Cyclotomic fields

Preliminary version. Version $-\infty+\epsilon$ — 22. oktober 2013 klokken 10:13

Roots of unity

The complex n-th roots of unity form a subgroup μ_n of the multiplicative group $\mathbb{C}^*$ of non-zero complex numbers. It is a cyclic group of order n, generated for example by $\exp 2\pi i/n$.

Any generator of μ_n is called a *primitive n-th root of unity*, and we shall denote such a root by ξ_n or merely ξ if n is clear from the context. If one primitive n-th root ξ is chosen, all the primitive n-th roots are of the form ξ^s where s can be any integer relatively prime to n. Since $\xi^n = 1$, the primitive n-th root are thus in one-one correspondence with the residue classes of integers relatively prime to n, that is, with the set of units in the ring $\mathbb{Z}/n\mathbb{Z}$. We stress that this correspondence is not canonical, but depends on the choice of the primitive root ξ.

We will in the sequel frequently refer to the subset of μ_n consisting of the *primitive* n-th root, and it is convenient to introduce the notation S_n for it.

THE AUTOMORPHISMS Since μ_n is abelian, the map $\mu_n \to \mu_n$ sending η to η^s is a group homomorphism. It is surjective, hence an isomorphism, precisely when s is relatively prime to n. Indeed, any primitive root, *i.e.,* a generator for μ_n, will then be mapped to a primitive root which is a generator. This shows that there is *canonical* isomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathrm{Aut}(\mu_n)$ sending the residue class of s to the s-power map $\eta \mapsto \eta^s$.

PROBLEM 1. Check that this canonical map is indeed an isomorphism. ✸

The order of $\mathrm{Aut}(\mu_n)$ is by definition the value taken by *Euler ϕ-function* at n, *i.e.,* $\phi(n) = |\mathrm{Aut}(\mu_n)|$. This is as well equal to the cardinality of the subset S_n. The following should be well known, but we offer a sketchy proof:

Proposition 1 *The ϕ-function has the following properties*

- ☐ *It is* multiplicative*, that is, $\phi(nm) = \phi(n)\phi(m)$ whenever n and m are relatively prime.*
- ☐ *If p^ν is a prime power, $\phi(p^\nu) = p^{\nu-1}(p-1)$. In particular, $\phi(p) = p-1$.*
- ☐ *For any natural number n one has $\frac{\phi(n)}{n} = \prod_{p|n}(1-\frac{1}{p})$.*

PROOF: The last statement follows immediately from the two first. If n and m are relatively prime, then $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ according to the Chinese remainder theorem, hence $(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$, and ϕ is multiplicative. That $\phi(p) = p-1$ is trivial, and the statement about the prime powers follows by an easy induction from the general lemma below with $I = p^{\nu-1}\mathbb{Z}/p^\nu\mathbb{Z}$. ❑

Lemma 1 *Let $R \to S$ be a surjective homomorphism between to rings with kernel I. Assume that $I^2 = 0$. Then there is an exact sequence of unit groups*

$$1 \longrightarrow 1 + I \longrightarrow R^* \longrightarrow S^* \longrightarrow 1$$

PROOF: Elements $1 + x$ with $x \in I$ are units since $(1 + x)(1 - x) = 1$, and they are exactly the units in R mapping to 1 in S. Every unit s in S can be lifted to an element r in R, which is easily checked to be a unit: Indeed, since if r' lifts s^{-1}, one has $rr' = 1+x$ with $x \in I$, and $1 + x$ is invertible. ❑

PROBLEM 2. Show that $\mathrm{Aut}(\mu_{p^\nu})$ is cyclic if p is an odd prime and that $\mathrm{Aut}(\mu_{2^s}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$. Show that $\mathrm{Aut}(\mu_{nm}) \simeq \mathrm{Aut}(\mu)_n \times \mathrm{Aut}(\mu)_m$ if n and m are relatively prime. ✸

NESTING The groups μ_n are nested, meaning that if $m|n$, then $\mu_m \subseteq \mu_n$. For any primitive n-th root of unity ξ, the subgroup μ_m is generated by $\xi^{n/m}$. If n and m are relatively prime, then $\mu_n \cap \mu_m = \{1\}$ and one has $\mu_{mn} = \mu_n\mu_m$.

PROBLEM 3. Show that $\mu_{mn} = \mu_n\mu_m$ in case n and m are relatively prime. HINT: Write $1 = an + bm$ so that any mn-th root satisfies $\eta = \eta^{an}\eta^{bm}$ ✸

The Galois group of the cyclotomic fields

Let n be a natural number. The field $\mathbb{Q}(\xi_n)$ obtained by by adjoining the primitive n-th root of unity ξ_n to the rationals, is called the *n-th cyclotomic field* or *the cyclotomic field of order n*.

The cyclotomic fields are nested just like the groups of roots of unity. If n and m are natural numbers such that $n|m$, then $\mathbb{Q}(\xi_n) \subseteq \mathbb{Q}(\xi_m)$. This holds since $\xi^{m/n}$ is a primitive n-th root of unity whenever $\xi \in S_m$.

