Chapter IV. Cyclotomic fields and applications

ROOTS OF UNITY AND CYCLOMOTIC POLYNOMIALS.

In this chapter we shall consider an important class of normal extensions of the rational number field \( \mathbb{Q} \). Historically these were the first algebraic extensions of \( \mathbb{Q} \) which were the subject of thorough investigations.

First some remarks about roots of unity.

The complex solutions of the equation \( x^n = 1 \), i.e. the numbers \( e^{2\pi i n k} \), \( 0 \leq k < n \), are called the \( n \)-th roots of unity. They form a multiplicative cyclic group of order \( n \). An \( n \)-th root of unity \( \varepsilon \) is called a primitive \( n \)-th root of unity, if it generates the group of \( n \)-th roots of unity. Therefore an \( n \)-th root of unity \( \varepsilon \) is a primitive \( n \)-th root of unity if and only if \( \varepsilon^k \neq 1 \), \( 0 < k < n \). The following lemma is quite elementary

**Lemma 4.1.** Let \( \varepsilon \) be a primitive \( n \)-th root of unity. The following conditions are equivalent

1) \( \varepsilon^k \) is a primitive \( n \)-th root of unity.
2) \( (k,n) = 1 \) (i.e. \( k \) and \( n \) are relatively prime).

*Proof.* Just an easy exercise in group theory. (Cf. Remark 1.82) \( \square \)

In particular \( e^{\frac{2\pi i k}{n}} \), \( 1 \leq k < n \), \( (k,n) = 1 \), are exactly all the primitive \( n \)-th roots of unity.

**Definition 4.2.** The polynomial \( F_n(x) = \prod_{1 \leq k \leq n, (k,n) = 1} (x - e^{\frac{2\pi i k}{n}}) \) is called the \( n \)-th cyclotomic polynomial.

The roots of \( F_n(x) \) are exactly the primitive \( n \)-th roots of unity. The degree of \( F_n(x) \) is \( \varphi(n) \), where \( \varphi(n) \) is the so-called "Eulers \( \varphi \)-function", defined as the number of residue classes modulo \( n \) prime to \( n \).

A priori it is only clear that \( F_n(x) \) has coefficients in \( \mathbb{C} \). However, as we shall see in the following theorem, \( F_n(x) \) has integer coefficients.

**Theorem 4.3.** \( F_n(x) \) is a polynomial in \( \mathbb{Z}[x] \).

To prove this we need the following

**Lemma 4.4.** \( x^n - 1 = \prod_{d|n} F_d(x) \), where \( d \) runs through the positive divisors of \( n \).

*Proof.* The monic polynomials \( x^n - 1 \) and \( \prod_{d|n} F_d(x) \) have no multiple roots (note that \( F_{d_1}(x) \) and \( F_{d_2}(x) \) have no common roots if \( d_1 \neq d_2 \)). Therefore it suffices to show that the two polynomials \( x^n - 1 \) and \( \prod_{d|n} F_d(x) \) have exactly the same roots.
Proof of Theorem 4.3. By induction on $n$ certain an
then all products of three distinct prime divisors, etc. For the sum we then find
$\sum_{n=1}^{\infty} F_n(x)$
by the induction assumption is a monic polynomial with integer coefficients. The
division algorithm now shows that $F_n(x)$ has integer coefficients. □

We now give an explicit formula for $F_n(x)$.

Theorem 4.5. $F_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$, where $\mu$ denotes the Möbius function introduced in Chap. II.

Proof. By lemma 4.4 and Theorem 2.83 in Chap. II we get:

$$\prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n} (\prod_{d|n} F_d(x))^{\mu(d)} = \prod_{d|n} F_d(x)^{\mu(d)}$$

By identifying the degrees of $F_n(x)$ has integer coefficients. □

Since $F_n(x)$ has degree $\varphi(n)$, where $\varphi(n)$ is Eulers $\varphi$-function, by comparison of
degrees we obtain

Corollary 4.6. $\varphi(n) = \sum_{d|n} \frac{n}{d} \mu(d) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$, where $p$ runs through the
distinct prime divisors of $n$.

Proof. By identifying the degrees of $F_n(x)$ and of $\prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}$ we see that
$\varphi(n) = \sum_{d|n} \frac{n}{d} \mu(d)$. It remains then to show that $\sum_{d|n} \frac{n}{d} \mu(d) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$.
Since $\mu(d) = 0$ if $d$ is divisible by the square of a prime, it suffices to consider
the square-free divisors of $n$. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the prime decomposition of $n$
where $p_1, \ldots, p_r$ are the distinct prime divisors of $n$. We consider first the divisor
1, then the prime divisors of $n$, then all products of two distinct prime divisors,
then all products of three distinct prime divisors, etc. For the sum we then find
$\sum_{d|n} \frac{n}{d} \mu(d) = n - \sum_{p|n} \frac{n}{p} + \sum_{p|n} \frac{n}{p^2} - \sum_{p|n} \frac{n}{p^3} + \ldots = n \cdot \prod_{p|n} (1 - \frac{1}{p})$, where the $p_i$'s
are the distinct prime divisors of $n$, the $p_i p_j$'s are the products of two distinct prime
divisors, $p_i p_j p_k$'s are the products of three distinct prime divisors etc. □
Some remarks concerning the coefficients of the cyclotomic polynomials.

Remark 4.7. For \( n > 2 \) the degree of \( F_n(x) \) is an even number and the constant term is 1.

Remark 4.8. The coefficient of the next highest term (i.e. the coefficient of \( x^{\varphi(n)-1} \)) is \(-\mu(n)\), since the sum of the primitive \( n \)-th roots of unity is \( \mu(n) \) (this is an exercise provable by induction).

Remark 4.9. Looking at the first cyclotomic polynomials one might have the temptation to conjecture that all the coefficients of the cyclotomic polynomials were 0 or 1. This, however, is not true. The first counterexample is \( F_{105} \) where the coefficient of \( x^7 \) is -2. But it can be proved that if \( n \) is divisible by at most two distinct odd prime numbers, then the coefficients of \( F_n(x) \) are 0, 1 or -1. (The proof is elementary, but not trivial.)

Remark 4.10. \( F_n(x) \) is "reciprocal" for \( n > 1 \), i.e. if \( a_i \) is the coefficient of \( x^i \) then \( a_i = a_{\varphi(n)-i} \) for \( 0 \leq i \leq \varphi(n) \).

Remark 4.11. For a prime number \( p \) one has \( F_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + x + 1 \).

Numerical examples 4.12. \( F_1(x) = x - 1 \), \( F_2(x) = x + 1 \), \( F_3(x) = x^2 + x + 1 \), \( F_4(x) = x^2 + 1 \), \( F_5(x) = x^4 + x^3 + x^2 + x + 1 \), \( F_6(x) = x^2 - x + 1 \), \( F_8(x) = x^4 + 1 \), \( F_9(x) = x^6 + x^3 + 1 \), \( F_{10}(x) = x^4 - x^3 - x^2 + x + 1 \), \( F_{12}(x) = x^4 - x^2 + 1 \), \( F_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \).

Explicit computations of some roots of unity.

Let \( \varepsilon_n \) be the \( n \)-th root of unity \( e^{2\pi i/n} \).

