that α lies in the fixed field for H. If now τ is *not* an element of H, then $\tau\alpha$ is the sum of basis elements (recall that any automorphism permutes the basis elements here), one of which is $\tau(\zeta_p)$. If we had $\tau\alpha = \alpha$ then since these elements are a basis, we must have $\tau(\zeta_p) = \sigma(\zeta_p)$ for one of the terms $\sigma\zeta_p$ in (10). But this implies $\tau\sigma^{-1} = 1$ since this automorphism is the identity on ζ_p. Then $\tau = \sigma \in H$, a contradiction. This shows that α is not fixed by any automorphism not contained in H, so that $\mathbb{Q}(\alpha)$ is precisely the fixed field of H.

For a specific example, consider the subfields of $\mathbb{Q}(\zeta_{13})$, which correspond to the subgroups of $(\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/12\mathbb{Z}$. A generator for this cyclic group is the automorphism $\sigma = \sigma_2$ which maps ζ_{13} to ζ_{13}^2. The nontrivial subgroups correspond to the nontrivial divisors of 12, hence are of orders 2, 3, 4, and 6 with generators σ^6, σ^4, σ^3 and σ^2, respectively. The corresponding fixed fields will be of degrees 6, 4, 3 and 2 over $\mathbb{Q}$, respectively. Generators are given by ($\zeta = \zeta_{13}$)

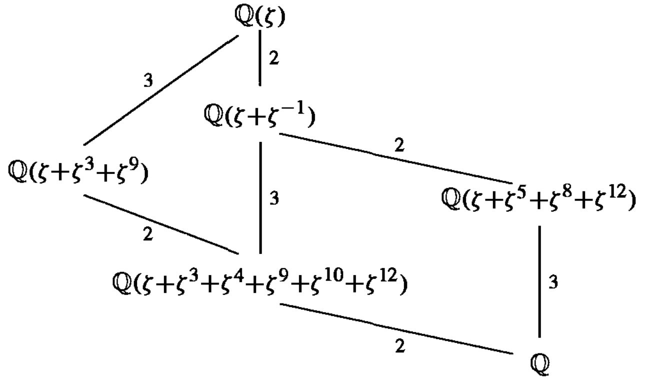
$$\zeta + \sigma^6\zeta = \zeta + \zeta^{2^6} = \zeta + \zeta^{-1}$$

$$\zeta + \sigma^4\zeta + \sigma^8\zeta = \zeta + \zeta^{2^4} + \zeta^{2^8} = \zeta + \zeta^3 + \zeta^9$$

$$\zeta + \sigma^3\zeta + \sigma^6\zeta + \sigma^9\zeta = \zeta + \zeta^8 + \zeta^{12} + \zeta^5$$

$$\zeta + \sigma^2\zeta + \sigma^4\zeta + \sigma^6\zeta + \sigma^8\zeta + \sigma^{10}\zeta = \zeta + \zeta^4 + \zeta^3 + \zeta^{12} + \zeta^9 + \zeta^{10}.$$

The lattice of subfields for this extension is the following:


$\mathbb{Q}(\zeta)$
3
2
$\mathbb{Q}(\zeta+\zeta^{-1})$
2
$\mathbb{Q}(\zeta+\zeta^3+\zeta^9)$
3
$\mathbb{Q}(\zeta+\zeta^5+\zeta^8+\zeta^{12})$
2
$\mathbb{Q}(\zeta+\zeta^3+\zeta^4+\zeta^9+\zeta^{10}+\zeta^{12})$
3
2
$\mathbb{Q}$

The elements constructed in equation (10) and their conjugates are called the *periods* of ζ and are useful in the study of the arithmetic of the cyclotomic fields. The study of their combinatorial properties is referred to as *cyclotomy*.