PROBLEM 4. Show that if n is odd, then $\mathbb{Q}(\xi_{2n}) = \mathbb{Q}(\xi_n)$. HINT: If ξ is a n-th root of unity, the $2n$-th root of unity $-\xi$ is already in $\mathbb{Q}(\xi_n)$. ✸

The cyclotomic field $\mathbb{Q}(\xi_n)$ is the root field of the polynomial $x^n - 1$. Indeed, every root of $x^n - 1$ is a power of the primitive root ξ_n, and these powers generate $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$. Hence $\mathbb{Q}(\xi_n)$ is a Galois extension of $\mathbb{Q}$.

Two natural questions arise. What is the Galois group, and what is the minimal polynomial of ξ_n?

TH GALOIS GROUP The Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ acts canonically on μ_n (elements in $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ evidently takes n-th roots of unity to n-th roots of unity), and this action is faithful since the n-th roots generate the cyclotomic field $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$, so the only automorphism of $\mathbb{Q}(\xi_{\xi_n})$ over $\mathbb{Q}$ that leaves all of μ_n untouched, is the identity. We may therefore consider G to be contained in $\mathrm{Aut}(\mu_n)$, and indeed, we shall soon see that equality holds. The order of $\mathrm{Aut}(\mu_n)$ being $\phi(n)$, the equality is equivalent to the degree $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ being $\phi(n)$.

THE CYCLOTOMIC POLYNOMIALS We define the *n-th cyclotomic polynomial* to be the polynomial

$$\Phi_n(x) = \prod_{\xi \in S_n} (x - \xi) \qquad (\diamond)$$

where we remind you that S_n is the set of primitive n-th roots of unity. The cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial of lowest degree whose roots are exactly all the primitive n-th roots. It is of degree $\phi(n)$, and clearly it is a factor of $x^n - 1$.

Lemma 2 *The cyclotomic polynomial $\Phi_n(x)$ has integral coefficients, that is $\Phi_n(x) \in \mathbb{Z}[x]$.*

PROOF: An element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ permutes the primitive n-th roots of unity, hence it permutes the factors of $\Phi_n(x)$, and $\Phi_n(x)$ is invariant under $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$. But this means that the coefficients are invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, and hence they must be rational. By Gauss's lemma they are integers, since $\Phi_n(x)$ is a factor in $x^n - 1$. ❑

The case of n being a prime power deserves special emphasis. If p is a prime, and $n = p^\nu$ one has

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1$$
$$\Phi_{p^\nu}(x) = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = x^{p^{\nu-1}(p-1)} + \cdots + x^{p^{\nu-1}} + 1$$

PROBLEM 5. Apply Eisenteins criterion to $\Phi_p(x-1)$ to show that Φ_p is irreducible. ✸

PROBLEM 6. Apply Eisenteins criterion to $\Phi_{p^\nu}(x-1)$ to show that Φ_{p^ν} is irreducible. ✸

PROBLEM 7. Show that $\Phi_{p^\nu}(x) = \Phi_p(x^{p^{\nu-1}})$. ✸

As all conjugates of ξ_n are primitive n-th roots of unity, the minimal polynomial of ξ_n must be a factor of Φ_n. *A priori* there might be n-th roots not conjugate to ξ_n, but in the end of the day, will shall see that this is indeed not the case. Hence Φ_n will be the minimal polynomial of any primitive n-th root. This is equivalent to Φ_n being irreducible, and since the degree of Φ_n is $\phi(n)$, it is as well equivalent to the degree $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$ being equal to $\phi(n)$.

THE FUNDAMENTAL THEOREM We proceed to prove the result that the whole theory of cyclotomic fields is built on. There are close to infinity many ways to organize this material and a myriads of proofs of the main result, our favorite being one invented by Dedkind and brushed up by van der Waerden.

Theorem 1 *Let n be an integer. Then*

- ☐ $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = \mathrm{Aut}(\mu_n)$
- ☐ $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$
- ☐ *The cyclotomic polynomial* Φ_n *is irreducible.*

PROOF: We already observed hat these three statements are equivalent, and we attack the statement in the the middle, *i.e.,* we shall show that $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$.

Let $f(x)$ be the minimal polynomial of ξ_n. It divides $x^n - 1$, so $x^n - 1 = f(x)g(x)$ where both $f(x)$ and $g(x)$ have integral coefficients (by Gauss' lemma). Let p be a prime not dividing n. We shall prove the following statement:

☐ If ξ is a primitive root n-th root being a root of $f(x)$, then ξ^p is a root of $f(x)$ as well.

As any primitive root is of the form ξ^s with s relatively prime to n, this shows that all primitive roots are roots of $f(x)$, and hence that the degree of f equals $\phi(n)$.