It is clear that \( \varepsilon_1 = 1 \) and \( \varepsilon_2 = -1 \) and \( \varepsilon_4 = i \). Similarly it is straightforward to check that \( \varepsilon_8 = \cos(\frac{2\pi}{8}) + isin(\frac{2\pi}{8}) = (1 + i)/\sqrt{2} \).

\( \varepsilon_3 \) is the root of \( F_3(x) \) lying in the upper half complex plane. Therefore \( \varepsilon_3 = (-1 + i\sqrt{3})/2 \).

\( \varepsilon_6 \) is the root of \( F_6(x) \) lying in the first quadrant of the complex plane; hence \( \varepsilon_6 = (1 + i\sqrt{3})/2 \).

As for \( \varepsilon_5 \) we write

\[ x^{-2}F_5(x) = x^2 + x^1 + x^{-1} + x^{-2} = (x + 1/x)^2 + (x + 1/x) - 1 \]

which implies that \( 2 \cos(\frac{2\pi}{5}) = \varepsilon_5 + \varepsilon_5^{-1} \) is the (positive) root of

\[ z^2 + z - 1 = 0 \]

hence \( 2 \cos(\frac{2\pi}{5}) = (\sqrt{5} - 1)/2 \) and \( \cos(\frac{2\pi}{5}) = (\sqrt{5} - 1)/4 \).

Now \( \sin(\frac{2\pi}{5}) = \sqrt{1 - \cos^2(\frac{2\pi}{5})} = \frac{1}{4}\sqrt{10 + 2\sqrt{5}} \) so that

\[ \varepsilon_5 = \frac{1}{4}\left(\sqrt{5} - 1 + i\sqrt{10 + 2\sqrt{5}} \right) \].
CYCLOTOMIC POLYNOMIALS ARE IRREDUCIBLE.

For the proof of the irreducibility of cyclotomic polynomials in \( \mathbb{Q}[x] \) we need the following lemmas.

**Lemma 4.13.** If \( f(x) \) and \( g(x) \) are monic polynomials in \( \mathbb{Q}[x] \) for which \( f(x) \cdot g(x) \in \mathbb{Z}[x] \), then \( f(x) \in \mathbb{Z}[x] \) and \( g(x) \in \mathbb{Z}[x] \).

*Proof.* There are natural numbers \( a \) and \( b \) such that \( af(x) \) and \( bg(x) \) are primitive polynomials in \( \mathbb{Z}[x] \). According to Gauss’s lemma the product \( af(x)bg(x) = abf(x)g(x) \) is also a primitive polynomial in \( \mathbb{Z}[x] \). But then \( ab \) must be \( +1 \), and therefore \( a \) and \( b \) must also be \( 1 \). This implies that \( f(x) \) and \( g(x) \) are polynomials in \( \mathbb{Z}[x] \).

**Lemma 4.14.** If \( p \) is a prime number and \( \overline{g}(x) \) is a polynomial in \( \mathbb{Z}_p[x] = \mathbb{F}_p[x] \) then \( \overline{g}(x^p) = (\overline{g}(x))^p \).

*Proof.* This follows from Freshman’s Dream and the fact that \( \alpha^p = \alpha \) for every \( \alpha \) in the finite field \( \mathbb{Z}_p \) with \( p \) elements.

**Theorem 4.15.** \( F_n(x) \) is irreducible in \( \mathbb{Q}[x] \).

*Proof.* Let \( f(x) \) be a monic irreducible polynomial in \( \mathbb{Q}[x] \). We prove:

1° If \( \varepsilon \) is a primitive \( n \)-th root of unity and \( p \) is a prime number that does not divide \( n \), then:

\[
 f(\varepsilon) = 0 \Rightarrow f(\varepsilon^p) = 0.
\]

*Proof of 1°:* Since \( f(x) = \text{Irr}(\varepsilon, \mathbb{Q}) \) the polynomial \( f(x) \) must divide \( x^n - 1 \) inside \( \mathbb{Q}[x] \). By lemma 4.13 it follows that \( f(x) \) must be a polynomial in \( \mathbb{Z}[x] \).

We now consider \( g(x) = \text{Irr}(\varepsilon^p, \mathbb{Q}) \). As before we see that \( g(x) \in \mathbb{Z}[x] \). The polynomial \( g(x^p) \) has \( \varepsilon \) as a root. Hence \( f(x)|g(x^p) \) inside \( \mathbb{Q}[x] \) and thus as before inside \( \mathbb{Z}[x] \). Therefore

\[
 g(x^p) = f(x) \cdot k(x),
\]

where \( k(x) \) a priori is in \( \mathbb{Q}[x] \) and then as before in \( \mathbb{Z}[x] \). Assume now \( f(\varepsilon^p) \neq 0 \). Then \( f(x) \) and \( g(x) \) would be two non-associate irreducible polynomials in \( \mathbb{Q}[x] \). Both of them divide \( x^n - 1 \). Since \( \mathbb{Q}[X] \) is a UFD, \( f(x) \cdot g(x)|x^n - 1 \) inside \( \mathbb{Q}[x] \) and thus as before inside \( \mathbb{Z}[x] \), consequently

\[
 x^n - 1 = f(x) \cdot g(x) \cdot h(x),
\]

where \( h(x) \in \mathbb{Z}[x] \).

For the polynomials \( \overline{f}(x), \overline{g}(x), \overline{h}(x) \) and \( \overline{k}(x) \in \mathbb{Z}_p[x] \) obtained by applying the homomorphism \( \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x] \), we conclude from (\text{\textbullet} ),and (\text{\textbullet\textbullet} )

\[
 \overline{g}(x)^p = \overline{f}(x) \overline{k}(x),
\]

(\text{\textbullet\textbullet\textbullet} )
\[ x^n - 1 = \overline{f}(x) \overline{g}(x) \overline{h}(x), \quad (***) \]

where we have used lemma 4.14 in (***)

From (*** *) we see that every irreducible factor \( \pi(x) \) of \( \overline{f}(x) \) also must appear in \( \overline{g}(x) \), so that the equation (*** *) implies that \( x^n - 1 \) (inside \( \mathbb{Z}_p[X] \)) must be divisible by the square of the polynomial \( \pi(x) \) of positive degree:

\[ x^n - 1 = \pi(x)^2 \cdot q(x), \quad \pi(x), q(x) \in \mathbb{Z}_p[X]. \]

By taking formal derivatives we get

\[ n x^{n-1} = \pi(x) [2 \pi'(x) q(x) + \pi(x) q'(x)]. \]

Here \( \odot \neq 0 \) in \( \mathbb{Z}_p \) since \( p \nmid n \); therefore \( \odot \) has an inverse \( \odot^{-1} \) in \( \mathbb{Z}_p \) and from the above we get

\[ \odot = \pi(x) \left\{ [2 \pi'(x) q(x) + \pi(x) q'(x)] x \cdot \odot^{-1} - \pi(x) q(x) \right\} \in \mathbb{Z}_p[X], \]

which gives the desired contradiction since \( \pi(x) \) has positive degree.

