ib \in K(i)^2$, say

$$\pm ib = (c + di)^2 = c^2 + 2cdi - d^2,$$

where $c, d \in K$. Then $c^2 = d^2$, so $c = \pm d$, and $\pm ib = 2cdi = \pm 2c^2 i$. Thus:

$$a = -b^2 = (\pm ib)^2 = (\pm 2c^2 i)^2 = -4c^4,$$

and $a \in -4K^4$, contradiction to Assumption 2.

It follows that the polynomials $X^{2^{r-1}} \pm ib$ must be irreducible over $K(i)$, and $X^{2^r} + a$ irreducible over K, by unique factorization.

3.3 Proof that the conditions are necessary

If Assumption 1 does not hold, then there are a prime p and an integer m such that $n = mp$. Furthermore, $a = b^p$ for some $b \in K$. Thus

$$X^m - b \mid X^{mp} - b^p = X^n - a,$$

so our polynomial is reducible.

If condition 2 is not verified, then $n = 4m$ for some integer m and there is an element $b \in K$ such that $a = -4b^4$. Then:

$$\begin{aligned} X^n - a &= X^{4m} + 4b^4 = \\ &= \left(X^{2m} - 2ib^2\right)\left(X^{2m} + 2ib^2\right) = \\ &= \left(X^m \pm (b + ib)\right)\left(X^m \pm (b - ib)\right) = \\ &= \left((X^m + b) \pm ib\right)\left((X^m - b) \pm ib\right) = \\ &= \left(X^{2m} + 2bX^m + 2b^2\right)\left(X^{2m} - 2bX^m + 2b^2\right), \end{aligned}$$

where both factors lie in the polynomial ring $K[X]$; hence the polynomial $X^n - a$ is reducible. □

3.4 Some consequences of the theorem

Corollary 3.4.1. *Let K be a field and $0 \neq a \in K$. Assume that a is not a p-th power for some prime p. If the characteristic is p or if p is odd, then for any integer $r \geq 1$ the polynomial $X^{p^r} - a$ is irreducible over K.*

Proof. The assertion is weaker than Theorem 3.1.1: we consider the polynomial $X^{p^r} - a \in K[X]$. The first condition of Theorem 3.1.1 is fulfilled, since the only prime number which divides p^r is p and by assumption a is not a p-th power. The second condition is also satisfied, because:

- if p is odd, 4 does not divide p^r;
- if $p = 2$ and the characteristic is 2, then $-4K^4 = 0 \neq a$.

□

Corollary 3.4.2 (Artin). *Let K be a field and assume that the algebraic closure $\overline{K}$ of K is of finite degree > 1 over K. Let i denote a square root of -1. Then $\overline{K} = K(i)$ and K has characteristic 0.*

Proof. We note that the extension $\overline{K} \mid K$ is normal, because the algebraic closure of a field contains the roots of all irreducible polynomials over K.

Assume that $\overline{K} \mid K$ is not separable. It follows that $\operatorname{char} K = p > 0$. So $\overline{K}$ must be purely inseparable over some subfield of degree > 1, by Proposition A.2.3. Thus there is a subfield E, $K \subseteq E \subseteq \overline{K}$, such that E is separable over K and $\overline{K}$ is purely inseparable over E. Hence by Definition A.2.2 there is an element $a \in E$ such that $X^p - a$ is irreducible over E.

By Corollary 3.4.1, for each integer $r \geq 1$, the polynomial $X^{p^r} - a$ is irreducible over E. Then

$$\prod_{r \geq 1} p^r \quad \text{divides} \quad \left[\overline{K} : E\right],$$

where the product is not finite. This means that the degree

$$\left[\overline{K} : K\right] = \left[\overline{K} : E\right] [E : K]$$

is not finite, contradiction.

Therefore we assume that $\overline{K}$ is separable over K, and since normal, also Galois.

Let $K_1 = K(i)$, where $i^2 = -1$. The extension K over K_1 is separable by Proposition A.1.2, and normal because $\overline{K}$ is an algebraic closure of K_1.

Hence $\overline{K}$ is Galois over K_1. Let G be its Galois group.

Assume there is a prime p dividing the order of G. Let H be a subgroup of G with order p and let F be its fixed field. Then $\overline{K}$ has degree p over F.

If $\operatorname{char} K = p$, we show that there is an irreducible polynomial over $\overline{K}$, which is a contradiction because this field is algebraically closed.