Now, $g(\xi^p) = 0$ implies that $g(x^p)$ has $f(x)$ as a factor, *i.e.,* $g(x^p) = f(x)h(x)$ for some polynomial $h(x) \in \mathbb{Z}[x]$. Reducing mod p, one obtains the equality $\bar{g}(x^p) = \bar{g}(x)^p = \bar{f}(x)\bar{h}(x)$ in $\mathbb{F}_p[x]$. Hence $\bar{g}(x)$ and $\bar{f}(x)$ have a common factor, and $x^n - 1$ has a double root in some extension Ω of $\mathbb{F}_p$. However, this can not be the case, since the derivative nx^{n-1} is non-zero in $\mathbb{F}_p$ (the prime p is not a factor in n) and has no root in common with $x^n - 1$. ❑

THE GALOIS GROUP AND FROBENIUS ELEMENTS Every automorphism of μ_n is given as power map $\eta \to \eta^s$ for some s, and therefore—in view of that we just showed the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ being equal $(\mathbb{Z}/n\mathbb{Z})^*$— every element of $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ acts on the roots of unity $\eta \in \mu_n$ as $\eta \mapsto \eta^s$. This Galois element we shall denote by σ_s, that is, σ_s is given by the expression

$$\sigma_s(\sum_i a_i \xi^i) = \sum_i a_i \xi^{si},$$

where the summation extends over the range $0 \leq i \leq \phi(n) - 1$. If p is a prime not dividing n, the element σ_p is usually called *the Frobenius element*. It plays a significant role in the theory.

Proposition 2 *If n and m are relatively prime natural numbers, then the two cyclotomic fields $\mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_m)$ are linearly disjoint. Their composite $\mathbb{Q}(\xi_n, \xi_m)$is equal to $\mathbb{Q}(\xi_{nm})$, and $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$.*

PROOF: Clearly the composite of $\mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_m)$ contains $\mathbb{Q}(\xi_{nm})$, the product $\xi_n\xi_m$ being a primitive nm-th root of unity. The Euler ϕ-function is multiplicative, so $[\mathbb{Q}(\xi_{nm}) : \mathbb{Q}] = [\mathbb{Q}(\xi_n) : \mathbb{Q}][\mathbb{Q}(\xi_m) : \mathbb{Q}]$, and we are done. ❑

PROBLEM 8. Show that if n and m are relatively prime, then $[\mathbb{Q}(\xi_{nm}) : \mathbb{Q}(\xi_m)] = \phi(n)$. What is the minimal polynomial of ξ^{nm} over $\mathbb{Q}(\xi_m)$? ✸

PROBLEM 9. Let p be a prime. Show that $[\mathbb{Q}(\xi_{\pi^{v+\mu}}) : \mathbb{Q}(\xi_{p^\nu})] = p^\mu$. ✸

PROBLEM 10. Show that if A is any finite abelian group, then there exists a finite extension K of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq A$. ✸

The prime power case

Assume that $n = p^\nu$ for a prime p. Then we have

$$\Phi_{p^\nu}(x) = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = x^{p^v(p-1)} + \cdots + x^{p^\nu} + 1. \qquad (\spadesuit)$$

Indeed, a p^ν-th root being primitive means it is not a root of $x^{p^{\nu-1}} - 1$. Reducing the cyclotomic polynomial Φ_{p^ν} mod p one finds that the equality

$$\Phi_{p^\nu}(x) = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = \frac{(x-1)^{p^\nu}}{(x-1)^{p^{\nu-1}}} = (x-1)^{\phi(p^\nu)} \qquad (\bigstar)$$

holds in $\mathbb{F}_p[x]$. Hence, it is plausible that the ideal pA is the $\phi(\pi^\nu)$-th power of the principal ideal $(1-\xi)$, where A denotes the ring of integers in $\mathbb{Q}(\xi_{p^\nu})$. If we knew that $A = \mathbb{Z}[\xi]$, this would follow directly from Kummer's theorem about the ring of integers. It is true that $A = \mathbb{Z}[\xi]$, but for the time being we do not know that, and in fact, we shall use the decomposition of p in A to establish that $A = \mathbb{Z}[\xi]$. One has

Proposition 3 *Let p be a prime and let ξ be a p^ν-th root of unity. Let A be the ring of integers in the cyclotomic field $\mathbb{Q}(\xi_{p^\nu})$. The principal ideal $(1-\xi)A$ is a prime ideal of relative degree 1, and $(p)A = (1-\xi)^{\phi(p^\nu)}A$.*

We remark that $\mathbb{Q}(\xi_{p^\nu})$ is *totally ramified* at p. The case $v = 1$ merits a special mentioning. In that case, the prime p decomposes in $\mathbb{Q}(\xi_p)$ as $(p)A = (1-\xi)^{p-1}A$.