\[ 2^\circ \text{If a monic irreducible polynomial } f(x) \in \mathbb{Q}[x] \text{ has some primitive } n\text{-th root of unity } \varepsilon \text{ as a root then all primitive } n\text{-th roots of unity will be roots of } f(x). \]

\textbf{Proof of } 2^\circ: Every primitive \( n\)-th root of unity has the form \( \varepsilon^k \), where \( (k, n) = 1 \) (cf. lemma 4.1). \( k \) can be written as a product of (not necessarily distinct) prime numbers. None of these prime factors divides \( n \). The assertion 2\(^\circ \) now follows by successive application of \( 1^\circ \).

\[ 3^\circ \text{ } F_n(x) \text{ is irreducible in } \mathbb{Q}[x]. \]

\textbf{Proof of } 3\(^\circ \): Let \( \varepsilon \) be a primitive \( n\)-th root of unity and let \( f(x) = \text{Irr}(\varepsilon, \mathbb{Q}) \). Then \( f(x) \) divides \( F_n(x) \). By \( 2^\circ \) all primitive \( n\)-th roots of unity will be roots of \( f(x) \). This implies that degree(\( f(x) \)) = degree(\( F_n(x) \)) and hence \( F_n(x) = f(x) \), since these polynomials are monic. But \( f(x) \) is by definition irreducible and therefore \( F_n(x) \) is also irreducible. \( \square \)

-- -- -- -- -- -- -- -- --

**DIRICHLETS THEOREM ABOUT PRIME NUMBERS IN ARITHMETIC PROGRESSIONS.**

We make a little digression, where we use that \( F_n(x) \in \mathbb{Z}[X] \).

Dirichlet's famous theorem about prime numbers in arithmetic progressions says that for every pair \( (a, n) \) of relatively prime natural numbers there exist infinitely many prime numbers that are \( \equiv a \) (mod \( n \)). We shall prove this theorem in an important special case:
Theorem 4.16. Dirichlet's Theorem for $a = 1$. For every natural number $n$ there are infinitely many prime numbers that are $\equiv 1 \pmod{n}$.

Proof. The statement “For every natural number $n$ there exists a prime number that is $\equiv 1 \pmod{n}$” implies the statement: “For every natural number $n$ there exist infinitely many prime numbers that are $\equiv 1 \pmod{n}$”. Indeed, let $p_1, \ldots, p_t$ be primes that are $\equiv 1 \pmod{np_1 \cdots p_t}$. By assumption there exists a prime number $p$ that is $\equiv 1 \pmod{np_1 \cdots p_t}$. This prime number $p$ is $\equiv 1 \pmod{n}$ and definitely $\neq p_i$ for $1 \leq i \leq t$.

Therefore it suffices to show that for every natural number $n$ there is a prime number that is $\equiv 1 \pmod{n}$.

We may, of course, assume that $n > 2$.

The desired theorem is a consequence of the following two assertions:

Assertion 1. $|F_n(n)| > 1$ for every natural number $n > 2$ and therefore $F_n(n)$ is divisible by at least one prime number.

Assertion 2. Every prime divisor $p$ of $F_n(n)$ is $\equiv 1 \pmod{n}$.

Proof of assertion 1. Since $F_n(n) = \prod_{1 \leq k < n \atop (k,n) = 1} (n - e^{2\pi i k/n})$ and every factor for $n > 2$ has absolute value $> 1$ the desired inequality follows.

Proof of assertion 2. Let $p$ be a prime divisor of $F_n(n)$, where $n > 2$. Since $F_n(x)$ has constant term 1 it follows that $F_n(n) \equiv 1 \pmod{n}$ and therefore $p$ does not divide $n$.

From lemma 4.4 we know that $x^n - 1 = \prod_{d|n} F_d(x)$ and by setting $x = n$ we see that $n^n - 1$ is divisible by $p$.

Therefore the group theoretical order $t$ of the residue class $\overline{1} \pmod{p}$ divides $n$. We claim that $t = n$. Indeed, assume that $t < n$. Then we would have the product representation

$$\frac{x^n - 1}{x^t - 1} = F_n(x) \prod_{\delta} F_\delta(x)$$

where $\delta$ runs through those divisors $\delta$ of $n$ for which $\delta < n$ and $\delta$ does not divide $t$. Setting $x = n$ shows that $F_n(n)$ divides $\frac{n^n - 1}{n^t - 1}$. On the other hand the identity

$$\frac{n^n - 1}{n^t - 1} = \frac{(n^t)^{\frac{n}{t}} - 1}{n^t - 1} = \left(n^t\right)^{\frac{n}{t}-1} + \left(n^t\right)^{\frac{n}{t}-2} + \ldots + n^t + 1$$

shows that

$$\frac{n^n - 1}{n^t - 1} \equiv 1 + \ldots + 1 = \frac{n}{t} \pmod{p}$$

with $\frac{n}{t}$ terms.
The above would therefore imply that \( p \) should divide \( \frac{n}{d} \) and thereby also \( n \) contradicting our first observation.

Consequently \( t = n \), and since the group theoretical order of every element in the multiplicative group \( (\mathbb{Z}_p \setminus \{0\}, \cdot) \) is a divisor of \( p - 1 \) it follows that \( p \equiv 1 \pmod{n} \). □

**CYCLOTOMIC FIELDS.**

We now consider the field \( \mathbb{Q}_n = \mathbb{Q} \left( e^{\frac{2\pi i}{n}} \right) \), which is called the \( n \)-th *cyclo-

tomic field*. \( \mathbb{Q}_n \) is the splitting field for \( x^n - 1 \) over \( \mathbb{Q} \). So \( \mathbb{Q}_n / \mathbb{Q} \) is a normal extension. Here is \([\mathbb{Q}_n : \mathbb{Q}] = \deg \left( \text{Irr} \left( e^{\frac{2\pi i}{n}}, \mathbb{Q} \right) \right) = \deg(F_n(x)) = \varphi(n)\). Let \( \varepsilon \) be \( e^{\frac{2\pi i}{n}} \). If \( \sigma \) is an automorphism in \( \text{Gal}(\mathbb{Q}_n / \mathbb{Q}) \) then (by Lemma 3.4) \( \sigma(\varepsilon) \) must be \( \varepsilon^a \), where \( \varepsilon^a \) is a root of \( F_n(x) \), i.e. \( \varepsilon^a \) is a primitive \( n \)-th root of unity. Hence \( (a, n) = 1 \) where \( a \) is determined modulo \( n \). Consequently we get a well defined map:

\[
\text{Gal}(\mathbb{Q}_n / \mathbb{Q}) \longrightarrow \mathbb{Z}_n^*, \quad \text{(where } \mathbb{Z}_n^* \text{ are the residue classes modulo } n \text{ prime to } n) \]

by

\[
\psi(\sigma) = @ \pmod{n}, \text{ if } \sigma(\varepsilon) = \varepsilon^a.
\]

