The theory of cyclotomy is concerned with the problem of dividing the perimeter of a circle into a given number of equal parts (cyclo-tomy means: circle-division). Consider the unit circle in the complex plane. The points dividing this unit circle into \( n \) equal parts are the points 
\[
e^{2\pi i/n} = \cos \left( \frac{2\pi}{n} \right) + i \sin \left( \frac{2\pi}{n} \right)
\]
and the geometric problem of cyclotomy is equivalent to studying the fields \( \mathbb{Q}(e^{2\pi i/n}) \subseteq \mathbb{C} \). The complex numbers \( e^{2\pi i/n} \) are roots of the polynomial \( x^n - 1 \) and \( \mathbb{Q}(e^{2\pi i/n}) \) is a splitting field of \( x^n - 1 \). The splitting fields of such polynomials over any field \( K \) will be called cyclotomic fields (although they may not be relevant to the geometric problem of circle division).

**58.1 Definition:** Let \( K \) be a field and \( 1 \in K \) the identity element of \( K \). Let \( n \in \mathbb{N} \). An extension field \( E \) of \( K \) is called a **cyclotomic extension of \( K \) (of order \( n \))** if \( E \) is a splitting field of \( x^n - 1 \in K[x] \) over \( K \).

**58.2 Definition:** Let \( K \) be a field. A root of the polynomial \( x^n - 1 \in K[x] \) is called an **\( n \)-th root of unity** or, if there is no need to be exact, simply a **root of unity**.

**58.3 Lemma:** Let \( K \) be a field of characteristic \( p \neq 0 \) and let \( n \in \mathbb{N} \), where \( n = p^a m \) and \( (p,m) = 1 \). Let \( u \) be an element in an extension field of \( K \). Then \( u \) is an \( n \)-th root of unity if and only if \( u \) is an \( m \)-th root of unity.

**Proof:** If \( u \) is an \( m \)-th root of unity, then \( u^m = 1 \), so \( u^n = (u^m)^{p^a} = 1^{p^a} = 1 \) and \( u \) is an \( n \)-th root of unity. If \( u \) is an \( n \)-th root of unity, then \( 0 = u^n - 1 = (u^m)^{p^a} - 1 = (u^m - 1)^{p^a} \), so \( u^m - 1 = 0 \) and \( u \) is an \( m \)-th root of unity.

\( \square \)
So in the situation of Lemma 58.3, a splitting field of $x^n - 1$ over $K$ is also a splitting field of $x^m - 1$ over $K$, and conversely. For this reason, in case $\text{char } K \neq 0$, it is no loss of generality to assume that the order of a cyclotomic extension is relatively prime to the characteristic of $K$.

58.4 Lemma: Let $K$ be a field and $E$ an extension field of $K$ containing all $n$-th roots of unity. Assume $\text{char } K = 0$ or $(\text{char } K, n) = 1$. Then the set of all $n$-th roots of unity is a cyclic group of order $n$ under multiplication.

Proof: If $u$ and $t$ are $n$-th roots of unity, then $(ut)^n = u^n t^n = 1 \cdot 1 = 1$ and $ut$ is also an $n$-th root of unity. Since the number of $n$-th roots of unity is at most $n$ (Theorem 35.7), it follows that the set of all $n$-th roots of unity is a subgroup of $K^\times$ (Lemma 9.3(1)). This group of $n$-th roots of unity is cyclic by Theorem 52.18. To prove that the order of this group is equal to $n$, we must only show that all roots of $x^n - 1$ are simple. This follows from the fact that the derivative $nx^{n-1}$ of $x^n - 1$ is distinct from zero (because of the assumption $\text{char } K = 0$ or $(\text{char } K, n) = 1$) so that $x^n - 1$ and $nx^{n-1}$ have no common root. □

58.5 Definition: Let $K$ be a field and $E$ an extension field of $K$ containing all $n$-th roots of unity. Assume $\text{char } K = 0$ or $(\text{char } K, n) = 1$. A generator of the cyclic group of all $n$-th roots of unity is called a primitive $n$-th root of unity.

$\zeta$ is a primitive $n$-th root of unity if and only if $o(\zeta) = n$. If $\zeta$ is a primitive $n$-th root of unity, then all $n$-th roots of unity are given without duplication in the list

$$1 = \zeta_0, \zeta_1, \zeta_2, \zeta_3, \ldots, \zeta_{n-1}$$

or in the list

$$\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}, \zeta^n = 1$$

and $\zeta^j$ has order $n/(n,j)$ (Lemma 11.9(2)). Hence $\zeta^j$ is a primitive $n$-th root of unity if and only if $(n,j) = 1$. There are therefore $\varphi(n)$ primitive $n$-th roots of unity (cf. §11).
If \( u \) is a root of unity and \( o(u) = d \), then, by definition, \( u \) is a primitive \( d \)-th root of unity.

1 is a primitive first root of unity, \(-1 \in \mathbb{C}\) is a primitive second root of unity, \( \omega \in \mathbb{C} \) and \( \omega^2 \) are primitive third roots of unity, \( i \in \mathbb{C} \) and \(-i \in \mathbb{C} \) are primitive fourth roots of unity.

**58.6 Definition:** Let \( K \) be a field and \( n \in \mathbb{N} \). Assume that \( \text{char} \ K = 0 \) or \( (\text{char} \ K, n) = 1 \). Let \( \zeta \) be a primitive \( n \)-th root of unity and
\[
\{ \zeta_1, \zeta_2, \ldots, \zeta_{\varphi(n)} \} = \{ \zeta^j : j = 1,2, \ldots, n \text{ and } (n,j) = 1 \}
\]
the set of all primitive \( n \)-th roots of unity in some extension field of \( K \). The monic polynomial
\[
(x - \zeta_1)(x - \zeta_2)\cdots(x - \zeta_{\varphi(n)})
\]
of degree \( \varphi(n) \) is called the \( n \)-th cyclotomic polynomial over \( K \) and is denoted by \( \Phi_n(x) \).

For example, over \( \mathbb{Q} \), the first few cyclotomic polynomials are
\[
\begin{align*}
\Phi_1(x) &= x - 1, & \Phi_2(x) &= x - (-1) = x + 1, \\
\Phi_3(x) &= (x - \omega)(x - \omega^2) = x^2 + x + 1, & \Phi_4(x) &= (x - i)(x + i) = x^2 + 1.
\end{align*}
\]
We see that these are in fact polynomials in \( \mathbb{Z}[x] \). This is true for any cyclotomic polynomial. The \( n \)-th cyclotomic polynomial over \( K \) does not depend on the extension field of \( K \) in which the primitive \( n \)-th roots of unity are assumed to lie. In fact, it does not even depend on \( K \) (but only on \( \text{char} \ K \)).