The following lemma is needed in the proof. It describes certain units in A called the *cyclotomic units*:

Lemma 3 *Let n be a natural number. If ξ and ξ' are two primitive n-roots, then $(1-\xi')/(1-\xi)$ is a unit in A_n.*

PROOF: There is an integer s, relatively prime to n, such that $\xi' = \xi^s$. The good old formula for the sum of a geometric series shows that

$$\frac{1-\xi'}{1-\xi} = 1 + \xi + \cdots + \xi^{s-1}.$$

Hence $(1-\xi')/(1-\xi)$ lies in A_n. Interchanging the roles of ξ and ξ' one sees that $(1-\xi)/(1-\xi')$ as well lies in A_n. ❑

PROOF OF THE PROPOSITION: The point of the proof is to compute the value $\Phi_{p^\nu}(1)$ of the cyclotomic polynomial Φ_{p^ν} at one in two different ways. On the one hand, putting $x = 1$ in (✦) one finds $\Phi_{p^\nu}(1) = p$. On the other hand, $x = 1$ in (✧) gives

$$\Phi_{p^\nu}(1) = \prod_{\xi' \in S_n} (1 - \xi') = (1 - \xi)^{\phi(p^\nu)} \prod_{\xi' \in S_n} \frac{1 - \xi'}{1 - \xi} = (1 - \xi)^{\phi(p^\nu)} \cdot \epsilon$$

where ϵ is a unit in A after lemma 3 above. Hence $p = \epsilon(1 - \xi)^{\phi(p^\nu)}$ and $pA = (1 - \xi)^{\phi(p^\nu)}A$.

Let $(1 - \xi)A = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}$ be the factorization of the principal ideal $(1 - \xi)A$ in a product of primes. Combining the equality

$$pA = (1 - \xi)^{\phi(n)}A = \mathfrak{p}_1^{\phi(n)e_1} \cdot \cdots \cdot \mathfrak{p}_r^{\phi(n)e_r}$$

with the fundamental equation relating degree, ramification indices and relative degrees from theorem 2 on page 15 in *Extensions*, we obtain the equality

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n) = \sum_{1 \le i \le r} e_i f_i \phi(n).$$

Clearly $r = 1$ and $e_1 = f_1$ is the only possibility, and therefore $1 - \xi$ is prime of relative degree one. This finishes the proof. ❑

PROBLEM 11. Show that $\Phi_{p^\nu}(x)$ is irreducible by applying Eisenstein's criterion to $\Phi_{p^\nu}(x - 1)$. HINT: Use the congruence (✯). ✸

The discriminant

One of the most important invariants of a number field is the discriminant, and it is both natural and of great interest to compute the discriminant of the cyclotomic fields. We do that in two steps. First, the discriminant of the cyclotomic fields of a prime power order is determined. It turns out to be a (high) power of p up to sign. In the second step we exploit the fact that cyclotomic fields of relatively prime order are linearly disjoint to give an induction argument where we appeal to proposition 11 on page 16.

Proposition 4 *Assume that p^ν is a prime power and that ξ is a primitive p^ν-th power of unity. The discriminant Δ of the power basis $1, \xi, \ldots, \xi^{\phi(p^\nu)-1}$ is given as*

$$\Delta = (-1)^{\phi(p^\nu)/2} p^{p^{\nu-1}(p\nu - \nu - 1)}.$$

PROOF: This is an exercise in norm computations, based on the formula

$$\Delta = (-1)^{d(d-1)/2} N_{\mathbb{Q}(\xi_{p^\nu})/\mathbb{Q}}(\Phi'_{p^\nu}(\xi))$$

where $d = [\mathbb{Q}(\xi_{p^\nu}) : \mathbb{Q}] = p^{v-1}(p-1)$. As a starter, we remark that the sign $(-1)^{d(d-1)/2}$ is the sign indicated stated in the proposition; but leaves the verification to the reader.

Now, as $x^{p^\nu} - 1 = (x^{p^{v-1}} - 1)\Phi_{p^\nu}(x)$, computing derivatives and evaluating at ξ, we obtain

$$\Phi'_{p^\nu}(\xi) = \frac{p^\nu \xi^{p^\nu - 1}}{\xi^{p^{v-1}} - 1} = \frac{p^v \xi^{-1}}{\eta - 1}$$

where we have introduced the primitive p-th root of unity $\eta = \xi^{p^{\nu-1}}$. We proceed by evaluating the norm of the nominator and the denominator separately.