By the linear independence of characters (Proposition A.3.1), there is an element $\beta \in \overline{K} \setminus F$ such that $\operatorname{Tr}_{\overline{K}|F}(\beta) \neq 0$. Then

$$\operatorname{Tr}_{\overline{K}|F}(\beta^p - \beta) = \sum_\sigma (\beta^p)^\sigma - \sum_\sigma \beta^\sigma = \sum_\sigma (\beta^p - \beta)^\sigma = 0,$$

since $\beta^p - \beta = \wp\beta \in F$.

By Hilbert's Theorem 90 (additive form, Theorem A.5.2), there exists an element $\alpha \in \overline{K}$ such that $\alpha^\sigma - \alpha = \beta^p - \beta$.

Consider now the polynomial $X^p - X - \alpha \in \overline{K}[X]$.

Its roots lie in $\overline{K}$, since this field is algebraically closed. Consider a root, say $\gamma \in \overline{K}$; then $\alpha = \gamma^p - \gamma$. We have

$$\beta^p - \beta = \alpha^\sigma - \alpha = \gamma^{\sigma^p} - \gamma^\sigma - \gamma^p + \gamma = (\gamma^\sigma - \gamma)^p - (\gamma^\sigma - \gamma)\,.$$

Then

$$\wp\beta = \wp\left(\gamma^\sigma - \gamma\right)$$

and, since $\wp$ is an additive homomorphism (by Lemma A.5.3),

$$\wp\left(\beta - (\gamma^\sigma - \gamma)\right) = 0.$$

The kernel of $\wp$ is $\mathbb{F}_p$ (Lemma A.5.3), so

$$\beta - (\gamma^\sigma - \gamma) = k \in \mathbb{F}_p,$$

$$\beta = \gamma^\sigma - \gamma + k.$$

Thus

$$\mathrm{Tr}_{\overline{K}|F}(\beta) = \mathrm{Tr}_{\overline{K}|F}(\gamma^\sigma - \gamma) + \mathrm{Tr}_{\overline{K}|F}(k) = 0,$$

which is a contradiction.

Hence, we may assume $\mathrm{char}\, K \neq p$. The p-th primitive roots of unity are roots of a polynomial of degree $\leq p-1$, because they are roots of

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 \in K[X].$$

Let $\varepsilon \in \overline{K}$ be a primitive root of unity. Then

$$[K(\varepsilon) : F] = \deg(m_{F,\varepsilon}) \leq p - 1.$$

On the other hand, by multiplicativity of degrees, it is

$$\left[\overline{K} : K(\varepsilon)\right]\left[K(\varepsilon) : F\right] = \left[\overline{K} : F\right] = p.$$

It follows that $[K(\varepsilon) : F] = 1$, i.e. $K(\varepsilon) = F$.

By Theorem A.5.1, part 1, $\overline{K}$ is splitting field of a polynomial $X^p - a$ for some $a \in F$.

We claim that the polynomial $X^{p^2} - a$ is reducible over F. Suppose not; then there is $\beta \in \overline{K}$ such that $\beta^{p^2} = a$ and $X^{p^2} - a = m_{F,\beta}$. Then

$$p^2 = \deg(m_{F,\beta}) = [F(\beta) : F] \mid \left[\overline{K} : F\right] = p,$$

which is a contradiction.

By Theorem 3.1.1 one of the following must hold:

- $a \in F^p$, or
- $4 \mid p^2$ and $a \in -4F^4$.

The first case yields a contradiction, because $\overline{K}$ is the splitting field of $X^p - a \in F[X]$ and $\left[\overline{K} : F\right] = p > 1$ means that $a \notin F^p$.

Hence $p = 2$ and $a = -4b^4$ for some $b \in F$.

Then $\left[\overline{K} : F\right] = 2$, and

$$X^2 - a = (X + a^{\frac{1}{2}})(X - a^{\frac{1}{2}}),$$

where $\pm\alpha = a^{\frac{1}{2}} \in \overline{K}$.

$$\overline{K} = F\left(a^{\frac{1}{2}}\right) = F\left((-4b^4)^{\frac{1}{2}}\right) = F\left(2ib^2\right) = F(i).$$

Since $i \in K_1 \subseteq F$, we get

$$\overline{K} = F(i) = F,$$

which is a contradiction, because $\left[\overline{K} : F\right] = p > 1$.

Therefore the Galois group of $\overline{K}$ over K_1 is 1, and $\overline{K} = K(i)$.

It remains to prove that $\mathrm{char}(K) = 0$.

First of all, note that in K a sum of squares is a square. To show this, let $x + iy \in \overline{K} = K(i)$, where $x, y \in K$. This is a square in $\overline{K}$, because this field is algebraically closed. Let

$$x + iy = (u + iv)^2$$

for some $u, v \in K$.