Here \( \psi \) is injective since \( \sigma \) is uniquely determined by its value on \( \varepsilon \). Because \( |\text{Gal}(\mathbb{Q}_n / \mathbb{Q})| = [\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}_n^*)| \) the mapping \( \psi \) is also surjective. The residue classes prime to \( n \) modulo \( n \) form a multiplicative group (notice that \( \mathbb{Z}_n^* \) consists of the invertible elements in \( \mathbb{Z}_n \)). Furthermore \( \psi \) is a homomorphism:

\[
\psi(\sigma_1 \sigma_2) \text{ determined by } \sigma_1 \sigma_2(\varepsilon) = \varepsilon^{\psi(\sigma_1 \sigma_2)}
\]

\[
\sigma_2(\varepsilon) = \varepsilon^{\psi(\sigma_2)}; \quad \sigma_1(\sigma_2(\varepsilon)) = \sigma_1 \left( \varepsilon^{\psi(\sigma_2)} \right) = (\sigma_1(\varepsilon))^{\psi(\sigma_2)} =
\]

\[
\left( \varepsilon^{\psi(\sigma_1)} \right)^{\psi(\sigma_2)} = \varepsilon^{\psi(\sigma_1) \psi(\sigma_2)} \text{ i.e.: } \psi(\sigma_1 \sigma_2) = \psi(\sigma_1) \psi(\sigma_2).
\]

Thus we have proved

**Theorem 4.17.** \( \text{Gal}(\mathbb{Q}_n / \mathbb{Q}) \simeq \mathbb{Z}_n^* \) (= *the multiplicative group of the prime residue classes modulo* \( n \)).

In particular, \( \text{Gal}(\mathbb{Q}_n / \mathbb{Q}) \) is abelian.

It is clear [cf. the fundamental theorem of Galois theory 4) and 5)] that every subfield \( K \subseteq \mathbb{Q}_n \) is normal over \( \mathbb{Q} \) with abelian Galois group, namely \( \text{Gal}(K / \mathbb{Q}) \simeq \text{Gal}(\mathbb{Q}_n / \mathbb{Q}) / \text{Gal}(\mathbb{Q}_n / K) \).

---

1"Beloved child has many names": There are several notations for the \( n \)-th cyclotomic field. Some authors use \( \mathbb{Q}(\zeta_n) \) or \( \mathbb{Q}(\mu_n) \), others \( \mathbb{Q}[n] \) or \( \mathbb{Q}^{(n)} \) and the list comprises at least 20 other names. We have chosen \( \mathbb{Q}_n \) since it is the shortest.
A classical (very deep) theorem gives a characterization of the normal extensions of $\mathbb{Q}$ with abelian Galois group.

**Theorem 4.18. Kronecker–Weber Theorem.** Let $K/\mathbb{Q}$ be a finite normal extension. Then: $K/\mathbb{Q}$ is normal with abelian Galois group $\iff K \subseteq \mathbb{Q}_n$ for a suitable $n$.

We have already proved $\Leftarrow$. The other implication $\Rightarrow$ is very hard to prove.

We shall just prove (the hard implication of) the theorem in the very special case where $\text{Gal}(K/\mathbb{Q})$ is cyclic of order 2.

First a quite elementary lemma.

**Lemma 4.19.** Let $K$ be a field of characteristic 0 and $L$ a quadratic extension of $K$, i.e. $[L : K] = 2$.

i) There exists an element $a$ in $K$ such that $L = K(\sqrt{a})$.

ii) If $K = \mathbb{Q}$ we can choose $a$ as a rational square-free integer (i.e. $a \in \mathbb{Z}$ and $a$ is not divisible by the square of any prime number).

**Proof.**

ad i) Any $\alpha \in L \setminus K$ generates $L$ over $K$, i.e. $L = K(\alpha)$. The polynomial $\text{Irr}(\alpha, K)$ can be written $x^2 + k_1 x + k_2$, where $k_1$ and $k_2$ belong to $K$. As a one may use the discriminant $k_1^2 - 4k_2$.

ad ii) The assertion follows from the fact, that for every rational number $q \neq 0$ there exists a rational number $q_1$ such that $qq_1$ is a square-free integer.

$\square$

**Proof of Kronecker-Webers theorem for quadratic extensions of $\mathbb{Q}$.**

Because of lemma 4.19 it suffices to show that $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}_{4|a|}$ for every square-free integer $a$. This will be done in 4 steps:

1. We observe that $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}_4 \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-2}) = \mathbb{Q}_8$.

2. For a natural number $n$ the cyclotomic field $\mathbb{Q}_n$ is the splitting field over $\mathbb{Q}$ for the polynomial $x^n - 1$. By Theorem 2.84 the square root $\sqrt{\text{disc}(x^n - 1)}$ lies in $\mathbb{Q}_n$. In Theorem 2.88 it was shown that this discriminant is $n^n(-1)^{(n-1)(n-2)}$. When $n$ is odd, the discriminant can be written $(n^{\frac{n-1}{2}})^2 \cdot (-1)^{\frac{n-1}{2}} \cdot n$. Therefore $\mathbb{Q}(\sqrt{\text{disc}(x^n - 1)}) = \mathbb{Q}(\sqrt{n(-1)^{\frac{n-1}{2}}})$ which is

$\mathbb{Q}(\sqrt{n})$, if $n \equiv 1$ (mod 4) and
$\mathbb{Q}(\sqrt{-n})$, if $n \equiv 3$ (mod 4).

3. If $n$ and $m$ are natural numbers and $n$ divides $m$ then obviously $\mathbb{Q}_n \subseteq \mathbb{Q}_m$.

4. If $a$ is a square-free integer, then $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}_{4|a|}$. There are two possibilities: i) $a$ is odd and ii) $a$ is even.
ad i) We distinguish between the case i1), where $a$ is positive and the case i2), where $a$ is negative.

First case i1): For $a \equiv 1 \mod 4$, the above assertions 2. and 3. imply that $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}_{a} \subseteq \mathbb{Q}_{4|a|}$.

For $a \equiv 3 \mod 4$, the above assertions 1. 2. and 3. imply that $\mathbb{Q}(\sqrt{-1}, \sqrt{-a}) \subseteq \mathbb{Q}_{4|a|}$.

Second case i2): Clearly $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{|a|})$. By the assertions 1. and 2. and the above treated case i1) we conclude that $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}_{4|a|}$.

ad ii) Here $a = 2u$, where $u$ is odd since $a$ is square-free. Obviously $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{u})$ which [according to assertions 1., 3. and the above case i)] is contained in $\mathbb{Q}_{8|4|u|} \subseteq \mathbb{Q}_{4|a|}$.

\[ \square \]

Example 4.20. If $p$ is an odd prime number the Galois group $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ is cyclic of order $p - 1$, since the multiplicative group of the non-zero elements in the finite field $\mathbb{Z}_p = \mathbb{F}_p$ is cyclic. Therefore $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ contains exactly one subgroup of index 2. By the fundamental theorem of Galois theory $\mathbb{Q}_p$ thus contains exactly one quadratic subfield. As the above proof shows, this quadratic subfield is $\mathbb{Q}(\sqrt{p})$ when $p \equiv 1 \mod 4$ and $\mathbb{Q}(\sqrt{-p})$ when $p \equiv 3 \mod 4$.

RELATIONS BETWEEN CYCLOTOMIC FIELDS.

We first give some useful applications of the formula for $\varphi(n)$ from the Corollary 4.6.

Lemma 4.21. Let $m$ and $n$ be positive integers and let $d$, resp. $f$, be the greatest common divisor of $m$ and $n$, resp. the least common multiple of $m$ and $n$. Then

i) $mn = df$

ii) $\varphi(m)\varphi(n) = \varphi(d)\varphi(f)$.