For the nominator, ξ^{-1} being a primitive p^ν-root and hence of norm 1, we find (remember that the norm is homogeneous of degree the degree of the extension):

$$N_{\mathbb{Q}(\xi_{p^\nu})/\mathbb{Q}}(p^\nu \xi^{-1}) = p^{\nu\phi(p^\nu)} N_{\mathbb{Q}(\xi_{p^\nu})/\mathbb{Q}}(\xi^{-1}) = p^{\nu p^{\nu-1}(p-1)} \qquad (✪)$$

For the denominator, we split the extension in two along the tower of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\xi_p) \subseteq \mathbb{Q}(\xi_{p^\nu})$. We saw that $p = \epsilon(\eta-1)^{p-1}$, for a unit ϵ, hence $N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\eta-1)^{p-1} = N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(p) = p^{p-1}$, and therefore $N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\eta - 1) = p$. Hence

$$N_{\mathbb{Q}(\xi_{p^\nu})/\mathbb{Q}}(\eta-1) = N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(N_{\mathbb{Q}(\xi_{p^{m\nu}})/\mathbb{Q}(\xi_p)}(\eta-1)) = (N_{\mathbb{Q}(\xi_p)/\mathbb{Q}}(\eta-1))^{p^\nu - 1} = p^{p^{\nu-1}}. \quad (✳)$$

Putting equations (✪) and (✳) together we get what we wanted. ❑

For the moment we do not know that the ring of integers A is equal to $\mathbb{Z}[\xi_{p^n}]$, but once we have established that, the formula gives the discriminant $\delta_{\mathbb{Q}(\xi_n)/\mathbb{Q}}$. However, since the discriminant divides the discriminant of any integral basis, we can nevertheless conclude that $\mathbb{Q}(\xi_{p^\nu})$ is unramified over $\mathbb{Q}$ at all other primes than p. We proceed to give the general formula for the discriminant, but give the proof only up to sign.

Theorem 2 *Let n ne a natural number. Then the discriminant of the cyclotomic field $\mathbb{Q}(\xi_n)$ is given as*

$$\delta_{\mathbb{Q}(\xi_n)/\mathbb{Q}} = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$$

PROOF: we shall only prove the equality up to sign. Let $\rho(n)$ denote the absolute value of the right side of the equality in the theorem. It is a straight forward calculation to check that $\rho(nm) = \rho(n)^{\phi(m)}\rho(m)^{\phi(n)}$ whenever n and m are relatively prime. Indeed, we have the two equalities below—based on the multiplicativity of the Euler ϕ-function, n and m being relatively prime—and together they give the claim:

$$nm^{\phi(nm)} = (n^{\phi(n)})^{\phi(m)}(m^{\phi(m)})^{\phi(n)}$$

$$\prod_{p|nm} p^{\phi(nm)/p-1} = \prod_{p|n}(p^{\phi(n)/p-1})^{\phi(m)} \prod_{p|m}(p^{\phi(m)/p-1})^{\phi(n)}$$

To prove the theorem, we use induction on the number of distinct prime factors in n. If $n = 1$ the statement of the theorem is just the prime power case we in proposition

4 above. If n and m are relatively prime, then the discriminants $\delta_{\mathbb{Q}(\xi_n)/\mathbb{Q}}$ and $\delta_{\mathbb{Q}(\xi_m)\mathbb{Q}}$ are relatively prime by induction, and after proposition 2 on page 4 the fields $\mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_m)$ are linearly disjoint. Hence it follows from 11 on page 16 that

$$\delta_{\mathbb{Q}(\xi_{nm})/\mathbb{Q}} = \pm(\delta_{\mathbb{Q}(\xi_n)/\mathbb{Q}})^{\phi(m)}(\delta_{\mathbb{Q}(\xi_m)/\mathbb{Q}})^{\phi(n)},$$

and by the computation we did in the beginning of this proof, the theorem holds for $\mathbb{Q}(\xi_{nm})$.

❑

The ring of integers in $\mathbb{Q}(\xi_n)$

It is in general difficult to describe the rings of integers in algebraic number fields. Very seldom they have a primitive element. However, he cyclotomic fields $\mathbb{Q}(\xi_n)$ are exceptions. Their rings of integers all have primitive elements, they are generated by any primitive n-th root over $\mathbb{Q}$.

The proof of this result is divided into two parts. In the first part, the fact that cyclotomic fields of relatively prime degree are linearly disjoint, is used—via an induction on the number of distinct prime factors of n—to reduces the question to the prime power case. This cases is then treated, the main ingredient being that the prime p is totally ramified in $\mathbb{Q}(\xi_{p^\nu})$.

Theorem 3 *Let n be a natural number and let ξ_n be a primitive n-th root of unity. The ring A of integers in $\mathbb{Q}(\xi_n)$ is generated by ξ_n, that is $A = \mathbb{Z}[\xi_n]$.*

PROOF: Assume that n and m are two relatively prime numbers. The two cyclotomic fields $\mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_m)$ are then linearly disjoint extensions of the rationals, and the cyclotomic $\mathbb{Q}(\xi_{mn})$ is equal to the composite $\mathbb{Q}(\xi_n, \xi_m)$ of the two. The discriminants of $\mathbb{Q}(\xi_n)$ and $\mathbb{Q}(\xi_m)$ are relatively prime since their prime divisors are divisors of n and m respectively. From xxx and by induction on the number of prime factors, it follows that the ring of integers in the composite field—which is equal to $\mathbb{Q}(\xi_{nm})$— is the composite of the rings $\mathbb{Z}[\xi_n]$ and $\mathbb{Z}[\xi_m]$. One easily verifies that this ring coincides with $\mathbb{Z}[\xi_{nm}]$. Indeed, the product $\xi_n\xi_m$ is a primitive nm-root of one.