We know

$$x + iy = (u + iv)^2 = u^2 - v^2 + 2iv,$$

then $x = u^2 - v^2$ and $y = 2v$. Thus

$$(u - iv)^2 = u^2 - v^2 - 2iv = x - iy.$$

Then

$$\begin{aligned}(u^2 + v^2)^2 &= ((u + iv)(u - iv))^2 = \\ &= (u + iv)^2(u - iv)^2 = \\ &= (x + iy)(x - iy) = \\ &= x^2 + y^2\end{aligned}$$

Now, x and y were arbitrary, and the sum of their squares is a square.

It follows that every finite sum of squares is a square in K.

Assume that $\mathrm{char}(K) > 0$. Then

$$-1 = \underbrace{1 + \cdots + 1}_{\mathrm{char}(K) \text{ times}}$$

is a finite sum, and since 1 is a square, also -1 is a square in K. This means that there is an element $c \in K$ such that $c^2 = -1$.

$$\overline{K} = K(i) = K(\sqrt{-1}) = K(\sqrt{c^2}) = K(c) = K.$$

But by assumption $\left[\overline{K} : K\right] > 1$, contradiction.

It follows that $\mathrm{char}(K) = 0$.

□

Chapter 4

Adjunction of n-th roots of primes

4.1 The result

In this chapter we show a result due to Richards, which can be found in [2].

Consider linear combinations of radicals, for example $\sqrt[3]{2} + \sqrt[4]{3} - \sqrt[5]{12}$. We will prove that such expressions are irrational whenever their terms do not cancel out in an obvious manner.

Theorem 4.1.1. *Let $n > 1$ be an integer, $p_1, p_2, \ldots, p_k$ distinct positive primes, and $p_i^{\frac{1}{n}}$ the positive n-th root of p_i $(i = 1, \ldots, k)$. Then the field $\mathbb{Q}(p_1^{\frac{1}{n}}, \ldots, p_k^{\frac{1}{n}})$ has degree n^k over $\mathbb{Q}$.*

Theorem 4.1.1 is equivalent to the following:

Theorem 4.1.2. *Let $\{e_i\}$ denote the set of n^k radicals*

$$\sqrt[n]{p_1^{m_1} \cdots p_k^{m_k}}, \quad \text{where} \quad 0 \leq m_i < n, \quad 1 \leq i \leq k.$$

Then the set $\{e_i\}$ is linearly independent over $\mathbb{Q}$.

To prove the equivalence, it is sufficient to note that the set $\{e_i\}$ spans the vector space $\mathbb{Q}(p_1^{\frac{1}{n}}, \ldots, p_k^{\frac{1}{n}})$.

Theorem 4.1.2 is due to Besicovitch, [6]. His proof is based on a Euclidean algorithm in several variables.

For the rest of the chapter, let ε denote a primitive n-th root of unity, and R, E, F the following extension fields of $\mathbb{Q}$:

$$R = \mathbb{Q}(\varepsilon),$$

$$E = \mathbb{Q}(p_1^{1/n}, \ldots, p_k^{1/n}),$$
$$F = R(p_1^{1/n}, \ldots, p_k^{1/n}).$$

4.2 Some examples

Consider the expression

$$\sqrt[3]{2} + \sqrt[4]{3} - \sqrt[5]{12}.$$

Set $n = 60$, $k = 2$ and $p_1 = 2$, $p_2 = 3$.

By Theorem 4.1.1, the degree of $\mathbb{Q}(\sqrt[60]{2}, \sqrt[60]{3})$ over $\mathbb{Q}$ is 3600. A basis of this extension is

$$\left\{ \sqrt[60]{2^a 3^b} : 0 \leq a, b < 60 \right\}.$$

The terms $\sqrt[3]{2} = \sqrt[60]{2^{20}}$, $\sqrt[4]{3} = \sqrt[60]{3^{15}}$ and $\sqrt[5]{12} = \sqrt[60]{12^{12}} = \sqrt[60]{2^{24}3^{12}}$, lie all in this basis. Hence they are linearly independent, and the equation

$$\sqrt[3]{2} + \sqrt[4]{3} - \sqrt[5]{12} = q,$$

where q is a rational number, is impossible, because also 1 is in the basis, so the terms are linearly independent.

Similarly, we can show that $\sqrt{5}$ does not belong to the field generated over $\mathbb{Q}$ by all the real n-th roots of 2 and 3.