**58.7 Lemma:** Let \( K \) be a field, \( n \in \mathbb{N} \) and assume that \( \text{char} \ K = 0 \) or \( (\text{char} \ K, n) = 1 \). Then
\[
(1) \ x^n - 1 = \prod_{d | n} \Phi_d(x).
\]
(2) \( \Phi_n(x) \in \mathbb{Z}[x] \) if \( \text{char} \ K = 0 \) and \( \Phi_n(x) \in \mathbb{Z}_p[x] = \mathbb{F}_p[x] \) if \( \text{char} \ K = p \neq 0 \).

**Proof:** (1) Any root \( u \) of \( x^n - 1 \) is an \( n \)-th root of unity and \( o(u) = d \) for some divisor of \( n \). Then \( u \) is a primitive \( d \)-th root of unity. Conversely, if \( d | n \), any primitive \( d \)-th root of unity is an \( n \)-th root of unity with \( o(u) = \ldots \)
Thus $\Phi_d(x) = \prod_{\substack{u^d = 1 \\ o(u) = d}} (x - u)$. Collecting together the roots of $x^n - 1$ with order $d$, for each divisor $d$ of $n$, we get

$$x^n - 1 = \prod_{u^d = 1} (x - u) = \prod_{d|n} \prod_{\substack{u^d = 1 \\ o(u) = d}} (x - u) = \prod_{d|n} \Phi_d(x).$$

(2) Let $D = \mathbb{Z}$ in case $\text{char } K = 0$ and $D = \mathbb{Z}_p = \mathbb{F}_p$ in case $\text{char } K = p \neq 0$. We prove $\Phi_n(x) \in D[x]$ by induction on $n$. Since $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$, we have $\Phi_n(x) \in D[x]$ when $n = 1, 2$.

Suppose now $n \geq 3$ and that $\Phi_d(x) \in D[x]$ for all $d = 1, 2, \ldots, n - 1$. From (1), we have $x^n - 1 = \Phi_n(x) \prod_{d|n} \Phi_d(x)$. Let us put $f(x) = \prod_{d|n} \Phi_d(x)$. Then $f(x)$ is a monic polynomial and $f(x) \in D[x]$ since, by induction, $\Phi_d(x) \in D[x]$ for all divisors $d$ of $n$ which are distinct from $n$. As $x^n - 1 \in D[x]$ and $f(x)$ is monic, there are unique polynomials $q(x)$ and $r(x)$ in $D[x]$ such that

$$x^n - 1 = q(x)f(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg f(x)$$

(Theorem 34.4). Now let $E$ be an extension field of $K$ containing all roots of $x^n - 1$. The division algorithm in $E[x]$ reads

$$x^n - 1 = \Phi_n(x)f(x) + 0.$$

Since $D \subseteq K \subseteq E$ and the quotient and remainder are uniquely determined, the unique quotient $q(x)$ in $D[x]$ must be the unique quotient $\Phi_n(x)$ in $E[x]$ and the unique remainder $r(x)$ in $D[x]$ must be the unique remainder 0 in $E[x]$. Hence $\Phi_n(x) = q(x) \in D[x]$. This completes the proof. \hfill \Box

The equation $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}$ is a recursive formula for $\Phi_n(x)$. Thus

$$\Phi_6(x) = x^6 - 1/\Phi_1(x)\Phi_2(x)\Phi_3(x)$$

$$= x^6 - 1/(x - 1)(x + 1)(x^2 + x + 1) = x^2 - x + 1.$$

Another recursive formula is for $\Phi_n(x)$ is given in the next lemma.
58.8 Lemma: Let $K$ be a field, $n \in \mathbb{N}$ and assume that char $K = 0$ or $(\text{char } K, n) = 1$. Then

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}.$$

Proof: This follows immediately from Lemma 58.7(1) and Lemma 52.14 (in Lemma 52.14, let the field be $K(x)$ and let the function $F: \mathbb{N} \to K(x)^x$ be $n \to \Phi_n(x)$).

For example, we have, over $\mathbb{Q}$:

$$\Phi_{12}(x) = (x^{12} - 1)^{\mu(1)}(x^6 - 1)^{\mu(2)}(x^4 - 1)^{\mu(3)}(x^3 - 1)^{\mu(4)}(x^2 - 1)^{\mu(6)}(x - 1)^{\mu(12)} = (x^{12} - 1)(x^2 - 1)/(x^6 - 1)(x^4 - 1) = x^4 - x^2 + 1,$$

$$\Phi_{15}(x) = (x^{15} - 1)^{\mu(1)}(x^5 - 1)^{\mu(3)}(x^3 - 1)^{\mu(5)}(x - 1)^{\mu(15)} = (x^{15} - 1)(x - 1)/(x^5 - 1)(x^3 - 1) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

58.10 Theorem: Let $K$ be a field, $n \in \mathbb{N}$ and assume that char $K = 0$ or $(\text{char } K, n) = 1$. Let $E$ be a cyclotomic extension of order $n$ and let $\zeta \in E$ be a primitive $n$-th root of unity and let $f(x) \in K[x]$ be the minimal polynomial of $\zeta$ over $K$. Then

1. $E = K(\zeta)$;
2. $E$ is Galois over $K$;
3. $|\text{Aut}_K E|$ divides $\varphi(n)$ and $\text{Aut}_K E$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$;
4. $\text{Aut}_K E \cong \mathbb{Z}_n^* \iff |\text{Aut}_K E| = \varphi(n) \iff f(x) = \Phi_n(x)$
   $\iff \Phi_n(x)$ is irreducible in $K[x]$.

Proof: (1) Let $a_1, a_2, \ldots, a_k$ be the natural numbers less than $n$ and relatively prime to $n$ (where $k = \varphi(n)$), so that $\zeta^{a_1}, \zeta^{a_2}, \ldots, \zeta^{a_k}$ are the roots of $\Phi_n(x)$. Now $E$ is a splitting field of $\Phi_n(x)$ by definition, so $E$ is generated by the roots of $\Phi_n(x)$ over $K$ (Example 53.5(d)) and $E = K(\zeta^{a_1}, \zeta^{a_2}, \ldots, \zeta^{a_k}) = K(\zeta)$. 

744
(2) The roots of $\Phi_n(x)$ are simple because $\Phi_n(x)$ is a divisor of $x^n - 1$ and the roots of $x^n - 1$ are simple (the derivative of $x^n - 1$, being distinct from 0 since $\text{char } K = 0$ or $(\text{char } K,n) = 1$, is relatively prime to $x^n - 1$). So the irreducible factors of $\Phi_n(x)$ are separable over $K$. Since $E$ is a splitting field of $\Phi_n(x)$, Theorem 55.7 shows that $E$ is Galois over $K$.