We are left with the prime power case, so assume that $n = p^\nu$ for a prime p. By xxx we know that the principal ideal $(1-\xi)A$ is a prime ideal lying over p of relative degree 1, that is $A/(1-\xi) = \mathbb{Z}/p\mathbb{Z}$, or in other words, $\pi A + \mathbb{Z}[\xi] = A$ where we have put $\pi = 1-\xi$ By induction on s it follows that $\pi^s A + \mathbb{Z}[\xi] = A$ for any natural number s. Indeed, we have

$$A = \pi A + \mathbb{Z}[x] \subseteq \pi^{s+1} A + \mathbb{Z}[\xi] \subseteq A$$

where the inclusion in the middle follows from the induction hypothesis. But $\pi^s A \subseteq \mathbb{Z}[x]$, for $s >> 0$, which is a consequence of the two facts that the discriminant Δ of the power basis is a power of π, and the that $\Delta A \subseteq \mathbb{Z}[\xi]$ as in proposition 24 on page 40 in *Discriminants*. Hence $A \subseteq \mathbb{Z}[\xi]$, and we are done. ❑

Decomposition of primes and Frobenius elements

One of the most fundamental questions about an algebraic number field is how a rational prime splits in the ring of algebraic integers. So also with the cyclotomic fields, but in that case, we are in the very lucky situation to have a not only complete answer, but a very natural, simple and elegant result.

In the proof the *Frobenius element* σ_p plays one of the main role, so we start by recalling what that is and establishing some of its properties. Then, in the cyclotomic field of order n, we decompose primes p not dividing the integer n. Finally we do the general case, which is rather simple reduction to the previous case.

THE FROBENIUS AUTOMORPHISM Fix a prime p not dividing n. Recall the definition of the corresponding *Frobenius element* in the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$. On a n-th root η it acts as the p-th power, that is $\sigma_p(\eta) = \eta^p$, and on a general element α the action is best described by expanding α in a basis $\mathcal{B}$ whose elements all are from n—for example a power basis $\mathcal{B} = \{1, \dots, \xi_n^{\phi(n)-1}\}$, where ξ_n is a fixed primitive n-th root of unity. So let $\alpha = \sum_{\xi\in\mathcal{B}} a_\xi \xi$, then the Frobenius map is given simply as

$$\sigma_p(\alpha) = \sum_{\xi\in\mathcal{B}} a_{Mx}\xi^p.$$

Of course, to get get the complete description one would have to expand each of the powers ξ^p in the basis, but luckily, we will not need that. The first property of the Frobenius we show, is its behavior mod p:

Lemma 4 *$\sigma_p(\alpha) = \alpha^p$ in A/pA.*

PROOF: One has

$$\alpha^p = (\sum_{\xi\in\mathcal{B}} a_\xi\xi)^p = \sum_{\xi\in\mathcal{B}} a_\xi^p\xi^p = \sum_{\xi\in\mathcal{B}} a_\xi\xi^p = \sigma_p(\alpha)$$

since the a_i's are integers and satisfy $a_i^p = a_i$ by little Fermat, and where we also use that the binomial coefficients $\binom{i}{p}$ all are 0 mod p when $1 < i < p$. ❑

The second important property of the Frobenius element is related to prime ideals lying over p. So let $\mathfrak{p}$ be one of them; that is $\mathfrak{p}$ is a prime in A with $\mathfrak{p}\cap\mathbb{Z} = (p)\mathbb{Z}$. One has

Lemma 5 *$\sigma_p(\mathfrak{p}) = \mathfrak{p}$.*

Otherwise said, the Frobenius element σ_p lies in the *decomposition groups* of the primes over p.

PROOF: Pick an element $\alpha \in \mathfrak{p}$. As $pA\subseteq\mathfrak{p}$ and $\sigma_p(\alpha) = \alpha^p + p\beta$ for some $\beta \in A$ by lemma 4, we see that α^p—and therefore α, the ideal $\mathfrak{p}$ being prime—belongs to $\mathfrak{p}$. Hence $\sigma_p(\mathfrak{p})\subseteq\mathfrak{p}$. Equality follows since σ_p is an automorphism. ❑

Let h be the least positive integer such that $p^h \equiv 1 \mod n$. Recall that we say that h is *the order of p modulo n*, and indeed, it is the order of the residue class p in the group of units $(\mathbb{Z}/n\mathbb{Z})^*$. As an element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, the Frobenius element σ_p has an order as well, and of course, the two orders are the same:

Lemma 6 *The order of the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ is the order of p modulo n, that is, the least positive integer h such that $p^h \equiv 1 \mod n$.*

PROOF: This pretty obvious: If ξ is a primitive n-th root, $\sigma_p^k(\xi) = \xi^{p^k}$ and this is equal to ξ if and only if $p^k \equiv 1 \mod n$. ❑