Set $k = 3$ and $p_i = \{2, 3, 5\}$ and leave $n \in \mathbb{N}$ undetermined. A basis of the extension $\mathbb{Q}(\sqrt[n]{2}, \sqrt[n]{3}, \sqrt[n]{5})$ over $\mathbb{Q}$ is

$$\left\{ \sqrt[n]{2^a 3^b 5^c} : 0 \leq a, b, c < n \right\}.$$

As a consequence, for each $0 \leq a, b < n$, the term $\sqrt[n]{2^a 3^b}$ is linearly independent of $\sqrt{5}$, since these terms belong to the same basis.

Note that the theorem fails if $\mathbb{Q}$ is replaced by the field R generated by the n-th roots of unity.

For example set $n = 5$ and let ε be a primitive 5-th root of unity, say

$$\frac{1}{4}\left(\sqrt{5} - 1 + i\sqrt{2}\sqrt{5+\sqrt{5}}\right)$$

Set $n = 10$. Since ε is also a 10-th root of unity, $\sqrt{5}$ is contained in the field R generated by the 10-th roots of unity.

Then the field $R(\sqrt[10]{5})$ is the field R, so its degree over R is 1 and not 10, as the theorem would claim.

4.3 The proof of the theorem

We note that if $[F : R] = n^k$, then also $[E : \mathbb{Q}] = n^k$, because the linear independence of the $\{e_i\}$ over R implies their independence over $\mathbb{Q}$ (here we are using Theorem 4.1.2).

First we prove an elementary result, and then we distinguish two cases, namely when n is odd or even.

Lemma 4.3.1. *Let L be an extension field of $R = \mathbb{Q}(\varepsilon)$ and $a \in L$. Then either:*

1. *the polynomial $X^n - a$ is irreducible over L, or*
2. *there exists an integer $m > 1$ such that $m \mid n$ and $\sqrt[m]{a} \in L$.*

Proof. In a suitable extension field we can write

$$X^n - a = \left(X - \varepsilon\sqrt[n]{a}\right)\left(X - \varepsilon^2\sqrt[n]{a}\right)\ldots\left(X - \sqrt[n]{a}\right)$$

If our polynomial $X^n - a$ is reducible over L, any of its nontrivial factors is of the form

$$\prod_{i=1}^{s}\left(X - \varepsilon^{t_i}\sqrt[n]{a}\right) \in L[X]$$

for an integer $1 \leq s < n$, where the $t_i \in \mathbb{Z}$ are all distinct modulo n. In particular the constant term $b = \varepsilon^r a^{s/n}$, for some integer r, lies in L.

Let $m = \dfrac{n}{\gcd(s,n)}$. Choose integers u, v such that $us + vn = \gcd(s,n)$. Then

$$L \ni b^u a^v = \varepsilon^{ru} a^{\frac{s}{n}u} a^v = \varepsilon^{ru} a^{\frac{1}{n}\gcd(s,n)} = \varepsilon^{ru} a^{\frac{1}{m}}$$

Condition 2 is fulfilled: $m = \dfrac{n}{\gcd(s,n)}$ divides n and $1 \leq m \leq n$; $m = 1$ if and only if $\gcd(s,n) = n$, which is not the case, because $0 < s < n$. □

4.3.1 Proof for the case where n is odd

Lemma 4.3.2. *Let $n, m > 0$ be odd integers and $0 < a \in \mathbb{Q}$. No irrational number of the form $\sqrt[m]{a}$ lies in any of the fields $\mathbb{Q}(\varepsilon)$ generated by n-th roots of unity.*

Proof. Without loss of generality, we can assume that m is prime. In fact, if $m = pq$, with p an odd prime and q odd, then $\sqrt[m]{a} = (\sqrt[p]{a})^{\frac{1}{q}}$. Let $\beta = \sqrt[p]{a} \notin \mathbb{Q}(\varepsilon)$. Assume that $\sqrt[q]{\beta} \in \mathbb{Q}(\varepsilon)$, then $\beta = \left(\sqrt[q]{\beta}\right)^q \in \mathbb{Q}(\varepsilon)$, contradiction.

Let ε_m denote a primitive m-th root of unity.

By Theorem 3.1.1 the polynomial $X^m - a$ is irreducible over $\mathbb{Q}$ and over $\mathbb{Q}(\varepsilon_m)$, so it is the minimum polynomial of $\sqrt[m]{a}$ over both fields. Then

$$[\mathbb{Q}(\sqrt[m]{a}) : \mathbb{Q}] = \deg(m_{\mathbb{Q}, \sqrt[m]{a}}) = \deg(X^m - a) = m.$$

On the other side, by Corollary A.4.5 we know that

$$[\mathbb{Q}(\varepsilon_m) : \mathbb{Q}] = m - 1,$$

so we conclude that $\sqrt[m]{a} \notin \mathbb{Q}(\varepsilon_m)$.