(3) Since $\zeta$ is a root of $\Phi_n(x) \in K[x]$ and $f(x)$ is the minimal polynomial of $\zeta$ over $K$, we see $f(x)$ divides $\Phi_n(x)$ in $K[x]$ and the roots of $f(x)$ are certain of the roots of $\Phi_n(x)$. Let $\deg f(x) = s$ and $\zeta^{m_1}, \zeta^{m_2}, \ldots, \zeta^{m_s}$ be the roots of $f(x)$, where $m_1, m_2, \ldots, m_s$ are some suitable natural numbers relatively prime to $n$ and less than $n$ and $m_1 = 1$, say. Thus

$$f(x) = (x - \zeta^{m_1})(x - \zeta^{m_2}) \ldots (x - \zeta^{m_s}).$$

Here we have $|\text{Aut}_K E| = |E:K| = |K(\zeta):K| = \deg f(x) = s$ because $E$ is Galois over $K$. Any $K$-automorphism of $E$ maps $\zeta$ to one of $\zeta^{m_1}, \zeta^{m_2}, \ldots, \zeta^{m_s}$. Let $\alpha_{m_i}$ be the $K$-automorphism $\zeta \to \zeta^{m_i} (i = 1, 2, \ldots, s)$. Since

$$\alpha_{m_i} = \alpha_{m_j} \iff \zeta^{m_i} = \zeta^{m_j} \iff m_i \equiv m_j \mod n \iff i = j,$$

$\alpha_{m_1}, \alpha_{m_2}, \ldots, \alpha_{m_s}$ are pairwise distinct and $\text{Aut}_K E = \{\alpha_{m_1}, \alpha_{m_2}, \ldots, \alpha_{m_s}\}$.

Let $m_i^*$ be the residue class of $m_i$ in $\mathbb{Z}_n$. Since $m_i$ and $n$ are relatively prime, there holds $m_i^* \in \mathbb{Z}_n^\times$. We put $G = \{m_1^*, m_2^*, \ldots, m_s^*\} \subseteq \mathbb{Z}_n^\times$. Consider the mapping

$$\alpha: G \to \text{Aut}_K E,$$

$$m_i^* \to \alpha_{m_i}.$$

As $\alpha_{m_i} = \alpha_{m_j} \iff m_i^* = m_j^*$, the mapping $\alpha$ is well defined and one-to-one. Both $G$ and $\text{Aut}_K E$ have $s$ elements, so $\alpha$ is also onto $\text{Aut}_K E$. Then $\alpha$ has an inverse $\beta$:

$$\beta: \text{Aut}_K E \to G \subseteq \mathbb{Z}_n^\times,$$

$$\alpha_{m_i} \to m_i^*.$$

Suppose $\alpha_{m_i} \alpha_{m_j} = \alpha_{m_k}$. Then

$$\zeta^{m_i} = \zeta \alpha_{m_i} = \zeta \alpha_{m_j} \alpha_{m_j} = (\zeta \alpha_{m_j}) \alpha_{m_j} = (\zeta \alpha_{m_j}) \alpha_{m_j} (\zeta \alpha_{m_j})^{-m_i} \alpha_{m_j} = (\zeta \alpha_{m_j})^{-m_i} \alpha_{m_j} = \zeta^{m_i} \alpha_{m_j},$$

so $m_k \equiv m_i m_j \mod n$, so $m_i^* m_j^* = m_k^*$ and therefore

745
\( (\alpha_m \circ \alpha_n) \beta = (\alpha_m) \beta = m_k^* = m_i^* m_j^* = (\alpha_m) \beta (\alpha_n) \beta. \)

Hence \( \beta: \text{Aut}_K E \to \mathbb{Z}_n^* \) is a one-to-one group homomorphism, and \( \text{Im} \ \beta = G \) is a subgroup of \( \mathbb{Z}_n^* \) and \( \beta \) is an isomorphism from \( \text{Aut}_K E \) onto \( G \). This proves that \( \text{Aut}_K E \) is isomorphic to a subgroup of \( \mathbb{Z}_n^* \). It follows from Lagrange's theorem that \( |\text{Aut}_K E| = |G| \) divides \( |\mathbb{Z}_n^*| = \varphi(n) \).

(4) Since \( \text{Aut}_K E \) is isomorphic to a subgroup of \( \mathbb{Z}_n^* \) and \( |\mathbb{Z}_n^*| = \varphi(n) \) is finite, we have the equivalence \( \text{Aut}_K E \cong \mathbb{Z}_n^* \iff |\text{Aut}_K E| = \varphi(n) \).

We have \( |\text{Aut}_K E| = \deg f(x) \) and \( \varphi(n) = \deg \Phi_n(x) \). Now \( f(x) \) divides \( \Phi_n(x) \) in \( K[x] \) and both \( f(x) \) and \( \Phi_n(x) \) are monic, so \( f(x) = \Phi_n(x) \) if and only if \( \deg f(x) = \deg \Phi_n(x) \), so if and only if \( |\text{Aut}_K E| = \varphi(n) \).

Finally, since \( \Phi_n(x) \) is monic and \( \zeta \) is a root of \( \Phi_n(x) \), irreducibility of \( \Phi_n(x) \) in \( K[x] \) implies that \( \Phi_n(x) \) is the minimal polynomial of \( \zeta \) over \( K \), i.e., that \( f(x) = \Phi_n(x) \). Conversely, if \( f(x) = \Phi_n(x) \), then \( \Phi_n(x) \) is irreducible. \( \square \)

When the base field is \( \mathbb{Q} \), we have sharper results.

**58.11 Theorem:** For any \( n \in \mathbb{N} \), the \( n \)-th cyclotomic polynomial \( \Phi_n(x) \) over \( \mathbb{Q} \) is irreducible in \( \mathbb{Z}[x] \).

**Proof:** Let \( n \in \mathbb{N} \) and let \( g(x) \) be an irreducible divisor of \( \Phi_n(x) \) in \( \mathbb{Z}[x] \), with \( \deg g(x) \geq 1 \) so that \( \Phi_n(x) = g(x)h(x) \), say, where \( g(x), h(x) \in \mathbb{Z}[x] \) are monic polynomials. Let \( \zeta \) be a root of \( g(x) \). Thus \( g(x) \) is the minimal polynomial of \( \zeta \) over \( \mathbb{Q} \).

Our first step will be to show that \( \zeta^p \) is also a root of \( g(x) \) for any prime number \( p \) relatively prime to \( n \). Now \( \zeta \) is a root of \( \Phi_n(x) \), so \( o(\zeta) = \varphi(n) \) and if \( p \) is a prime number such that \( (p,n) = 1 \), then \( o(\zeta^p) = \varphi(n) \) and \( \zeta^p \) is also a primitive \( n \)-th root of unity: \( \zeta^p \) is a root of \( \Phi_n(x) \), so \( \zeta^p \) is a root of \( g(x) \) or of \( h(x) \). Let us assume, by way of contradiction, that \( \zeta^p \) is not a root of \( g(x) \). Then \( \zeta^p \) is a root of \( h(x) \). Then \( \zeta \) is a root of \( h(x^p) \) and \( h(x^p) \) is divisible by the minimal polynomial \( g(x) \) of \( \zeta \) over \( \mathbb{Q} \).