Proof. Consider the prime decompositions of $m$ and $n$

$$m = \prod_p p^{m_p}, \quad m_p \geq 0 \quad \text{and} \quad n = \prod_p p^{n_p}, \quad n_p \geq 0$$

where $p$ runs through the primes dividing $m$ or $n$. Then the prime decompositions of $d$ and $f$ are

$$d = \prod_p p^\min(m_p,n_p) \quad \text{and} \quad f = \prod_p p^\max(m_p,n_p).$$

This immediately shows i).

By the formula for Euler’s $\varphi$-function we have
\[ \varphi(m) = \prod_p \varphi(p^{m_p}) \quad \text{and} \quad \varphi(n) = \prod_p \varphi(p^{n_p}) \]

as well as

\[ \varphi(d) = \prod_p \varphi(p^{\min(m_p,n_p)}) \quad \text{and} \quad \varphi(f) = \prod_p \varphi(p^{\max(m_p,n_p)}) , \]

where we have defined \( \varphi(1) \) to be 1.

The above expressions for \( \varphi(m), \varphi(n), \varphi(d) \) and \( \varphi(f) \) immediately yield ii). □

**Lemma 4.22.** Let \( m \) be a positive integer and \( p \) a prime number. Then \( \varphi(mp) = \varphi(m) \iff m \) is odd and \( p = 2 \).

**Proof.** The "\( \Rightarrow \)" part is an immediate consequence of the formula for Euler's \( \varphi \)-function.

The "\( \Leftarrow \)" part: If \( p \) divides \( m \) the formula for Euler's \( \varphi \)-function shows that \( \varphi(mp) = \varphi(m) \cdot p \) which is \( \neq \varphi(m) \).

If \( p \) does not divide \( m \) the formula for Euler's \( \varphi \)-function shows that \( \varphi(mp) = \varphi(m) \cdot (p - 1) \) which is \( \neq \varphi(m) \) for \( p \neq 2 \). Hence \( m \) must be odd and \( p \) must be 2 if \( \varphi(mp) = \varphi(m) \). □

Euler's \( \varphi \)-function is not multiplicative in the sense that it unconditionally sends products into products, but it has the weaker property that \( \varphi(m) \) divides \( \varphi(n) \) if \( m \) divides \( n \). This follows either from the formula for Euler's \( \varphi \)-function or from the fact that the natural homomorphism from \( \mathbb{Z}/n^\ast \) to \( \mathbb{Z}/m^\ast \) is surjective when \( m \) divides \( n \). We formulate this as

**Lemma 4.23.** Let \( m \) and \( n \) be natural numbers. If \( m \) divides \( n \), then \( \varphi(m) \) divides \( \varphi(n) \).

**Lemma 4.24.** Let \( m \) and \( n \) be natural numbers. If \( m \mid n \), then \( \varphi(m) = \varphi(n) \), if and only if either \( m = n \) or \( m \) is odd and \( n = 2m \).

**Proof.** The "\( \text{if} \)" part is an immediate consequence of the formula for Euler's \( \varphi \)-function.

As for the "only if" part assume that \( m < n \) and \( m \) divides \( n \). Then \( n = mb \), where \( b > 1 \). Assume \( \varphi(m) = \varphi(n) \). If \( p \) is any prime divisor of \( b \) Lemma 4.23 implies \( \varphi(m) \mid \varphi(mp) \mid \varphi(mb) = \varphi(n) \), hence \( \varphi(m) = \varphi(mp) \). By Lemma 4.22 we see that \( m \) must be odd and \( p \) must be 2. Moreover, \( b/p \) cannot contain any prime divisor at all, hence \( b = p = 2 \) and \( n = 2m \). □
**Theorem 4.25.** Let $m$ and $n$ be positive integers and let $d$, resp. $f$, be the greatest common divisor of $m$ and $n$, resp. the least common multiple of $m$ and $n$. Then the compositum $Q_m Q_n = Q_f$ and the intersection $Q_m \cap Q_n = Q_d$.

**Proof.** By lemma 4.21 the greatest common divisor of $m$ and $n$ is $mn/f$, hence there exist integers $a$ and $b$ such that $am + bn = mn/f$ and thus $a/n + b/m = 1/f$. Therefore

$$(e^{2\pi i/n})^a(e^{2\pi i/m})^b = e^{2\pi i/f}$$

which implies that $Q_f$ is contained in the compositum $Q_m Q_n$. Since clearly $Q_m$ and $Q_n$ are contained in $Q_f$ it follows that $Q_m Q_n = Q_f$.

Clearly $Q_d \subseteq Q_m$ and $Q_d \subseteq Q_n$, hence $Q_d \subseteq Q_m \cap Q_n$.

The translation theorem (Theorem 3.46) applied on

$$Q_m \quad Q_m Q_n = Q_f \quad Q_m \cap Q_n \quad Q_n$$

yields

$$[Q_m : (Q_m \cap Q_n)] = [Q_f : Q_n] = \varphi(f)/\varphi(n) = \varphi(m)/\varphi(d)$$

where we have used Lemma 4.21 to obtain the last equality.

Therefore $[(Q_m \cap Q_n) : Q] = \varphi(d)$. Since $[Q_d : Q] = \varphi(d)$ this together with above inclusion $Q_d \subseteq Q_m \cap Q_n$ shows that $Q_m \cap Q_n = Q_d$. \hfill \Box

In view of Theorem 3.48 about the compositum of finite normal extensions Theorem 4.25 implies the following

**Corollary 4.26.** Let $n_1, \ldots, n_t$ be pairwise coprime natural numbers. If we set $n = n_1 \cdots n_t$ then $Q_n$ is the compositum of the fields $Q_{n_1}, \ldots, Q_{n_t}$ and $\text{Gal}(Q_n/Q)$ is isomorphic to the direct product $\text{Gal}(Q_{n_1}/Q) \times \cdots \times \text{Gal}(Q_{n_t}/Q)$. Moreover, if for each $i$, $1 \leq i \leq t$, $K_i$ is a subfield of $Q_{n_i}$ then the compositum $K_1 \cdots K_t$ is a normal extension of $Q$ whose Galois group is isomorphic to the direct product $\text{Gal}(K_1/Q) \times \cdots \times \text{Gal}(K_t/Q)$.

**Theorem 4.27.** Let $m \leq n$ be natural numbers. Then $Q_m = Q_n$ if and only if either $m = n$ or $m$ is odd and $n = 2m$.