Then

$$\begin{aligned} [\mathbb{Q}(\sqrt[m]{a}, \varepsilon_m) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt[m]{a}, \varepsilon_m) : \mathbb{Q}(\varepsilon_m)][\mathbb{Q}(\varepsilon_m) : \mathbb{Q}] = \\ &= \deg(X^m - a) \cdot (m-1) = \\ &= m(m-1). \end{aligned}$$

$\mathbb{Q}(\sqrt[m]{a}, \varepsilon_m) \mid \mathbb{Q}$ is a Galois extension and its Galois group G has order $m(m-1)$.

The automorphisms in G take roots of $X^m - a$ and of $\frac{X^m-1}{X-1}$ in roots, then all the "plausible" automorphisms are actually in G.

Consider the following automorphisms:

$$\varphi_1 : \begin{cases} \sqrt[m]{a} \mapsto \varepsilon_m \sqrt[m]{a} \\ \varepsilon_m \mapsto \varepsilon_m \end{cases}$$

$$\varphi_2 : \begin{cases} \sqrt[m]{a} \mapsto \sqrt[m]{a} \\ \varepsilon_m \mapsto \varepsilon_m^2 \end{cases}$$

Compose them in both the possible ways, and obtain:

$$\varphi_1\varphi_2(\sqrt[m]{a}) = \varepsilon_m \sqrt[m]{a}$$

and

$$\varphi_2\varphi_1(\sqrt[m]{a}) = \varepsilon_m^2 \sqrt[m]{a}$$

This proves that G is not abelian.

But $\mathbb{Q}(\varepsilon_n) \mid \mathbb{Q}$ is an abelian extension for all positive integers n, by Proposition A.4.2. Then for each $n \in \mathbb{N}$,

$$\mathbb{Q}(\sqrt[m]{a}, \varepsilon_m) \not\subseteq \mathbb{Q}(\varepsilon_n).$$

Now, if $\sqrt[m]{a} \in \mathbb{Q}(\varepsilon_m)$, then $\sqrt[m]{a} \in \mathbb{Q}(\varepsilon_{mn})$, since $\varepsilon_n \in \mathbb{Q}(\varepsilon_{mn})$.
Also $\varepsilon_m \in \mathbb{Q}(\varepsilon_{mn})$, then $\sqrt[m]{a}, \varepsilon_m \in \mathbb{Q}(\varepsilon_{mn})$, and

$$\mathbb{Q}(\sqrt[m]{a}, \varepsilon_m) \subseteq \mathbb{Q}(\varepsilon_{mn}),$$

which is not the case.

Then our lemma is proved. □

Remark. The assertion holds also for $\sqrt[4]{a}$, where $0 < a \in \mathbb{Q}$, if $\sqrt{a}$ is irrational.

In fact, if $\sqrt{a}$ is not rational, then the polynomial $X^4 - a$ is irreducible over $\mathbb{Q}$, by Theorem 3.1.1, because $a \notin \mathbb{Q}^2$ and $a \notin -4\mathbb{Q}^4$, since $a > 0$. The rest of the proof is the same.

Lemma 4.3.3. *Assume that Theorems 4.1.1 and 4.1.2 hold for some fixed k with $\mathbb{Q}$ replaced by R, i.e. the field $R(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$ has degree n^k over R, i.e. the set $\{e_i\}$ is linearly independent over R.*
Take a prime p_{k+1} distinct from the primes $p_1, \ldots, p_k$. Then, for any integer $m > 1$ which divides n, the equation

$$\sqrt[m]{p_{k+1}} = \sum_{i=1}^{n^k} c_i e_i, \quad c_i \in R \tag{4.3.1}$$

is impossible.

Proof. Assume that the equation 4.3.1 is satisfied for some $c_i \in R$. We distinguish two cases; both lead to a contradiction.

Suppose that there is only one $c_i \neq 0$. Then

$$\sqrt[m]{p_{k+1}} = c_j e_j = c_j \sqrt[n]{p_1^{m_1}, \ldots, p_k^{m_k}}, \tag{4.3.2}$$

for some $c_j \in R$.

m is odd, since it divides n, which is odd.

We claim that $\sqrt[m]{p_{k+1}} \notin \mathbb{Q}$. Otherwise there would exist coprime integers q, r, such that $\sqrt[m]{p_{k+1}} = \dfrac{q}{r}$; then $r^m p_{k+1} = q^m$. This is a contradiction, because r and q are coprime and $m > 1$.