Let us write \( h(x^p) = g(x)p(x) \), where \( p(x) \in \mathbb{Q}[x] \). Let
\[ h(x^p) = g(x)q(x) + r(x), \quad r(x) = 0 \text{ or } \deg r(x) < \deg g(x) \]

be the division algorithm in \( \mathbb{Z}[x] \) (\( g(x) \) is monic). The uniqueness of the quotient and remainder in \( \mathbb{Z}[x] \triangleq \mathbb{Q}[x] \) implies \( p(x) = q(x) \) and \( r(x) = 0 \). Thus we have \( h(x^p) = g(x)p(x) \), where \( p(x) \in \mathbb{Z}[x] \).

Let \( \nu: \mathbb{Z} \to \mathbb{F}_p \) be the natural homomorphism and let \( \hat{\nu}: \mathbb{Z}[x] \to \mathbb{F}_p[x] \) be the homomorphism of Lemma 33.7. We shall write \( \overline{s}(x) \) instead of \( (s(x))\hat{\nu} \) for \( s(x) \in \mathbb{Z}[x] \). Then \( h(x^p) = g(x)p(x) \) implies

\[
\overline{h}(x^p) = \overline{g(x)p(x)} \quad \text{in} \quad \mathbb{F}_p[x].
\]

Since \( \text{char } \mathbb{Z}_p = p \), there holds \( \overline{h}(x^p) = \overline{h}(x)^p \) in \( \mathbb{F}_p[x] \) and we get

\[
\overline{h}(x)^p = \overline{g(x)p(x)} \quad \text{in} \quad \mathbb{F}_p[x].
\]

So there is an irreducible factor of \( \overline{g}(x) \) in \( \mathbb{F}_p[x] \) which divides \( \overline{h}(x)^p \) and which therefore divides \( \overline{h}(x) \) in \( \mathbb{F}_p[x] \). Thus \( \overline{g}(x) \) and \( \overline{h}(x) \) have a common factor in \( \mathbb{F}_p[x] \). Since \( g(x)h(x) = \Phi_n(x) \) divides \( x^n - 1 \) in \( \mathbb{Z}[x] \), there is a \( k(x) \) in \( \mathbb{Z}[x] \) such that

\[
g(x)h(x)k(x) = x^n - 1 \quad \text{in} \quad \mathbb{Z}[x],
\]

so

\[
g(x)\overline{h}(x)\overline{k}(x) = x^n - 1 = x^n - 1 \quad \text{in} \quad \mathbb{F}_p[x]
\]

and \( x^n - 1 \in \mathbb{F}_p[x] \) has a multiple root. But the derivative of \( x^n - 1 \in \mathbb{F}_p[x] \) is not \( 0 \in \mathbb{F}_p[x] \), so relatively prime to \( x^n - 1 \) and \( x^n - 1 \in \mathbb{F}_p[x] \) has no multiple roots. This contradiction shows that \( \zeta^p \) must be a root of \( g(x) \).

Hence if \( p \) is a prime number,

\[(p,n) = 1,
\]

\( \zeta \) is a root of \( g(x) \), then \( \zeta^p \) is a root of \( g(x) \).

Let \( m \) be any natural number satisfying \( 1 \leq m \leq n \) and \( (n,m) = 1 \). Then \( m = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r} \) with suitable prime numbers \( p_i \) relatively prime to \( n \).

Repeated application of the result we have just proved shows that \( \zeta^m \) is a root of \( g(x) \) when \( \zeta \) is. This is true for each of the \( \varphi(n) \) natural numbers \( m \) such that \( 1 \leq m \leq n \) and \( (n,m) = 1 \). Thus \( g(x) \) has \( \varphi(n) \) (distinct) roots \( \zeta^m \) and \( g(x) \) is divisible by \( \prod_{1 \leq m \leq n} (x - \zeta^m) = \Phi_n(x) \). Hence \( \Phi_n(x) = g(x) \) and \( \Phi_n(x) \) is irreducible in \( \mathbb{Z}[x] \). \( \square \)
58.12 Theorem: Let \( n \in \mathbb{N} \) and let \( \zeta \) be a primitive \( n \)-th root of unity in some extension of \( \mathbb{Q} \). Then \( \mathbb{Q}(\zeta) \) is Galois over \( \mathbb{Q} \) and \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \cong \mathbb{Z}_n^\times \).

Proof: Since \( \Phi_n(x) \) is monic and irreducible in \( \mathbb{Z}[x] \), it is irreducible in \( \mathbb{Q}[x] \) (Lemma 34.11). The claim follows now from Theorem 58.10.

We consider the special case of Theorem 58.12 where \( n \) is prime. Let \( p \) be a prime number. Then the isomorphism \( \mathbb{Z}_p^\times \cong \text{F}_p^\times \cong \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \) is given, in the notation of the proof of Theorem 58.10, by \( m_i^* \rightarrow \alpha_{m_i} \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \), where \( \alpha_{m_i} : \zeta \rightarrow \zeta^{m_i} \). Both \( \mathbb{F}_p^\times \) and \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \) are cyclic. Let \( g \in \mathbb{Z} \) be such that its residue class \( g^* \in \mathbb{F}_p^\times \) is a generator of \( \mathbb{F}_p^\times \). Then \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \langle \sigma \rangle \), where \( \sigma = \alpha_g \), i.e., \( \sigma \) is the automorphism \( \zeta \rightarrow \zeta^g \).

Then the \( p \)-th primitive roots of unity are

\[ \zeta, \zeta^g, \zeta^{g^2}, \zeta^{g^3}, \ldots, \zeta^{g^{p-2}} \]

and we have \( \sigma^k : \zeta \rightarrow \zeta^{g^k} \). Let us put \( \zeta_k = \zeta^{g^k} \). Then \( \zeta_{k+(p-1)} = \zeta \sigma^{k+(p-1)} = \zeta \sigma^k = \zeta_k \) so that any index \( k \) can be replaced by any \( j \) with \( k \equiv j \pmod{p-1} \). Now \( \zeta_k \sigma = (\zeta^g)^\sigma = (\zeta \sigma)^g = (\zeta^g)^{g^k} = \zeta^{g^{k+1}} \) and \( \zeta_k \sigma^m = (\zeta^g)^{g^k} \sigma^m = (\zeta^g)^{g^k} = \zeta^{g^{k+m}} = \zeta_{k+m} \). Thus \( \sigma \) raises the index by 1 and more generally \( \sigma^m \) raises the index by \( m \).