THE DECOMPOSITION OF PRIMES PRIME TO n Let $\mathfrak{p}$ be any prime in A lying over p. Then the residue field $\mathbb{F}_\mathfrak{p} = A_n/\mathfrak{p}$ is a finite extension of the field $\mathbb{F}_p$ whose degree $f = [\mathbb{F}_\mathfrak{p} : F_p]$ is the relative or local degree of $\mathfrak{p}$

From lemma 5 follows that the Frobenius element σ_p induces an automorphism of the field $\mathbb{F}_\mathfrak{p}$ which leaves elements of $\mathbb{F}_p$ fixed, hence an element in the Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. This group is cyclic of order f and is generated by the p-power map $x \mapsto x^p$. After lemma 4, the element σ_p induces this generating automorphism. This induced Frobenius automorphism (by the way, also usually called the Frobenius, which is not a coincidence) has an order which by the structure of finite fields is equal to the degree $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$, *i.e.,* the relative degree f.

If $\sigma_p^k = \mathrm{id}$, clearly the same applies to the reduction, so if h denotes the order of σ_p, one has $f|h$. We shall see that in fact equality holds. The point is the following:

Lemma 7 *The map $\mu_n \to \mathbb{F}_\mathfrak{p}^* = A/\mathfrak{p}^*$ that sends an element to its reduction modulo $\mathfrak{p}$ is an injective group homomorphism. Furthermore one has $p^f \equiv 1 \mod n$.*

PROOF: The polynomial has $x^n - 1$ all roots distinct in $\mathbb{F}_\mathfrak{p}$ since its derivative nx^{n-1} is non-zero modulo p and has no common root with $x^n - 1$. This means that μ_n is isomorphic with a subgroup of the group of units $\mathbb{F}_\mathfrak{p}^*$, and its order divides that of $\mathbb{F}_\mathfrak{p}^*$, in other words $n|p^f - 1$, or $p^f \equiv 1 \mod n$. ❑

This lemma shows that if h is the order of p modulo n, then $h|f$. On the other hand, we checked above that $f|h$, and hence $f = h$. We have

Proposition 5 *Assume that p is a prime not dividing n and let $\mathfrak{p} \subseteq A_n$ be a prime with $\mathfrak{p} \cap \mathbb{Z} = (p)$. The relative degree of $\mathfrak{p}$ over $\mathbb{Q}$ is the order of p mod n, that is the least positive integer f such that $p^f \equiv 1 \mod n$. One has $pA_n = \mathfrak{p}_1, \cdots \mathfrak{p}_s$ where the $\mathfrak{p}_i$'s are distinct primes in A_n and $s = \phi(n)/f$.*

PROOF: Most of this is done. We have checked the statement about the relative degree, and know that p is unramified. Hence $pA_n = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_s$ for some s, and the fundamental relation gives $\phi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}] = sf$. ❑

We remark that this proposition, by Kummer's theorem, this is equivalent to saying that the cyclotomic polynomial $\Phi_n(x)$ factors mod p as a product of s irreducible polynomials, each of degree f, where f and s are as in the theorem. Of course, this says nothing about the exact shape of those factors.

THE GENERAL CASE Now we describe the decomposition of any prime p regardless of its diving n or not. In line with the comment at the end of the previous paragraph, this amounts to describe the factorization of the cyclotomic polynomial $\Phi_n(x)$ in the ring $\mathbb{F}_p[x]$. This holds because of Kummer's result and the fact that the ring of integers in $\mathbb{Q}(\xi_n)$ equals $\mathbb{Z}[\xi_n]$ (which is needed in the ramified primes). The result is as follows:

Theorem 4 *Let n be a natural number and let p be a a rational prime. Let $n = p^\nu m$ where m does not have p as a factor. Then p decomposes in A_n as*

$$pA_n = (\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_s)^{\phi(p^\nu)}$$

where $s = \phi(n)/f$ and f is the order of p modulo m; that is, the least positive integer with $p^f \equiv 1 \mod m$.

PROOF: By the beginning remark, we need to show that in the ring $\mathbb{F}_p[x]$ there is a factorization

$$\Phi_n(x) = (\Psi_1(x) \cdot \cdots \cdot \Psi_s(x))^{\phi(p^\nu)}$$

where the Ψ_i's are irreducible of degree f.

Let η_i be the primitive p^ν-th roots of unity and ξ_j the primitive m-th roots. Then the products $\eta_i\xi_j$ are all the primitive n-th roots.