So we can apply Lemma 4.3.2: we obtain $\sqrt[m]{p_{k+1}} \notin \mathbb{Q}(\varepsilon) = R$.

Raising this equality to the power n we obtain:

$$p_{k+1}^{\frac{n}{m}} = c_j^n p_1^{m_1}, \ldots, p_k^{m_k}$$

Therefore $m_1 = \cdots = m_k = 0$, $c_j = p_{k+1}$ and $\frac{n}{m} = n$; so $m = 1$, contradiction.

Consider now the case where there are at least two terms $c_j, c_h \neq 0$, with $j \neq h$.

If $\frac{e_j}{e_h} \in R$, then $e_j \in R(e_h)$, contradiction to the linear independence of $\{e_i\}$ over R. Then $\frac{e_j}{e_h} \notin R$.

The extension $F \mid R$ is separable and normal, because R is the splitting field of $(X^n - p_1) \cdots (X^n - p_k)$.

Consider the automorphisms $F \to F$. There is one of these automorphisms φ such that

$$\frac{\varphi(e_j)}{\varphi(e_h)} \neq \frac{e_j}{e_h}.$$

Apply φ to the equation 4.3.1.

Since every e_h is the n-th root of an integer, for each h it is:

$$\varphi(e_h) = \varepsilon^{r_h} e_h$$

for some integer r_h, and

$$\varphi(\sqrt[n]{p_{k+1}}) = \varepsilon^{r_0} e_0$$

for some integer r_0.

Furthermore, for $i \neq j$,

$$r_i \not\equiv r_j \mod n,$$

i.e. e_i and e_j are multiplied by different n-th roots of unity under the action of φ. In fact,

$$e_i \mapsto \varepsilon^{r_i} e_i$$

$$e_j \mapsto \varepsilon^{r_j} e_j$$

$$\varepsilon \mapsto \varepsilon$$

and $\varepsilon^{r_i} e_i e_j = e_j \varphi(e_i) \neq e_i \varphi(e_j) = \varepsilon^{r_j} e_j e_i$.

Since $\varepsilon \in R$, this contradicts the assumed linear independence of $\{e_i\}$ over R. □

Now we are ready to prove the theorem for the case where n is odd.

Proof. We proceed by induction over k, and prove the theorem with $\mathbb{Q}$ replaced by R. We have already noted that from this follows the thesis.

When $k = 0$, there is nothing to prove.

Suppose that our assumption is true for some k, i.e.

$$[F : R] = n^k,$$

where $F = R\left(p_1^{1/n}, \ldots, p_k^{1/n}\right)$. Choose a prime p_{k+1} distinct from each $p_1, \ldots, p_k$.

By lemmas 1 and 3 the polynomial

$$X^n - p_{k+1} \in F[X]$$

is irreducible over F. Then

$$[F\,(\sqrt[n]{p_{k+1}}) : F] = n.$$

By multiplicativity if degrees, we obtain

$$[F\,(\sqrt[n]{p_{k+1}}) : R] = n^{k+1}.$$

It follows that

$$[E\,(\sqrt[n]{p_{k+1}}) : \mathbb{Q}] = n^{k+1},$$

so our theorem is proved. □

4.3.2 Proof for the case where n is even

Let $g \geq k$ be a fixed integer. We define the fields:

$$S_g = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_g})$$

$$T_g = R(\sqrt{p_1}, \ldots, \sqrt{p_g})$$

$$E^* = S_g(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$$

$$F^* = T_g(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$$

If $g = k$, the field E^* and F^* are equal to E and F respectively, since $\sqrt{p_i} \in \mathbb{Q}(\sqrt[n]{p_i})$, because n is even.

Lemma 4.3.4. *Let $n, m > 0$ be integers, n even and m odd, and $0 < a \in \mathbb{Q}$. No irrational number of the form $\sqrt[m]{a}$ lies in any of the fields T_g.*

Proof. As in the proof of Lemma 4.3.2, $\sqrt[m]{a} \notin R$, and the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[m]{a}, \varepsilon) \mid \mathbb{Q})$ is not abelian.

It only remains to prove that T_g is an abelian extension of $\mathbb{Q}$. This is true, because R is abelian and all intermediate fields have degree $[R(\sqrt{p_1}, \ldots, \sqrt{p_{i+1}}) : R(\sqrt{p_1}, \ldots, \sqrt{p_i})] = 2$. □

Remark. The assertion holds also for $\sqrt[4]{a}$, where $0 < a \in \mathbb{Q}$, if $\sqrt{a}$ is irrational.