Let us find the intermediate fields of the extension \( \mathbb{Q}(\zeta)/\mathbb{Q} \). Since \( \mathbb{Q}(\zeta) \) is Galois over \( \mathbb{Q} \), and since \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = \langle \sigma \rangle \) is cyclic of order \( p-1 \), there is one and only one intermediate field for each positive divisor \( e \) of \( p-1 \), namely the one that corresponds to the subgroup \( \langle \sigma^e \rangle \) of \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \). Hence this field, say \( K_e \), is the fixed field of \( \sigma^e \) and \( |K_e:\mathbb{Q}| = |\langle \sigma \rangle: \langle \sigma^e \rangle| = e \). In order to describe \( K_e \) explicitly, we note first that

\[ \{1, \zeta, \zeta^g, \zeta^{g^2}, \zeta^{g^3}, \ldots, \zeta^{g^{p-2}}\} = \{1, \zeta_0, \zeta_1, \zeta_2, \zeta_3, \ldots, \zeta_{p-2}\} = \{1, \zeta, \zeta^g, \zeta^2, \zeta^3, \ldots, \zeta^{p-2}\} \]

is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\zeta) \) since this set is equal to \( \{1, \zeta, \zeta^2, \ldots, \zeta^{p-1}\} \), which is a \( \mathbb{Q} \)-basis of \( \mathbb{Q}(\zeta) \) by Theorem 50.7. So any element \( u \) in \( \mathbb{Q}(\zeta) \) can be written in the form

\[ u = a_0 \zeta_0 + a_1 \zeta_1 + a_2 \zeta_2 + a_3 \zeta_3 + \cdots + a_{p-1} \zeta_{p-1} \]

748
with uniquely determined \( a_0 a_1, a_2, \ldots, a_{p-1} \in \mathbb{Q} \). Here

\[
u \sigma^e = (a_0 \zeta_0 + a_1 \zeta_1 + a_2 \zeta_2 + a_3 \zeta_3 + \cdots + a_{p-2} \zeta_{p-2}) \sigma^e
= a_0 \zeta_{e+0} + a_1 \zeta_{e+1} + a_2 \zeta_{e+2} + a_3 \zeta_{e+3} + \cdots + a_{p-2} \zeta_{e+(p-2)}
\]

and \( u \) is fixed by \( \sigma^e \), i.e., \( u \sigma^e = u \) if and only if

\[
a_0 \zeta_{e+0} + a_1 \zeta_{e+1} + a_2 \zeta_{e+2} + a_3 \zeta_{e+3} + \cdots + a_{p-2} \zeta_{e+(p-2)}
= a_{e+0} + a_{e+1} \zeta_{e+1} + a_{e+2} \zeta_{e+2} + a_{e+3} \zeta_{e+3} + \cdots + a_{e+(p-2)} \zeta_{e+(p-2)}
\]

which is equivalent, when we put \( f = (p - 1) / e \), to

\[
a_0 = a_{e+0} = a_{2e+0} = a_{3e+0} = \cdots = a_{(f-1)e+0}
\]
\[
a_1 = a_{e+1} = a_{2e+1} = a_{3e+1} = \cdots = a_{(f-1)e+1}
\]
\[
a_2 = a_{e+2} = a_{2e+2} = a_{3e+2} = \cdots = a_{(f-1)e+2}
\]

\[
\vdots
\]
\[
a_{(e-1)} = a_{e+(e-1)} = a_{2e+(e-1)} = a_{3e+(e-1)} = \cdots = a_{(f-1)e+(e-1)}
\]

and this means \( u = a_0 (\zeta_0 + \zeta_e + \zeta_{2e} + \zeta_{3e} + \cdots + \zeta_{(f-1)e})
+ a_1 (\zeta_1 + \zeta_{e+1} + \zeta_{2e+1} + \zeta_{3e+1} + \cdots + \zeta_{(f-1)e+1})
+ a_2 (\zeta_2 + \zeta_{e+2} + \zeta_{2e+2} + \zeta_{3e+2} + \cdots + \zeta_{(f-1)e+2})
+ \cdots
+ a_{e-1} (\zeta_{e-1} + \zeta_{e+(e-1)} + \zeta_{2e+(e-1)} + \zeta_{3e+(e-1)} + \cdots + \zeta_{(f-1)e+(e-1)})
\).

We put \( \eta_k = \zeta_k + \zeta_{e+k} + \zeta_{2e+k} + \zeta_{3e+k} + \cdots + \zeta_{(f-1)e+k} \) \( (k = 1, 2, \ldots, e - 1) \). The elements \( \eta_k \) are called the periods of \( f \) terms. We see \( u \) is fixed by \( \sigma^e \) if and only if \( u = a_0 \eta_0 + a_1 \eta_1 + a_2 \eta_2 + \cdots + a_{e-1} \eta_{e-1} \) with \( a_0, a_1, a_2, \ldots, a_{e-1} \in \mathbb{Q} \).

So \( \{ \eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1} \} \) is a \( \mathbb{Q} \)-basis of \( K_e \).

Note that \( \sigma : \eta_0 \rightarrow \eta_1, \eta_1 \rightarrow \eta_2, \eta_2 \rightarrow \eta_3, \ldots, \eta_{e-2} \rightarrow \eta_{e-1}, \eta_{e-1} \rightarrow \eta_0 \). Thus each of \( \eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1} \) is fixed by \( \sigma^e \) and by powers of \( \sigma^e \), but not by any other automorphism of \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \). Hence all intermediate fields \( \mathbb{Q}(\eta_0), \mathbb{Q}(\eta_1), \mathbb{Q}(\eta_2), \ldots, \mathbb{Q}(\eta_{e-1}) \) of \( \mathbb{Q}(\zeta) / \mathbb{Q} \) correspond to the same subgroup \( \langle \sigma^e \rangle \) of \( \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \). This forces \( \mathbb{Q}(\eta_0) = \mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2) = \cdots = \mathbb{Q}(\eta_{e-1}) = K_e \). So any period of \( f \) terms is a primitive element of \( K_e \), the unique intermediate field of \( \mathbb{Q}(\zeta) / \mathbb{Q} \) with \( |K_e : \mathbb{Q}| = e \).
We summarize our results.

58.13 **Theorem:** Let $p$ be a prime number and $\zeta$ a primitive $p$-th root of unity in some extension field of $\mathbb{Q}$. Let $g \in \mathbb{Z}$ be such that its residue class $g^2$ in $\mathbb{F}_p$ is a generator of $\mathbb{F}_p^\times$. Then

1. $\mathbb{Q}(\zeta)$ is Galois over $\mathbb{Q}$;
2. $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\zeta)$ is a cyclic group of order $p - 1$. A generator of $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\zeta)$ is the $\mathbb{Q}$-automorphism $\sigma: \zeta \mapsto \zeta^g$.
3. Let $e$ and $f$ be natural numbers such that $ef = p - 1$, and put
   $$\eta_k = \zeta^{ge^k} + \zeta^{2ge^k} + \cdots + \zeta^{(f-1)ge^k} \quad (k = 0, 1, 2, \ldots, e - 1).$$

Then there is one and only one intermediate field of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ whose $\mathbb{Q}$-dimension is equal to $e$. This field is $\mathbb{Q}(\eta_k)$ for any $k = 0, 1, 2, \ldots, e - 1$. The set $\{\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\eta_k)$. All intermediate fields of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are found in this way as $e$ ranges through the positive divisors of $p - 1$. \hfill \square

58.14 **Examples:** (a) We find all intermediate fields of $\mathbb{Q}(\zeta)$, where the complex number $\zeta \in \mathbb{C}$ is a primitive 7-th root of unity. These are the simple extensions of $\mathbb{Q}$ whose primitive elements are the periods. In order to construct the periods, we need a generator of $\mathbb{F}_7^\times$. One checks easily that the residue class of 3 is a generator of $\mathbb{F}_7^\times$. The images of $\zeta$ under powers of the automorphism $\sigma: \zeta \mapsto \zeta^3$ are

$$\zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5.$$  

The 1-term periods are $\zeta, \zeta^3, \zeta^2, \zeta^6, \zeta^4, \zeta^5$ and $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^3) = \mathbb{Q}(\zeta^2) = \mathbb{Q}(\zeta^6) = \mathbb{Q}(\zeta^4) = \mathbb{Q}(\zeta^5)$ is the intermediate field with $|\mathbb{Q}(\zeta):\mathbb{Q}| = 6$.  

