1 Cyclotomic Fields

Let's return to one of our original examples: $K = Q(\epsilon)$ with $\epsilon = e^{2\pi i / 5}$.

The minimal polynomial for $\epsilon$ in $\mathbb{Q}[x]$ is $(x^5 - 1)/(x - 1)$ which has roots $\epsilon, \epsilon^2, \epsilon^3, \epsilon^4$ which all in $K$. Thus $K$ is the splitting field of that polynomial (over $\mathbb{Q}$) and hence $K$ is normal over $\mathbb{Q}$.

The Galois Group is $\mathbb{Z}_5^*$ which is cyclic. Let $\sigma \in \Gamma[K : \mathbb{Q}]$ be determined by $\sigma(\epsilon) = \epsilon^2$. Then $\sigma^2(\epsilon) = \epsilon^4$ and $\sigma^3(\epsilon) = \epsilon^8 = \epsilon^3$ and $\sigma^4(\epsilon) = \epsilon^{16} = \epsilon$ so $\sigma^4 = e$. There is one nontrivial subgroup: $H = \{e, \sigma^2 \}$. From the Galois Correspondence theorem ?? this means there is one nontrivial intermediate field $\mathbb{Q} \subset L \subset Q(\epsilon)$ and $L = H^\dagger$. As $2 = |H| = |Q(\epsilon) : L|$ we have $|L : \mathbb{Q}| = 2$, so $L$ is a quadratic extension of $\mathbb{Q}$.

To find $L$ we look for which $\alpha \in Q(\epsilon)$ are in $H^\dagger$. As $\epsilon$ fixes all elements, $\alpha \in Q(\epsilon)$ if and only if $\sigma^2(\alpha) = \alpha$. Writing $\alpha = a + b\epsilon + c\epsilon^2 + d\epsilon^3$ we must have

$$\alpha = \sigma^2(\alpha) = a + b\epsilon^4 + c\epsilon^8 + d\epsilon^{12} = a + b(-1 - \epsilon - \epsilon^2 - \epsilon^3) + c\epsilon^3 + d\epsilon^2 \quad (1)$$

Equating the coefficients using the basis $1, \epsilon, \epsilon^2, \epsilon^3$ yields the equation system: $a = a - b$, $b = -b$, $c = d - b$, $d = c - b$ which reduces to $b = 0$, $c = d$. Thus the elements of $L$ may be uniquely written as $a + c(\epsilon^2 + \epsilon^3)$.

Set $\kappa = \epsilon^2 + \epsilon^3$. As $L = Q(\kappa)$, $\kappa$ must satisfy a quadratic. We find it by calculating $\kappa^2 = \epsilon^4 + 2 + \epsilon = 1 - \epsilon^2 - \epsilon^3$. Then $1, \kappa, \kappa^2$ are dependent, more precisely $\kappa^2 = 1 - \kappa$. Solving the quadratic gives

$$\kappa = \frac{-1 \pm \sqrt{5}}{2} \quad (2)$$

(The actual sign is minus, but this method doesn’t tell us that.) Thus we find $L = Q(\kappa) = Q(\sqrt{5})$.

When $p$ is an odd prime we can define $K = Q(\epsilon)$ with $\epsilon = e^{2\pi i / p}$. The minimal polynomial for $\epsilon$ is $p(x) = (x^p - 1)/(x - 1)$ which has roots $\epsilon, \epsilon^2, \ldots, \epsilon^{p-1}$. Again, $K$ is normal over $\mathbb{Q}$. The Galois Groups $\Gamma[K : \mathbb{Q}]$ has automorphisms $\sigma_i$ given by $\sigma_i(\epsilon) = \epsilon^i$ for each $i \in \mathbb{Z}_p^*$ and $\sigma_i \sigma_j = \sigma_{ij}$ where multiplication is done modulo $p$. Thus $\Gamma[K : \mathbb{Q}] \cong \mathbb{Z}_p^*$. It is known that this is a cyclic group of order $p - 1$, so $\Gamma[K : \mathbb{Q}] \cong (\mathbb{Z}_{p-1}, +)$. This group has a unique subgroup with half the elements, namely the multiples of 2 (thinking of it as $\mathbb{Z}_{p-1}$). Hence, by the Galois Correspondence Theorem ?? there is a unique quadratic extension of $\mathbb{Q}$ lying inside of $Q(\epsilon)$.

Here is a way of finding the square root in $Q(\epsilon)$ for general odd prime $p$. Rather than the usual basis $1, \epsilon, \ldots, \epsilon^{p-2}$ we use the basis (Exercise:
Show this is a basis. \( \epsilon, \epsilon^2, \ldots, \epsilon^{p-1} \). The Galois Group \( \Gamma(Q(\epsilon) : Q) \) consists of \( \sigma_i \) for \( 1 \leq i \leq p - 1 \) where \( \sigma_i(\epsilon) = \epsilon^i \). Associating \( \sigma_i \) with \( i \in \mathbb{Z}_p^* \), the group is isomorphic to \( \mathbb{Z}_p^* \). The unique subgroup \( H \) of \( \mathbb{Z}_p^* \) of index 2 (that is, size \( (p - 1)/2 \)) consists of the squares (modulo \( p \)). That is \( H \) has the automorphisms \( \sigma_{k^2} \) for \( 1 \leq k \leq p - 1 \). (Each square appears twice so there are \( (p - 1)/2 \) elements of \( H \). Now write an arbitrary element \( \alpha \in Q(\epsilon) \) with the new basis as

\[
\alpha = \sum_{i=1}^{p-1} a_i \epsilon^i
\]

(3)