Lemma 4.3.5. *Assume that Theorems 4.1.1 and 4.1.2 hold for some fixed k with $\mathbb{Q}$ replaced by T_g, i.e. the field $T_g(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$ has degree n^k over T_g, i.e. the set $\{e_i\}$ is linearly independent over T_g.*
Take a prime p_{k+1} distinct from the primes $p_1, \ldots, p_k$. Then, for any integer $m > 2$ which divides n, the equation

$$\sqrt[m]{p_{k+1}} = \sum_{i=1}^{n^k} c_i e_i, \tag{4.3.3}$$

where the c_i lie in T_g, is impossible.

Proof. Since $m > 2$, either 4 divides m or m has an odd factor. The proof is the same as Lemma 4.3.3. □

Now the proof of the theorem for even n.

Proof. Apply Lemma 4.3.1 to the polynomial

$$X^{n/2} - \sqrt{p_{k+1}}$$

to show that it is irreducible and by Lemma 4.3.5 obtain the relations:

$$[F^* : T_g] = \left(\frac{n}{2}\right)^k \quad \text{for all } k \leq g$$

$$[S_g : \mathbb{Q}] = 2^g \quad \text{for all } g.$$

The first relation implies that $[E^* : S_g] = \left(\frac{n}{2}\right)^k$.

For $g = k$ we get

$$[E : \mathbb{Q}] = [E : S_k][S_k : \mathbb{Q}] = n^k,$$

so our theorem is proved. □

4.3.3 Elementary proof for the case $n = 2$

The case $n = 2$ is much easier than the general case.

In the nontrivial case considered in Lemma 4.3.5, we have

$$\sqrt{p_{k+1}} = \sum_{i=1}^{2^k} c_i e_i,$$

where $c_i \in \mathbb{Q}$, with at least two nonzero terms.

There must be at least one p_i which occurs with different exponents (0 and $\frac{1}{2}$) in this sum. We can assume that this $p_i = p_k$. We obtain

$$\sqrt{p_{k+1}} = a + b\sqrt{p_k},$$

where $0 \neq a, b \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$.

Squaring both sides we obtain

$$p_{k+1} = a^2 + b^2 p_k + 2ab\sqrt{p_k}.$$

Hence $\sqrt{p_k} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$, and this contradicts the induction hypothesis.

Appendix A

Some results in Galois theory

In this chapter we illustrate some definitions and results concerning field extensions and Galois theory, which we used in the previous chapters. We shall not write the proofs, which can be found in every book treating Galois theory, for example [1] or [3].

A.1 Separable extensions

Proposition A.1.1 (Multiplicativity of degrees). *Let $K \subseteq F \subseteq L$ be a tower of fields, where each step has finite degree. Then*

$$[L : K] = [L : F]\,[F : K]$$

Proposition A.1.2. *Let $L|K$ be an algebraic extension, and F a subfield of L, $K \subseteq F$. Then $L|K$ is separable if and only if $L|F$ and $F|K$ are separable extensions.*

Definition A.1.3. *Let $L|K$ be an extension and $\sigma : K \to F$ be an embedding of K in an algebraically closed field F. The separable degree of L over K*

$$[L : K]_s$$

is the cardinality of the set of extensions of σ to an embedding of L in F.

A.2 Purely inseparable extensions

Definition A.2.1. *Let $L|K$ be an extension and α an element in L algebraic over K. We say that α is purely inseparable over K if there exixsts an integer $n \geq 0$ such that $\alpha^{p^n} \in K$.*

Definition A.2.2. *We say that the extension $L|K$ is purely inseparable if one of the following equivalent conditions holds:*

1. *$[L : K]_s = 1$;*
2. *every element $\alpha \in L$ is purely inseparable over K;*
3. *for every $\alpha \in L$, the minimum polynomial of α over K is of the form $X^{p^n} - a$ for some $n \geq 0$ and some $a \in K$;*
4. *there exists a set of generators $\{\alpha_i\}_{i \in I}$ of L over K such that each α_i is purely inseparable over K.*

Proposition A.2.3. *Let L be an algebraic extension of K. Let E be the compositum of all subfields F of L such that $K \subseteq F$ and F is separable over K. Then E is separable over K and L is purely inseparable over E.*

A.3 The norm and the trace

Let $L|K$ be a separable field extension of degree n, and $\sigma_1 = \mathrm{id}_L, \sigma_2, \ldots \sigma_n : L \to \overline{K}$ the distinct embeddings of L in an algebraic closure $\overline{K}$ of K.