750
The 2-term periods are \( \zeta + \zeta^6, \zeta^3 + \zeta^4, \zeta^2 + \zeta^5 \) and \( \mathbb{Q}(\zeta + \zeta^6) \) is the intermediate field \( |\mathbb{Q}(\zeta + \zeta^6):\mathbb{Q}| = 3 \). We also have \( \mathbb{Q}(\zeta + \zeta^6) = \mathbb{Q}(\zeta + \zeta^4) = \mathbb{Q}(\zeta^3 + \zeta^4) = \mathbb{Q}(\zeta^2 + \zeta^5) \).

The 3-term periods are \( \eta = \zeta + \zeta^2 + \zeta^4, \eta' = \zeta^3 + \zeta^6 + \zeta^5 \) and \( \mathbb{Q}(\eta) = \mathbb{Q}(\eta') \) is the intermediate field with \( |\mathbb{Q}(\eta):\mathbb{Q}| = 2 \).

The 6-term period is \( \zeta^3 + \zeta^2 + \zeta^6 + \zeta^4 + \zeta^5 + \zeta = -1 \) and \( \mathbb{Q}(-1) = \mathbb{Q} \) is the intermediate field with \( |\mathbb{Q}(-1):\mathbb{Q}| = 1 \).

(b) We determine the intermediate fields of \( \mathbb{Q}(\zeta)/\mathbb{Q} \), where \( \zeta \) is a primitive 17-th root of unity. The divisors of 17 - 1 = 16 are 1,2,4,8,16 and there are five intermediate fields, of dimensions 1,2,4,8,16 over \( \mathbb{Q} \).

The residue class of 3 \( \in \mathbb{Z} \) in \( \mathbb{F}_{17}^* \) is a generator of \( \mathbb{F}_{17}^* \). The successive powers of 3 are congruent, modulo 17, to

\[
1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6
\]

The 8-term periods are

\[
\eta_0 = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 \\
\eta_1 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6
\]

An elementary computation shows that \( \eta_0 + \eta_1 = -1 \) and \( \eta_0 \eta_1 = -4 \). So \( \eta_0 \) and \( \eta_1 \) are the roots of \( x^2 + x - 4 \). Hence \( \eta_0, \eta_1 = \frac{-1 \pm \sqrt{17}}{2} \). Which of \( \eta_0, \eta_1 \) has the plus sign depends on the choice of \( \zeta \). We may assume \( \zeta \) is a 17-th root of unity that appears in the period with the plus sign (otherwise replace \( \zeta \) by one of the roots of unity that appear in the period with the plus sign). Then \( \eta_0 = \frac{-1 + \sqrt{17}}{2} \) and \( \eta_1 = \frac{-1 - \sqrt{17}}{2} \).

The 4-term periods are

\[
\chi_0 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4, \quad \chi_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2
\]
\[\begin{align*}
\chi_1 &= \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12}, \\
\chi_3 &= \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6
\end{align*}\]

and \[\chi_0 + \chi_2 = \eta_0, \quad \chi_0\chi_2 = -1; \quad \chi_1 + \chi_3 = \eta_1, \quad \chi_1\chi_3 = -1.\]

Hence \(\chi_0\) and \(\chi_2\) are the roots of \(x^2 - \eta_0x - 1\) and \(\chi_1\) and \(\chi_3\) are the roots of \(x^2 - \eta_1x - 1\). Here we may put \(\chi_0 = \frac{\eta_0 + \sqrt{\eta_0^2 + 4}}{2}\) and \(\chi_2 = \frac{\eta_0 - \sqrt{\eta_0^2 + 4}}{2}\) by assuming that \(\zeta\) is a 17-th root of unity that appears in the period \(\chi\) with the plus sign. The signs of radicals in \(\chi_1\chi_3 = \frac{\eta_1 + \sqrt{\eta_1^2 + 4}}{2}\), however, can no longer be arbitrarily assigned by choosing \(\zeta\) suitably. To determine which of \(\chi_1\chi_3\) has the positive radical, we note

\[
(\chi_0 - \chi_2)(\chi_1 - \chi_3) = 2(\eta_0 - \eta_1) \cdot \frac{\sqrt{\eta_0^2 + 4}}{2} \cdot (\chi_1 - \chi_3) = \sqrt{17},
\]

so that \(\chi_1 - \chi_3\) is positive. This gives \(\chi_1 = \frac{\eta_1 + \sqrt{\eta_1^2 + 4}}{2}\) and \(\chi_3 = \frac{\eta_1 - \sqrt{\eta_1^2 + 4}}{2}\).

The 2-term periods are

\[
\psi_0 = \zeta + \zeta^{16}, \quad \psi_4 = \zeta^{13} + \zeta^4, \\
\psi_1 = \zeta^3 + \zeta^{14}, \quad \psi_5 = \zeta^5 + \zeta^{12}, \\
\psi_2 = \zeta^9 + \zeta^8, \quad \psi_6 = \zeta^{15} + \zeta^2, \\
\psi_3 = \zeta^{10} + \zeta^7, \quad \psi_7 = \zeta^{11} + \zeta^6.
\]

Here \(\psi_0 + \psi_4 = \chi_0\) and \(\psi_0\psi_4 = \chi_1\), so \(\psi_0\) and \(\psi_4\) are roots of \(x^2 - \chi_0x + \chi_1\).

Thus \(\psi_0, \psi_4 = \frac{\chi_0 + \sqrt{\chi_0^2 - 4\chi_1}}{2}\). We put \(\psi_0 = \frac{\chi_0 + \sqrt{\chi_0^2 - 4\chi_1}}{2}\). In like manner as above, one can find polynomials whose roots are \(\psi_j\) and determine the roots without ambiguity.

A 1-term period is \(\zeta\), which is a root of \(x^2 - \psi_0x + 1\). Hence we may put \(\zeta = \frac{\psi_0 + \sqrt{\psi_0^2 - 4}}{2}\).