For \( \alpha \in H^\dagger \) we need that for each \( k \) we have \( \sigma_{k^2}(\alpha) = \alpha \). That is,

\[
\alpha = \sigma_{k^2}(\alpha) = \sum_{i=1}^{p-1} a_i \epsilon^{k^2 i}
\]

(4)

Here as \( \epsilon^p = 1 \) we can consider the exponent \( k^2 i \) as calculated in \( \mathbb{Z}_p \). Thus the condition becomes

\[
a_i = a_{k^2 i} \text{ for all } i, k \in \mathbb{Z}_p^*
\]

(5)

But (5) just says that \( a_i \) is constant over the quadratic residues and constant (maybe a different constant) over the quadratic nonresidues. (0 is special and is counted neither as a quadratic residue nor as a quadratic non residue.) Let \( R, N \subset \mathbb{Z}_p^* \) denote the sets of quadratic residues and quadratic nonresidues respectively. Set

\[
\kappa = \sum_{r \in R} \epsilon^r = \frac{1}{2} \sum_{k=1}^{p-1} \epsilon^{k^2}
\]

(6)

\[
\lambda = \sum_{r \in N} \epsilon^r
\]

(7)

Then \( \kappa, \lambda \) form a basis for \( H^\dagger \). It is convenient to note that

\[
\kappa + \lambda = \sum_{r=1}^{p-1} \epsilon^r = -1
\]

(8)

so

\[
\lambda = -1 - \kappa
\]

(9)

and we can replace the basis \( \kappa, \lambda \) with the basis \( 1, \kappa \). Thus

\[
H^\dagger = \{ a + b \kappa : a, b \in Q \}
\]

(10)

is the unique quadratic extension of \( Q \) inside \( Q(\epsilon) \). Thus \( \kappa \) satisfies a quadratic equation (and is not itself rational) and one can write \( \kappa = a_1 + a_2 \sqrt{d} \) so that the unique quadratic extension of \( Q \) inside \( Q(\epsilon) \) can be written \( Q(\sqrt{d}) \).

One can also find \( \kappa \) explicitly. From (6) we find

\[
\kappa^2 = \frac{1}{4} \sum_{x,y=1}^{p-1} \epsilon^{x^2+y^2}
\]

(11)
This gets into some interesting number theory. For each \( r \in \mathbb{Z}_p \) one examines the number of solutions to the equation \( x^2 + y^2 = r \) over \( \mathbb{Z}_p \) with \( x, y \neq 0 \). Let \( r, s \) both be quadratic residues. Then we can write \( r = st^2 \). Each solution \( x^2 + y^2 = r \) corresponds to a solution of \( x_1^2 + y_1^2 = s \) by setting \( x_1 = xt, y_1 = yt \). We can go in the other direction, dividing a solution by \( t \).

Thus there is a value, call it \( R \), so that \( x^2 + y^2 = r \) has precisely \( R \) solutions for every quadratic residue \( r \). Now let \( r, s \) both be quadratic nonresidues. Again we can write \( r = st^2 \) and again the number solutions is the same. Thus there is value value, call it \( N \), so that \( x^2 + y^2 = r \) has precisely \( N \) solutions for every quadratic nonresidue \( r \). Also, let \( Z \) be the number of solutions to \( x^2 + y^2 = 0 \). We apply (11) to find

\[
\kappa^2 = \frac{1}{4} [Z + R\kappa + N\lambda] = \frac{1}{4} [Z + R\kappa + L(-1-\kappa)] = \frac{1}{4} [(Z - L) + (R - L)\kappa]
\] (12)

which we can solve by the quadratic formula. Actually, we won’t know the choice of \( \pm \) in the quadratic formula, but in either case we get \( Q(\kappa) = Q(\sqrt{d}) \) for the same explicit \( d \).

**Example:** Take \( p = 11 \) and \( \epsilon = e^{2\pi i/11} \). The residues are \( 1, 4, 9, 16 = 5, 25 = 3 \) so the nonresidues are \( 2, 6, 7, 8, 10 \). Then

\[
\kappa = \epsilon + \epsilon^3 + \epsilon^4 + \epsilon^5 + \epsilon^9
\] (13)

Now consider the terms in \( \kappa^2 \), always reducing the exponent modulo 11. We get (this is not always the case!) no terms of \( \epsilon^0 \). We get \( 2\epsilon^3\epsilon^9 = 2\epsilon^1 \) as well as \( 2\epsilon^3, 2\epsilon^4, 2\epsilon^5, 2\epsilon^9 \). For the nonresidues we get \( \epsilon^1\epsilon^1 + 2\epsilon^4\epsilon^9 = 3\epsilon^2 \) as well as \( 3\epsilon^6, 3\epsilon^7, 3\epsilon^8, 3\epsilon^{10} \). Thus

\[
\kappa^2 = 2\kappa + 3\lambda = 2\kappa + 3(-1-\kappa) = -3 - \kappa
\] (14)

so that

\[
\kappa = \frac{-1 \pm \sqrt{-11}}{2}
\] (15)

The unique quadratic field inside \( Q(\epsilon) \) is therefore \( Q(\sqrt{-11}) \).

Hmmmmmm, when \( p = 5 \) the quadratic field was \( Q(\sqrt{5}) \) and when \( p = 11 \) the quadratic field was \( Q(\sqrt{-11}) \). Coincidence? No! The quadratic field will be \( Q(\sqrt{p}) \) when \( p \) is a prime of the form \( 4k + 1 \) and will be \( Q(\sqrt{-p}) \) when \( p \) is a prime of the form \( 4k + 3 \). But we’ll leave this nice fact unproven.