Proposition A.3.1 (Linear independence of characters). *If $c_1, \ldots, c_n \in \overline{K}$ are such that*

$$\sum_{i=1}^{n} c_i x^{\sigma_i} = 0$$

for all $x \in L^*$, then $c_1 = \cdots = c_n = 0$.

Definition A.3.2. *Let $\alpha \in L$. We define the norm of α as the product*

$$N_{L|K}(\alpha) = \prod_{i=1}^{n} \alpha^{\sigma_i}$$

and the trace of α as the sum

$$\mathrm{Tr}_{L|K}(\alpha) = \sum_{i=1}^{n} \alpha^{\sigma_i}.$$

Proposition A.3.3. *The norm $N_{L|K}$ is a multiplicative homomorphism of L^* into K^*.*
The trace $\mathrm{Tr}_{L|K}$ is an additive homomorphism of L into K.

A.4 Cyclotomic fields

Definition A.4.1. *Let $n \geq 2$ be an integer and K be a field, whose characteristic does not divide n. The n-th cyclotomic field K_n over K is the splitting field of $X^n - 1 \in K[X]$.*

Proposition A.4.2. *The extension K_n over K is abelian, i.e. Galois with abelian group.*

Definition A.4.3. *Let $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ denote the distinct primitive n-th roots of unity over a field K (where $r = \varphi(n)$). The polynomial*

$$\Phi_n = \Phi_n(X) = \prod_{i=1}^{r} (X - \varepsilon_i) \in K_n[X]$$

is called the n-th cyclotomic polynomial over K.

Theorem A.4.4 (Gauss). *Φ_n is irreducible over $\mathbb{Q}$.*

Corollary A.4.5. *The degree of the extension $\mathbb{Q}_n$ over $\mathbb{Q}$ is equal to $\varphi(n)$, where φ denotes the Euler φ function and*

$$\mathrm{Gal}\,(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

A.5 Cyclic extensions

Theorem A.5.1. *Let K be a field, and $n > 0$ an integer prime to the characteristic of K. Assume that there is a primitive n-th root of unity in K.*

- *Let L be a cyclic extension of degree n. Then there exists $\alpha \in L$, such that $L = K(\alpha)$ and α satisfies an equation $X^n - a = 0$ for some $a \in K$.*
- *Conversely, let $a \in K$. Let α be a root of $X^n - a$. Then $K(\alpha)$ is cyclic over K and has degree d, where d divides n. Furthermore, α^d lies in K.*

Theorem A.5.2 (Hilbert's Theorem 90). *Let $L|K$ be a cyclic extension of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in L$.*

- *The norm $N_{L|K}(\beta)$ is equal to 1 if and only if there exists an element $0 \neq \alpha \in L$ such that*
$$\beta = \frac{\alpha}{\alpha^\sigma}.$$
- *The trace $\mathrm{Tr}_{L|K}(\beta)$ is equal to 0 if and only if there exists an element $\alpha \in L$ such that*
$$\beta = \alpha - \alpha^\sigma.$$

Lemma A.5.3. *Let K be a field of characteristic $p > 0$. Define $\wp : K \to K$ as follows:*
$$\wp X = \wp(X) := X^p - X.$$
$\wp$ is an additive homomorphism and its kernel is the primefield,
$$\ker \wp = P = \mathbb{F}_p = \{0, 1, \ldots, p-1\}.$$

Theorem A.5.4 (Artin-Schreier). *Let K be a field with characteristic $p > 0$.*

- *Let $L|K$ be a cyclic extension of degree p. Then there exists an element $\alpha \in L$ such that $L = K(\alpha)$ and α is root of an Artin-Schreier polynomial $X^p - X - a$ with some $a \in K$.*
- *Conversely, given the polynomial $X^p - X - a$ with some $a \in K$, either it has one root in K, in which case all its roots are in K, or it is irreducible. In the latter case, if α is a root, then $K(\alpha)$ is cyclic of degree p over K.*

Bibliography

[1] S. Lang,
Algebra,
Addison-Wesley, 1993.

[2] I. Richards,
An application of Galois theory to elementary arithmetic,
Advanced Mathematics **13** (1974), pp. 268-273.

[3] S. Bosch,
Algebra,
Springer, 2001.

[4] B. L. van der Waerden,
Algebra I,
Springer, 1960.

[5] R. L. Roth,
On extensions of $\mathbb{Q}$ *by square roots*,
Amer. Math. Monthly **78** (1971), pp. 392-393.

[6] A. S. Besicovitch,
On the linear independence of fractional powers of integers,
J. London Math. Soc. **15** (1940), pp. 3-6.

[7] E. Artin,
Algebra II,
Vorlesungsausarbeitung Hamburg, Wintersemester 1961/62.