The subfield structure of \(\mathbb{Q}(\zeta)\) is depicted below.
We now prove an important theorem due to J. H. M. Wedderburn which states that any finite division ring is commutative. The proof makes use of the class equation (Lemma 25.16) of the multiplicative group of nonzero elements in a finite division ring. Let us recall the class equation of any finite group $G$ is

$$|G| = \sum_{i=1}^{k} |G:C_G(x_i)|,$$

where $k$ is the number of distinct conjugacy classes, $x_1, x_2, \ldots, x_k$ are representatives of these classes and $C_G(x_i) = \{g \in G : x_i g = g x_i\}$ are the centralizers of $x_i$ ($i = 1, 2, \ldots, k$).

In addition to these centralizer groups, we consider centralizer rings and evaluate their dimensions to find the terms in the class equation. An argument involving cyclotomic polynomials shows that the class equation cannot hold unless the division ring is commutative.

In order not to interrupt the main argument, we establish two lemmas we will need.
58.15 Lemma: Let \( n \) be a natural number greater than one and let \( \Phi_n(x) \) be the \( n \)-th cyclotomic polynomial over \( \mathbb{Q} \). Then, for any a proper divisor \( d \) of \( n \), we have

\[
\Phi_n(x) \bigg| \frac{x^n - 1}{x^d - 1} = x^{(n/d) - 1} + x^{(n/d) - 2} + \cdots + x^{(n/d)} + 1 \quad \text{in} \quad \mathbb{Z}[x]
\]

and, for any natural number \( q \),

\[
\Phi_n(q) \bigg| \frac{q^n - 1}{q^d - 1} \quad \text{in} \quad \mathbb{Z}.
\]

Proof: Since \( \Phi_n(x)|(x^n - 1) \) and \( x^n - 1 = (x^d - 1)[(x^n - 1)/(x^d - 1)] \), it is sufficient to show that \( \Phi_n(x) \) is relatively prime to \( x^d - 1 \) for any proper divisor \( d \) of \( n \). But this is clear, because \( \Phi_n(x) \) and \( x^d - 1 \) have no root in common: the roots of \( \Phi_n(x) \) are primitive \( n \)-th roots of unity, whereas a root of \( x^d - 1 \) cannot be a primitive \( n \)-th root of unity if \( d \) is a proper divisor of \( n \). This proves the divisibility relation in \( \mathbb{Z}[x] \). Substituting any integer \( q \) for \( x \) (and using \( \Phi_n(x) \), \( (x^n - 1)/(x^d - 1) \in \mathbb{Z}[x] \)) we obtain the divisibility relation in \( \mathbb{Z} \).

\[\square\]

58.16 Lemma: If \( n > 1 \) and \( \Phi_n(x) \) is the \( n \)-th cyclotomic polynomial over \( \mathbb{Q} \), then \( |\Phi_n(q)| > q - 1 \) for all \( q \in \mathbb{N} \) with \( q \geq 2 \).

Proof: We have \( \Phi_n(x) = \prod_{(k,n)=1} (x - \zeta^k) \), where \( \zeta \) is a primitive \( n \)-th root of unity in some extension field of \( \mathbb{Q} \). For example, we may take \( \zeta = e^{2\pi i/n} \). Substituting \( q \) for \( x \) and using the triangle inequality \( |a - b| \geq | |a| - |b| | \), we get

\[
|\Phi_n(q)| = \prod_{(k,n)=1} |q - \zeta^k| = \prod_{(k,n)=1} |q - e^{2\pi ki/n}| \geq \prod_{(k,n)=1} |q| - |e^{2\pi ki/n}| = \prod_{(k,n)=1} |q - 1| = (q - 1)^{\varphi(n)} = (q - 1)(q - 1)^{\varphi(n)-1} > q - 1
\]

754
in case \( \varphi(n) - 1 \geq 1 \) since \( q > 1 \). In case \( \varphi(n) - 1 = 0 \), we have \( n = 2 \) and 

\[ |\Phi_2(q)| = q + 1 > q - 1. \]

\[ \blacksquare \]

58.17 Theorem (Wedderburn's theorem): If \( D \) is a finite division ring, then \( D \) is a field.

Proof: Let \( D \) be a division ring with finitely many elements. \( D^* = D \setminus \{0\} \) is then a finite group under multiplication and the class equation of \( D^* \) is

\[ |D^*| = \sum_{i=1}^{k} |D^*:C_D(x_i)|, \]

where \( k \) is the number of distinct conjugacy classes of \( D^* \) and \( x_1, x_2, \ldots, x_k \) are representatives of these classes.

We now put \( C_D(x_i) = \{ a \in D : x_i a = ax_i \} = C_D(x_i) \cup \{0\} \subseteq D \). Since \( a, b \in C_D(x_i) \) implies \( x_i(a + b) = x_i a + x_i b = ax_i + bx_i = (a + b)x_i \), we see \( C_D(x_i) \) is closed under addition and thus \( C_D(x_i) \) is a subgroup of \( D \) under addition (Lemma 9.3(2)). As \( C_D(x_i) \setminus \{0\} = C_D(x_i) \) is a subgroup of \( D^* \), we conclude that \( C_D(x_i) \) is a division ring (a subdivision ring of \( D \)).

The same argument proves that the center of the ring \( D \):

\[ Z = \{ a \in D : xa = ax \text{ for all } x \in D \} = Z(D^*) \cup \{0\} \]

is a a subdivision ring of \( D \). But \( Z \) is a commutative division ring, i.e., \( Z \) is a field. Then \( \text{char } Z = p \) for some prime number \( p \) and \( |Z| = p^t \) for some natural number \( t \). We put \( q = p^t = |Z| \) for brevity.

We have \( Z \subseteq C_D(x_i) \subseteq D \). Since multiplication in \( D \) is associative and distributive over addition, and since \( 1a = a \) for all \( a \in C_D(x_i) \), we get that \( C_D(x_i) \) and \( D \) are vector spaces over \( Z \). Let \( \text{dim}_Z C_D(x_i) = m_i \) and \( \text{dim}_Z D = n \). Then, as in Lemma 52.1, we have \( |C_D(x_i)| = |Z|^{m_i} = q^{m_i} \) and \( |D| = |Z|^n = q^n \).

This gives \( |C_D(x_i)| = |C_D(x_i)\setminus\{0\}| = |C_D(x_i)| - 1 = q^{m_i} - 1 \) and likewise \( |D^*| = |D\setminus\{0\}| = |D| - 1 = q^n - 1 \). The class equation is therefore

\[ q^n - 1 = \sum_{i=1}^{k} |D^*:C_D(x_i)| = \sum_{i=1}^{k} \frac{|D^*|}{|C_D(x_i)|} = \sum_{i=1}^{k} \frac{q^n - 1}{q^{m_i} - 1}. \]

755
Now $|D^*: C_D(x_i)|$ is an integer, so $q^{m_i} - 1$ divides $q^n - 1$ and this implies that $m_i$ divides $n$ (Lemma 52.7(1)).