Suppose that $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the decomposition of n into distinct prime powers. Since $\zeta_n^{p_2^{a_2} \cdots p_k^{a_k}}$ is a primitive $p_1^{a_1}$-th root of unity, the field $K_1 = \mathbb{Q}(\zeta_{p_1^{a_1}})$ is a subfield of $\mathbb{Q}(\zeta_n)$. Similarly, each of the fields $K_i = \mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \ldots, k$ is a subfield of $\mathbb{Q}(\zeta_n)$. The composite of the fields contains the product $\zeta_{p_1^{a_1}} \zeta_{p_2^{a_2}} \cdots \zeta_{p_k^{a_k}}$, which is a primitive n^{th} root of unity, hence the composite field is $\mathbb{Q}(\zeta_n)$. Since the extension degrees $[K_i : \mathbb{Q}]$ equal $\varphi(p_i^{a_i})$, $i = 1, 2, \ldots, k$ and $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k})$, the degree of the composite of the fields K_i is precisely the product of the degrees of the K_i. It follows from Proposition 21 (and a simple induction from the two fields considered in the proposition to the k fields here) that the intersection of all these fields is precisely $\mathbb{Q}$. Then Corollary 22 shows that the Galois group for $\mathbb{Q}(\zeta_n)$ is the direct product of the Galois groups over $\mathbb{Q}$ for the subfields K_i. We summarize this as the following corollary.

Corollary 27. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the decomposition of the positive integer n into distinct prime powers. Then the cyclotomic fields $\mathbb{Q}(\zeta_{p_i^{a_i}})$, $i = 1, 2, \dots, k$ intersect only in the field $\mathbb{Q}$ and their composite is the cyclotomic field $\mathbb{Q}(\zeta_n)$. We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_2^{a_2}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q})$$

which under the isomorphism in Theorem 26 is the Chinese Remainder Theorem:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$

Proof: The only statement which has not been proved is the identification of the isomorphism of Galois groups with the statement of the Chinese Remainder Theorem on the group $(\mathbb{Z}/n\mathbb{Z})^\times$, which is quite simple and is left for the exercises.

By Theorem 26 the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is in particular an abelian group.

Definition. The extension K/F is called an *abelian* extension if K/F is Galois and $\mathrm{Gal}(K/F)$ is an abelian group.

Since all the subgroups and quotient groups of abelian groups are abelian, we see by the Fundamental Theorem of Galois Theory that every subfield containing F of an abelian extension of F is again an abelian extension of F. By the results on composites of extensions in the last section, we also see that the composite of abelian extensions is again an abelian extension (since the Galois group of the composite is isomorphic to a subgroup of the direct product of the Galois groups, hence is abelian).

It is an open problem to determine which groups arise as the Galois groups of Galois extensions of $\mathbb{Q}$. Using the results above we can see that every *abelian* group appears as the Galois group of some extension of $\mathbb{Q}$, in fact as the Galois group of some subfield of a cyclotomic field.

Let $n = p_1 p_2 \cdots p_k$ be the product of distinct primes. Then by the Chinese Remainder Theorem

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times (\mathbb{Z}/p_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times \\ &\cong Z_{p_1-1} \times Z_{p_2-1} \times \cdots \times Z_{p_k-1}. \end{aligned} \tag{14.11}$$

Now, suppose G is any finite abelian group. By the Fundamental Theorem for Abelian Groups,

$$G \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_k}$$

for some integers $n_1, n_2, \dots, n_k$. We take as known that given any integer m there are infinitely many primes p with $p \equiv 1 \bmod m$ (see the exercises following Section 13.6

for one proof using cyclotomic polynomials). Given this result, choose distinct primes $p_1, p_2, \ldots, p_k$ such that

$$\begin{aligned} p_1 &\equiv 1 \bmod n_1 \\ p_2 &\equiv 1 \bmod n_2 \\ &\vdots \\ p_k &\equiv 1 \bmod n_k \end{aligned}$$

and let $n = p_1 p_2 \cdots p_k$ as above.

By construction, n_i divides $p_i - 1$ for $i = 1, 2, \ldots, k$, so the group $Z_{p_i - 1}$ has a subgroup H_i of order $\dfrac{p_i - 1}{n_i}$ for $i = 1, 2, \ldots, k$, and the quotient by this subgroup is cyclic of order n_i. Hence the quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ in equation (11) by $H_1 \times H_2 \times \cdots \times H_k$ is isomorphic to the group G.

By Theorem 26 and the Fundamental Theorem of Galois Theory, we see that there is a subfield of $\mathbb{Q}(\zeta_{p_1 p_2 \cdots p_k})$ which is Galois over $\mathbb{Q}$ with G as Galois group. We summarize this in the following corollary.

Corollary 28. Let G be any finite abelian group. Then there is a subfield K of a cyclotomic field with $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

There is a converse to this result (whose proof is beyond our scope), the celebrated Kronecker–Weber Theorem:

Theorem *(Kronecker–Weber)* Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.