**Proof.** Since $\varphi(m) = \varphi(2m)$ for any odd natural number $m$ the ”if” part is clear. Indeed, in this case $Q_m \subseteq Q_n$ and $[Q_{2m} : Q] = [Q_m : Q]$. 
As for the ”only if” part let \( d \), resp. \( f \), be the greatest common divisor of \( m \) and \( n \) resp. the least common multiple of \( m \) and \( n \). By the preceding theorem we conclude that \( \mathbb{Q}_d = \mathbb{Q}_m = \mathbb{Q}_n = \mathbb{Q}_f \). Since \( d \) divides \( f \) we deduce from \( [\mathbb{Q}_d : \mathbb{Q}] = \varphi(d) \) and \( [\mathbb{Q}_f : \mathbb{Q}] = \varphi(f) \) that \( \varphi(d) = \varphi(f) \). If \( m < n \), then \( d \) is a proper divisor of \( f \) and Lemma 4.24 implies that \( d \) is odd \( f = 2d \). From the equations \( 2d^2 = df = mn = d^2 \left( \frac{m}{d} \right) \left( \frac{n}{d} \right) \) it follows that \( \left( \frac{m}{d} \right) \left( \frac{n}{d} \right) = 2 \), hence \( \frac{m}{d} = 1 \) and \( \frac{n}{d} = 2 \), which implies that \( m \) is odd and \( n = 2m \).

It is now not hard to prove

**Theorem 4.28.** Let \( m \) and \( n \) be natural numbers. Then \( \mathbb{Q}_m \subseteq \mathbb{Q}_n \) if and only if either \( m \) divides \( n \) or \( m = 2u \) for some odd divisor \( u \) of \( n \).

**Proof.** The ”if” part follows from the previous theorem since \( \mathbb{Q}_{2u} = \mathbb{Q}_u \) for an odd \( u \) and \( \mathbb{Q}_u \subseteq \mathbb{Q}_n \) if \( u \) divides \( n \).

The ”only if” part: Let as usual \( d \) be the greatest common divisor of \( m \) and \( n \). From Theorem 4.25 we get \( \mathbb{Q}_d = \mathbb{Q}_m \). Since \( d \) divides \( m \) the previous theorem implies that either \( d = m \) or \( d \) is odd and \( m = 2d \). In the first case \( m \) must divide \( n \) and in the second case \( d \) is an odd divisor of \( n \), so that \( m = 2 \cdot \text{(an odd divisor of } n) \). \( \square \)

**Corollary 4.29.** \( \mathbb{Q}_n \) contains the number \( i (= \sqrt{-1}) \) if and only if \( 4 \) divides \( n \).

**THE DEGREES OF COS(2\( \pi/n \)) AND SIN(2\( \pi/n \)).

**The Degree of cos\( 2\pi/n \).**

Since \( \cos \frac{2\pi}{n} \) is rational for \( n = 1 \) or \( 2 \) we may restrict ourselves to the case where \( n > 2 \).

Consider the primitive \( n \)-th root of unity \( \varepsilon_n = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + isin \frac{2\pi}{n} \).

Clearly \( \mathbb{Q}(\cos \frac{2\pi}{n}) = \mathbb{Q}(\varepsilon_n + \varepsilon_n^{-1}) \), since \( 2\cos \frac{2\pi}{n} = \varepsilon_n + \varepsilon_n^{-1} \).

Let \( \tau \) be the automorphism (complex conjugation) sending \( \varepsilon_n \) to \( \varepsilon_n^{-1} \).

Obviously the fixed field \( \mathcal{F}(\tau) (= \mathbb{Q}_n \cap \mathbb{R}) \) contains the field \( \mathbb{Q}(\cos \frac{2\pi}{n}) \). Since \( \mathbb{Q}_n \) contains non-real numbers for \( n > 2 \), the automorphism \( \tau \) has order 2. The fundamental theorem of Galois theory implies that \([\mathbb{Q}_n : \mathcal{F}(\tau)] = 2 \).

Since \( \varepsilon_n \) is a root of the polynomial \( (x - \varepsilon_n)(x - \varepsilon_n^{-1}) = x^2 - 2\cos \frac{2\pi}{n} x + 1 \) having coefficients in \( \mathbb{Q}(\cos \frac{2\pi}{n}) \) it follows that \([\mathbb{Q}_n : \mathbb{Q}(\cos \frac{2\pi}{n})] = [\mathbb{Q}(\varepsilon_n) : \mathbb{Q}(\cos \frac{2\pi}{n})] \leq 2 \).

Because \( \mathcal{F}(\tau) \supseteq \mathbb{Q}(\cos \frac{2\pi}{n}) \) we conclude that \( \mathcal{F}(\tau) = \mathbb{Q}(\cos \frac{2\pi}{n}) \), hence \([\mathbb{Q}(\cos \frac{2\pi}{n}) : \mathbb{Q}] = \varphi(n)/2 \). In other words \( \cos \frac{2\pi}{n} \) is an algebraic number of degree \( \varphi(n)/2 \) for \( n > 2 \).

**The Degree of sin\( 2\pi/n \).**
As before we may assume that \( n > 2 \) since \( \sin \frac{2\pi}{n} \) is rational for \( n = 1 \) or 2.

We first determine the degree of \( \sin \frac{2\pi}{n} \). With the notations from above we have
\[
2 \sin \frac{2\pi}{n} = \varepsilon_n - \varepsilon_n^{-1}.
\]

Clearly \( \sin \frac{2\pi}{n} \) lies in \( \mathbb{Q}_n \). To find the degree of \( \sin \frac{2\pi}{n} \) we determine the automorphisms in \( \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \) that fix \( \varepsilon_n - \varepsilon_n^{-1} \).

Every automorphism of \( \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \) is of the form \( \sigma_a \) defined by
\[
\sigma_a(\varepsilon_n) = \varepsilon_n^a, \text{ where } 1 \leq a < n, (a, n) = 1.
\]

Here \( \sigma_a(\varepsilon_n - \varepsilon_n^{-1}) = \varepsilon_n - \varepsilon_n^{-1} \) if and only if \( \sin \frac{2\pi}{n} = \sin \frac{2\pi a}{n} \).

Now \( \sin x = \sin y \iff x - y \) is an integral multiple of \( 2\pi \) or \( x + y = \pi + \) an integral multiple of \( 2\pi \).

In our situation this means that \( \sin \frac{2\pi}{n} = \sin \frac{2\pi a}{n} \) if and only if either \( a = 1 \) or
\[
n \equiv a + \frac{2\pi}{n} \equiv \pi.
\]

The latter condition means that
\[
2(a + 1) = n \tag{(*)}
\]

If \( n \) is odd (\(*\)) has no solutions in \( a \).

If \( n = 2 \) (an odd number) a solution of (\(*\)) in \( a \) must be even, so \( (a, n) > 1 \).

Therefore, if \( n \) is not divisible by 4, \( \sigma_1 \) is the only automorphism fixing \( \varepsilon_n - \varepsilon_n^{-1} \), hence \( \mathbb{Q}(\sin \frac{2\pi}{n}) = \mathbb{Q}_n \) and the degree of \( \sin \frac{2\pi}{n} \) is \( \varphi(n) \).

By Corollary 4.29 \( \mathbb{Q}_n = \mathbb{Q}(\sin \frac{2\pi}{n}) \) does not contain \( i \) when \( n \) is not divisible by 4. We conclude from Example 3.50 (Chap. III) that the degree of \( \sin \frac{2\pi}{n} \) is \( \varphi(n) \).

If \( n \) is divisible by 4 we first discard the case \( n = 4 \): Here \( \sin \frac{2\pi}{4} = i \) has the degree 2 and \( \sin \frac{2\pi}{4} = 1 \) has degree 1.

So we now assume \( n > 4 \) and \( n \) is divisible by 4.