We want to show that $D$ is commutative, or, what is the same thing, that $Z = D$. We will assume $Z \neq D$ and derive a contradiction. Well, if $Z \neq D$, then $n > 1$ and there is at least one $x_i$ such that $|D^*: C_D(x_i)| \neq 1$, because $|D^*: C_D(x_i)| = 1$ if and only if $x_i \in Z(D^*)$. We so choose the notation that \( \{x_1, x_2, \ldots, x_h\} = Z(D^*) \) and $x_{h+1}, \ldots, x_k$ are not in the center of $D^*$. Then the class equation becomes

$$q^n - 1 = \sum_{i=1}^{h} |D^*: C_D(x_i)| + \sum_{i=h+1}^{k} |D^*: C_D(x_i)| = |Z(D^*)| + \sum_{i=h+1}^{k} \frac{q^n - 1}{q^{m_i} - 1}.$$  

and $m_i$ is a proper divisor of $n$ for $i = h + 1, \ldots, k$. As $n > 1$ by assumption, $\Phi_n(q)$ divides $\frac{q^n - 1}{q^{m_i} - 1}$ for all $i = h + 1, \ldots, k$ (Lemma 58.15); $\Phi_n(q)$ divides also $q^n - 1$. We read from the class equation that $\Phi_n(q)$ divides $q - 1$. But this is impossible, for $|\Phi_n(q)| > q - 1$ by Lemma 58.16.

Thus $n = 1$ and $D = Z$ is commutative.

\[\square\]

**Exercises**

1. Find the $m$-th cyclotomic polynomial $\Phi_m(x)$ over $\mathbb{Q}$ for $m \leq 50$.

2. Let $\Phi_n(x)$ denote the $m$-th cyclotomic polynomial over $\mathbb{Q}$. Prove:
   (a) $\Phi_{2n}(x) = \Phi_n(-x)$ if $2 \nmid n$.
   (b) $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ if $p$ is an odd prime number and $p \nmid n$.

3. Evaluate the $p^k$-th cyclotomic polynomial $\Phi_{p^k}(x)$ over $\mathbb{Q}$ if $p$ is a prime number and $k \in \mathbb{N}$.

4. Let $p, k \in \mathbb{N}$ and $p$ be prime. Let $\Phi_p(x)$ denote the $p$-th cyclotomic polynomial over $\mathbb{Q}$. Prove that, if $d \nmid \Phi_p(k)$, then $d \equiv 1 \pmod{p}$ or $d = p$. 

756
5. Let \( p \in \mathbb{N} \) be prime, \( k \in \mathbb{Z} \) and let \( k^* \) be the residue class of \( k \) in \( \mathbb{F}_p \). Let \( n \in \mathbb{N} \) and \( \Phi_n(x) \) the \( n \)-th cyclotomic polynomial over \( \mathbb{Q} \). Suppose that \( p \nmid n \). Prove the following statements.
   (a) \( p \mid \Phi_n(k) \) if and only if \( o(k^*) = n \) (order of \( k^* \) in \( \mathbb{F}_p^x \) is \( n \)).
   (b) There is an integer \( a \) with \( p \mid \Phi_n(a) \) if and only if \( p \equiv 1 \pmod{n} \).

6. Let \( \gamma \in \mathbb{N} \) and \( \Phi_n(x) \) the \( n \)-th cyclotomic polynomial over \( \mathbb{Q} \) and let \( p_1p_2\ldots p_m \) be prime numbers of the form \( tn + 1 \) \((t,n \in \mathbb{Z})\). Use Ex. 5 and prove the following statements.
   (a) \( \Phi_n(anp_1p_2\ldots p_m) \equiv \pm 1 \pmod{np_1p_2\ldots p_m} \) for any \( a \in \mathbb{N} \).
   (b) \( \Phi_n(anp_1p_2\ldots p_m) \not\equiv \pm 1 \pmod{a} \) if \( a \in \mathbb{N} \) is sufficiently large.
   (c) For some \( a \in \mathbb{N} \), there is a prime divisor \( p \) of \( \Phi_n(anp_1p_2\ldots p_m) \) which is distinct from \( p_1p_2\ldots p_m \).
   (d) There are infinitely many prime numbers \( p \) of the form \( tn + 1 \).
   (This is a special case of the following celebrated theorem of Dirichlet: if \( a,b \) are any relatively prime integers, then there infinitely many prime numbers of the form \( an + b \).)

7. Find all subfields of \( \mathbb{Q}(\zeta) \), where \( \zeta \in \mathbb{C} \) is a primitive \( n \)-th root of unity and \( n = 4,5,6,8,12 \). Prove \( e^{2\pi i/5} = \frac{-1+i\sqrt{5}+\sqrt{10+2\sqrt{5}}}{4} \).

8. Prove the formula due to Gauss:

\[
\cos \frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16} \sqrt{17} + \frac{1}{16} \sqrt{34 - 2\sqrt{17}} + \frac{1}{8} \sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.
\]

9. Under the hypotheses of Theorem 58.13, show that the set of periods independent of the integer \( g \) for which \( g^* \) is a generator of \( \mathbb{F}_p^x \), but the indices of individual periods do depend on \( g \). Describe this dependence.

10. Let the hypotheses of Theorem 58.13 be valid, with \( p \) an odd prime number, and let \( \eta_0, \eta_1 \) be the \([(p-1)/2]-term periods. Prove that \( \eta_0\eta_1 = -(p-1)/4 \) or \( (p + 1)/4 \) according as \( p \equiv 1 \pmod{p} \) or \( p \equiv 3 \pmod{p} \). Show that \( \eta_0 - \eta_1 = \pm \sqrt{(-1)^{(p-1)/2}}p \). (The sign depends on the primitive \( p \)-th root of unity \( \zeta \) we take. If we choose \( \zeta = e^{2\pi i/p} \in \mathbb{C} \), then the sign is plus. This is considerably difficult to prove. This exercise shows \( \mathbb{Q}(\zeta) \) is contained in the cyclotomic field \( \mathbb{Q}(\zeta) \). A theorem of class
field theory, known as Kronecker-Weber theorem, states that any finite dimensional Galois extension of \( \mathbb{Q} \) whose Galois group is abelian is contained in a suitable cyclotomic extension of \( \mathbb{Q} \).

11. Let \( \zeta_k \in \mathbb{C} \) denote a primitive \( k \)-th root of unity. Show that, if \( (n,m) = 1 \), then \( \mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm}) \) and \( \mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q} \).

12. Let \( \zeta \in \mathbb{C} \) be a primitive \( n \)-th root of unity. Prove that all roots of unity in \( \mathbb{Q}(\zeta) \) are \( \tau \zeta^j \) (\( j = 0,1,2, \ldots, n - 1 \)).

13. Let \( p \in \mathbb{N} \) be a prime number and \( \Phi_p(x) \) the \( p \)-th cyclotomic polynomial over \( \mathbb{Q} \). Find the discriminant of \( \Phi_p(x) \).

14. Show that any finite subring of a division ring is a division ring.