The abelian extensions of $\mathbb{Q}$ are the "easiest" Galois extensions (at least in so far as the structure of their Galois groups is concerned) and the previous result shows they can be classified by the cyclotomic extensions of $\mathbb{Q}$. For other finite extensions of $\mathbb{Q}$ as base field, it is more difficult to describe the abelian extensions. The study of the abelian extensions of an arbitrary finite extension F of $\mathbb{Q}$ is referred to as *class field theory*. There is a classification of the abelian extensions of F by invariants associated to F which greatly generalizes the results on cyclotomic fields over $\mathbb{Q}$. In general, however, the construction of abelian extensions is not nearly as explicit as in the case of the cyclotomic fields. One case where such a description is possible is for the abelian extensions of an imaginary quadratic field ($\mathbb{Q}(\sqrt{-D})$ for D positive), where the abelian extensions can be constructed by adjoining values of certain elliptic functions (this is the analogue of adjoining the roots of unity, which are the values of the exponential function e^x for certain x). The study of the arithmetic of such abelian extensions and the search for similar results for non-abelian extensions are rich and fascinating areas of current mathematical research.

We end our discussion of the cyclotomic fields with the problem of the constructibility of the regular n-gon by straightedge and compass.

Recall (cf. Section 13.3) that an element α is constructible over $\mathbb{Q}$ if and only if the field $\mathbb{Q}(\alpha)$ is contained in a field K obtained by a series of quadratic extensions:

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_i \subset K_{i+1} \subset \cdots \subset K_m = K \tag{14.12}$$

with

$$[K_{i+1} : K_i] = 2, \qquad i = 0, 1, \dots, m-1.$$

The construction of the regular n-gon in $\mathbb{R}^2$ is evidently equivalent to the construction of the n^{th} roots of unity, since the n^{th} roots of unity form the vertices of a regular n-gon on the unit circle in $\mathbb{C}$ with one vertex at the point 1.

The construction of ζ_n is equivalent to the constructibility of the first coordinate x in $\mathbb{R}^2$ of ζ_n, namely the real part of ζ_n. Since the complex conjugate of ζ_n is just ζ_n^{-1}, the real part of ζ_n is $x = \dfrac{1}{2}(\zeta_n + \zeta_n^{-1})$. Note that ζ_n satisfies the quadratic equation $\zeta_n^2 - 2x\zeta_n + 1 = 0$ over $\mathbb{Q}(x)$. Since $\mathbb{Q}(x)$ consists only of real numbers, it follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(x)] = 2$, so that $\mathbb{Q}(x)$ is an extension of degree $\varphi(n)/2$ of $\mathbb{Q}$.

It follows that if the regular n-gon can be constructed by straightedge and compass then $\varphi(n)$ must be a power of 2. Conversely, if $\varphi(n) = 2^m$ is a power of 2, then the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is an abelian group whose order is a power of 2, so the same is true for the Galois group $\mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$. It is easy to see by the Fundamental Theorem for Abelian Groups that an abelian group G of order 2^m has a chain of subgroups

$$G = G_m > G_{m-1} > \cdots > G_{i+1} > G_i > \cdots > G_0 = 1$$

with

$$[G_{i+1} : G_i] = 2, \qquad i = 0, 1, 2, \dots, m-1.$$

Applying this to the group $G = \mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q})$ and taking the fixed fields for the subgroups G_i, $i = 0, 1, \dots, m-1$, we obtain (by the Fundamental Theorem of Galois Theory) a sequence of quadratic extensions as in (12) above.

We conclude that the regular n-gon can be constructed by straightedge and compass if and only if $\varphi(n)$ is a power of 2. Decomposing n into prime powers to compute $\varphi(n)$ we see that this means $n = 2^k p_1 \cdots p_r$ is the product of a power of 2 and distinct odd primes p_i where $p_i - 1$ is a power of 2. It is an elementary exercise to see that a prime p with $p - 1$ a power of 2 must be of the form

$$p = 2^{2^s} + 1$$

for some integer s. Such primes are called *Fermat primes*. The first few are

$$\begin{aligned} 3 &= 2^1 + 1 \\ 5 &= 2^2 + 1 \\ 17 &= 2^4 + 1 \\ 257 &= 2^8 + 1 \\ 65537 &= 2^{16} + 1 \end{aligned}$$

(but $2^{32} + 1$ is not a prime, being divisible by 641). It is not known if there are infinitely many Fermat primes. We summarize this in the following proposition.