If \( n \) is divisible by 4 the equation (\(*\)) has exactly one solution in \( a \), where \( 1 \leq a < n, (a, n) = 1 \), namely \( a = \frac{n}{2} - 1 \). Since \( n > 4 \), \( a = \frac{n}{2} - 1 \neq 1 \). Thus \( \sigma_1 \) and \( \sigma_{\frac{n}{2} - 1} \) are the only automorphisms fixing \( \varepsilon_n - \varepsilon_n^{-1} \). Hence \( [\mathbb{Q}_n : \mathbb{Q}(\sin \frac{2\pi}{n})] = 2 \), so the degree of \( \sin \frac{2\pi}{n} \) is \( \varphi(n)/2 \).

\( \mathbb{Q}_n \) contains \( i \) when \( n \) is divisible by 4. In view of Example 3.50 (Chap. III), to find the degree of \( \sin \frac{2\pi}{n} \) we have to determine the values of \( n \) for which \( i \) lies in \( \mathbb{Q}(\sin \frac{2\pi}{n}) \). This boils down to finding the \( n \)'s for which \( \mathbb{Q}(i) \subseteq \mathbb{Q}(\sin \frac{2\pi}{n}) \). By the main theorem of Galois theory this is equivalent to finding the \( n \)'s for which \( T(\mathbb{Q}(i)) \supseteq T(\mathbb{Q}(\sin \frac{2\pi}{n})) \). We know that \( T(\mathbb{Q}(\sin \frac{2\pi}{n})) = \{\sigma_1, \sigma_{\frac{n}{2} - 1}\} \). Since
\[
\sigma_{\frac{n}{2} - 1}(i) = \sigma_{\frac{n}{2} - 1}(\varepsilon_n) = \varepsilon_n^{\frac{n}{2} - 1} = i \frac{n}{2} - 1
\]
the automorphism \( \sigma_{\frac{n}{2} - 1} \) fixes \( i \) exactly if
\[
n \equiv 1 \pmod{4} \iff n - 2 \equiv 2 \pmod{8} \iff n \equiv 4 \pmod{8}.
\]
Consequently, if \( n \equiv 4 \pmod{8} \), then \( i \) lies in \( \mathbb{Q}(isin\frac{2\pi}{n}) \) and therefore (by Example 3.50, Chap. III) the degree of \( sin\frac{2\pi}{n} \) is \( \frac{\varphi(n)}{2} \).

If, however, \( n \equiv 0 \pmod{8} \) then \( i \) does not lie in \( \mathbb{Q}(isin\frac{2\pi}{n}) \) and therefore (by Example 3.50, Chap III) \( sin\frac{2\pi}{n} \) and \( isin\frac{2\pi}{n} \) have the same degree, namely \( \varphi(n)/2 \).

Let us summarize the above results in the following

**Theorem 4.30.** Apart from the degenerate cases \( n = 1, 2 \) or \( 4 \), then:
- \( cos\frac{2\pi}{n} \) has the degree \( \varphi(n)/2 \) for all \( n \).
- \( sin\frac{2\pi}{n} \) has the degree \( \varphi(n) \) if \( n \) is not divisible by 4.
- \( sin\frac{2\pi}{n} \) has the degree \( \varphi(n)/2 \) if \( n \equiv 0 \pmod{8} \).
- \( sin\frac{2\pi}{n} \) has the degree \( \varphi(n)/4 \) if \( n \equiv 4 \pmod{8} \).

**Exercise 4.31.** Show that \( \mathbb{Q}(sin\frac{2\pi}{n}) \subseteq \mathbb{Q}(cos\frac{2\pi}{n}) \) if and only if \( n = 1, 2 \) or \( n \equiv 0 \pmod{4} \).

Show that \( \mathbb{Q}(sin\frac{2\pi}{n}) = \mathbb{Q}(cos\frac{2\pi}{n}) \) if and only if \( n = 1, 2, 4 \) or \( n \equiv 0 \pmod{8} \).
CONSTRUCTION OF REGULAR POLYGONS BY COMPASS AND STRAIGHTEDGE.

In this section we use cyclotomic fields to answer some classical problems dating back to Euclid.

These problems concern the construction of one geometrical segment from another, using only an (unmarked) straightedge and a (collapsible) compass.

With the straightedge we can draw the line through through two given points and with the compass we can draw the circle with a given point as centre and a given radius.

We assume that we have a starting figure in the real Euclidean plane, consisting of the points $(0, 0)$ and $(1, 0)$. A point is called \textit{constructible}, if it can be obtained from the starting figure by successive applications of the following operations:

1) draw the straight line through two given or already constructed points.
2) draw the circle with a given or already constructed point as its centre and the distance between two given or already constructed points as its radius.
3) Add intersection points between two constructed straight lines, between a constructed straight line and a constructed circle or between two constructed circles.

By straightforward computation one shows

\textbf{Theorem 4.32.} Assume a construction successively give the following points $P_0 = (0, 0), P_1 = (1, 0), P_2, P_3, \ldots, P_n, P_{n+1}, \ldots$. If the coordinates of $P_0, P_1, \ldots, P_n$ belong to some real number field $K$ the coordinates of $P_{n+1}$ either belong to $K$ or a number field of the form $K(\sqrt{d})$, where $d$ is a positive real number which is not the square of a number in $K$.

\textbf{Definition 4.33.} A complex number $a + ib$ is called \textit{constructible}, if the point $(a, b)$ is constructible according to the above definition.

Theorem 4.32 then yields:

\textbf{Theorem 4.34.} For every complex constructible number $z$ there exists a sequence of quadratic extensions $K = \mathbb{Q}, K_1 = \mathbb{Q}(i), (i = \sqrt{-1}), K_2 = K_1(\sqrt{d_1}), (d_1 \in K_1), K_3 = K_2(\sqrt{d_2}), (d_2 \in K_2), \ldots, K_t = K_{t-1}(\sqrt{d_{t-1}}), (d_{t-1} \in K_{t-1})$, such that $z \in K_t$.

Since we may assume that $K_1 \nsubseteq K_2 \nsubseteq K_3$ etc., the dimension $[K_t : \mathbb{Q}]$ (by the transitivity theorem, Theorem 2.47 in Chap. II) is $2^t$. This implies (again using the transitivity theorem, Theorem 2.47 in Chap. II):

\[ z \text{ constructible number } \Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] \text{ is a power of } 2. \]
Furthermore classical constructions (formerly known from high school mathematics) show

**Theorem 4.35.** The set of all constructible complex numbers is a field \( K \) closed under formation of square roots (i.e. \( \alpha \in K \Rightarrow \sqrt{\alpha} \in K \)).

**Definition 4.36.** The regular \( n \)-gon is called constructible, if \( e^{\frac{2\pi i}{n}} \) is a constructible number.

It was known already to Euclid that a regular \( n \)-gon is constructible if and only if \( 2^k+1 \) is a prime number, \( k \) is necessarily a power of 2. Indeed, otherwise \( k = u \cdot s \), \( u \) being an odd number \( > 1 \), and: \( 2^k+1 = (2^s)^u+1 = (2^s)^u - (-1)^u = (2^s - (-1)). \) In other words \( 2^s + 1 \) divides \( 2^k + 1 \). Since \( u > 1 \) the number \( s \) is \( < k \). Hence \( 2^s + 1 \) is a non-trivial divisor of \( 2^k + 1 \), which thus cannot be a prime number.

**Remark 4.38.** If \( 2k+1 \) is a prime number, \( k \) is necessarily a power of 2. Indeed, otherwise \( k = u \cdot s \), \( u \) being an odd number \( > 1 \), and: \( 2^k+1 = (2^s)^u+1 = (2^s)^u - (-1)^u = (2^s - (-1)). \) In other words \( 2^s + 1 \) divides \( 2^k + 1 \). Since \( u > 1 \) the number \( s \) is \( < k \). Hence \( 2^s + 1 \) is a non-trivial divisor of \( 2^k + 1 \), which thus cannot be a prime number.

**Proof of Gauss’ theorem.** Since the regular \( n \)-gon is constructible if and only if the regular \( 2n \)-gon is constructible (“bisection of angles”) it suffices to show Gauss’ theorem for an odd number \( n \).

“\( \Rightarrow \)” Every odd number \( n \) is a power of 2. Indeed, otherwise \( k = u \cdot s \), \( u \) being an odd number \( > 1 \), and: \( 2^k+1 = (2^s)^u+1 = (2^s)^u - (-1)^u = (2^s - (-1)). \) In other words \( 2^s + 1 \) divides \( 2^k + 1 \). Since \( u > 1 \) the number \( s \) is \( < k \). Hence \( 2^s + 1 \) is a non-trivial divisor of \( 2^k + 1 \), which thus cannot be a prime number.

“\( \Leftarrow \)” If \( n \) has the form indicated in the theorem the computation in the first half of the proof shows that \( |\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}| \) is a power of 2. The Galois group \( G = \text{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}) \) is then an abelian 2-group. In particular, \( G \) is solvable so that the factors in a
composition series \( G \supset G_1 \supset G_2 \supset \cdots \supset G_k = \{e\} \) are cyclic of order 2, (a well-known theorem in group theory): \([G : G_1] = [G_1 : G_2] = \cdots = [G_{k-1} : G_k] = 2\).

We have the following situation:

\[
\begin{array}{c|c}
G_k = \{e\} & \mathcal{F}(G_k) = \mathbb{Q}_n \\
2 & 2 \\
G_{k-1} & \mathcal{F}(G_{k-1}) \\
2 & 2 \\
& \vdots \\
2 & 2 \\
G_2 & \mathcal{F}(G_2) \\
2 & 2 \\
G_1 & \mathcal{F}(G_1) \\
2 & 2 \\
G & \mathcal{F}(G) = \mathbb{Q}
\end{array}
\]

\( \mathcal{F}(G_1) \) is a quadratic extension of \( \mathcal{F}(G) \) and therefore (by Lemma 4.19) obtainable by adjunction of the square root of a number in \( \mathcal{F}(G) \). Furthermore \( \mathcal{F}(G_2) \) is a quadratic extension of \( \mathcal{F}(G_1) \) and therefore obtainable by adjunction of the square root of a number in \( \mathcal{F}(G_1) \) etc.

Since the field \( \mathcal{K} \) of the constructible numbers is closed under formation of square roots (Theorem 4.35) and the rational numbers are constructible, it follows that \( \mathbb{Q}_n \) is contained in \( \mathcal{K} \). In particular \( e^{2\pi i n} \) lies in the field of constructible numbers. \( \square \)

**Remark 4.39 concerning the prime numbers appearing in Gauss’ theorem.** These prime numbers are called the *Fermat prime numbers*. \( 2^1 + 1 = 3, 2^2 + 1 = 5, 2^4 + 1 = 17, 2^8 + 1 = 257, 2^{16} + 1 = 65537 \) are Fermat prime numbers. More Fermat prime number than those are not known. (A criterion for \( 2^{2^n} + 1 \) to be a prime number can be found in Chap. VI:)

**Remark 4.40 about the ”trisection of an arbitrary angle”.** From Gauss’ theorem it in particular follows that a regular 9-gon cannot be constructed by compass and straightedge. This gives a negative solution of the classical problem whether every angle can be trisected by compass and straightedge.
AN APPLICATION TO THE ‘INVERSE PROBLEM OF GALOIS THEORY’.

We conclude this chapter by yet another application of cyclotomic fields. It is a famous problem (dating back to Hilbert (1892)), whether every finite group can be realized as the Galois group of a finite normal extension of the rational number field $\mathbb{Q}$. This problem, the inverse problem of Galois theory, is still unsolved and has a central place in current research in Galois theory.

We shall here prove, that every finite abelian group can be realized as a Galois group over $\mathbb{Q}$.

We first deal with the cyclic case.

**Theorem 4.41.** Let $\mathbb{Z}_n$ be the cyclic group of order $n$ and let $p$ be a prime number such that $p \equiv 1 \pmod{n}$. Then there exists a subfield of $\mathbb{Q}_p$ which is normal over $\mathbb{Q}$ with $\mathbb{Z}_n$ as its Galois group.

**Proof.** Since $\text{Gal}(\mathbb{Q}_p/\mathbb{Q}) \simeq \mathbb{Z}_p^* \simeq (\mathbb{Z}_{p-1}, +)$ there exists a (uniquely determined) subgroup $H$ of $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})$ of order $\frac{p-1}{n}$. The fixed field $F(H)$ is according to the fundamental theorem of Galois theory a normal extension of $\mathbb{Q}$ with $\text{Gal}(\mathbb{Q}_p/\mathbb{Q})/H \simeq \mathbb{Z}_n^*$ as its Galois group. \[\square\]

We are now in a position to prove

**Theorem 4.42.** Every finite abelian group can be realized as the Galois group for a finite normal extension of $\mathbb{Q}$.

**Proof.** Let $A$ be a finite abelian group. By a well-known theorem $A$ is a direct product of cyclic groups

$$A \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}.$$

By the earlier proved special case of Dirichlet’s theorem about prime numbers in arithmetic progressions there exist distinct prime numbers $p_1, \ldots, p_t$ such that

$$p_1 \equiv 1 \pmod{n_1}, \quad p_2 \equiv 1 \pmod{n_2}, \ldots, \quad p_t \equiv 1 \pmod{n_t}.$$

By Theorem 4.41 there are subfields of $K_1 \subseteq \mathbb{Q}_{p_1}$, $K_2 \subseteq \mathbb{Q}_{p_2}$, ..., $K_t \subseteq \mathbb{Q}_{p_t}$ which are normal over $\mathbb{Q}$ and

$$\text{Gal}(K_1/\mathbb{Q}) \simeq \mathbb{Z}_{n_1}, \quad \text{Gal}(K_2/\mathbb{Q}) \simeq \mathbb{Z}_{n_2}, \ldots, \quad \text{Gal}(K_t/\mathbb{Q}) \simeq \mathbb{Z}_{n_t}.$$

Combining the above theorem, Corollary 4.26 and Corollary 3.48 we conclude that $K_1K_2\ldots K_t$ is normal over $\mathbb{Q}$ and

$$\text{Gal}(K_1K_2\ldots K_t/\mathbb{Q}) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} \simeq A.$$

\[\square\]