The η_i's are all congruent one modulo $\mathfrak{p}$, hence in $A/\mathfrak{p}$ one has

$$\Phi_n(x) = \prod(x - \eta_i\xi_j) = \prod_j (x - \xi_j)^{\phi(p^\nu)}$$

and the result follows by the unramified case. ❑

As an immediate application of this result, we can give a precise criterion for when a prime p splits completely in $\mathbb{Q}(\xi_n)$. By definition, this happens when p is unramified and the relative degrees of primes over p all are equal to one. By the theorem, this occurs exactly when $p \equiv 1 \mod n$. We have

Proposition 6 *Let n be a natural number and let p be a rational prime. Then p splits completely in the cyclotomic field $\mathbb{Q}(\xi_n)$ if and only if $p \equiv 1 \mod n$.*

Quadratic subfields of $\mathbb{Q}(\xi_p)$

Let p be an odd prime. The sign $(-1)^{(p-1)/2}$ pops up frequently in number theory, and the notation $p^* = (-1)^{(p-1)/2}p$ is used by many authors. We shall adopt that convention. In this paragraph we shall see that p^* has a square root in $\mathbb{Q}(\xi_p)$, and we shall exhibit an explicit formula for that root. This shows that the quadratic number field $\mathbb{Q}(\sqrt{p^*})$ is a subfield of the cyclotomic field $\mathbb{Q}(\xi_p)$, and in fact it turns out to be the only quadratic field contained there.

Proposition 7 *Let p be an odd prime. Then $\sqrt{p^*} \in \mathbb{Q}(\xi_p)$.*

PROOF: The identity (✧) with $n = p$ and $x = 1$ gives

$$\Phi_p(1) = \prod_{\xi \in S_p} (1 - \xi)$$

The cardinality of S_p is $p - 1$, and since $p \neq 2$ one has $\xi \neq \xi^{-1}$. The factors in the product above can be regrouped in the $(p-1)/2$ pairs $(1-\xi)(1-\xi^{-1})$, which gives the following formula where $S'_p \subseteq S_p$ is the subset with $(p-1)/2$ elements consisting of one of the elements from each pair $\{\xi, \xi^{-1}\}$.

$$p = \Phi_p(1) = \prod_{\xi \in S'_p} (1 - \xi)(1 - \xi^{-1}) = (-1)^{(p-1)/2} \epsilon \prod_{\xi \in S'_p} (1 - \xi)^2$$

where $\epsilon = \prod_{\xi \in S'_p} \xi^{-1}$ is an element in μ_p, and hence is a square (any element in μ_p is since p is odd). It follows that p^* is a square. ❑

As promised, we show that there no other quadratic fields in $\mathbb{Q}(\xi_p)$:

Proposition 8 *Let p be an odd prime. The field $\mathbb{Q}(\sqrt{p^*})$ is the only quadratic number field being a subfield of $\mathbb{Q}(\xi_p)$.*

PROOF: If $K \subseteq \mathbb{Q}(\xi_p)$ is a subfield of degree 2 over $\mathbb{Q}$, it is the fixed field of a subgroup of the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ of index two. But the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is cyclic, and a cyclic group has a unique subgroup of index two. Hence there is just one subfield being a quadratic extension of $\mathbb{Q}$. ❑

PROBLEM 12. Let p be a prime and let ξ be a primitive p-th root of unity.

a) Show that $\xi + \xi^{-1}$ is a real number and that it has exactly $(p-1)/2$ different conjugates, all of which are real. HINT: The conjugates are all of the form $\eta + \eta'$ for p-roots η of unity.

b) Show that the field $\mathbb{Q}(\xi + \xi^{-1}) = \mathbb{Q}(\cos(2\pi/p))$ is Galois over $\mathbb{Q}$ of degree $(p-1)/2$.

c) Show that the cyclotomic field $\mathbb{Q}(\xi)$ is an extension of $\mathbb{Q}(\xi + \xi^{-1})$ of degree two.

d) The Galois group $\mathbb{Q}(\xi)$ over $\mathbb{Q}$ is cyclic of order $p-1$. Hence has a unique element of order two. Show that that element is given by complex conjugation and that $\mathbb{Q}(\xi) \cap \mathbb{R} = \mathbb{Q}(\xi + \xi^{-1})$.

✸

PROBLEM 13. Describe all subfields of $\mathbb{Q}(\xi_5)$, $\mathbb{Q}(\xi_7)$, $\mathbb{Q}(\xi_{11})$ and of $\mathbb{Q}(\xi_{23})$. ✸

PROBLEM 14. Show that $\mathrm{Gal}(\mathbb{Q}(\xi_8)/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show that $\mathbb{Q}(\xi_8)$ contains exactly three quadratic fields. Give an explicit description of these three fields.

✸

Quadratic reciprocity

Recall the Legendre symbol $\left(\frac{a}{p}\right)$ where a is an integer and p is a rational prime. It takes the value 0 for integers a divisible by p , and 1 or -1 for the rest, according to a being a square mod p or not.

One has the equation $\left(\frac{a}{p}\right) \equiv (\bar{a})^{(p-1)/2} \mod p$.

The famous law of quadratic reciprocity states:

Theorem 5 *Let p and q be two different rational primes. Then one has*

$$(\frac{q}{p}) = (\frac{p^*}{q})$$

PROOF: We shall make use of the square root τ of p^* in the cyclotomic field $\mathbb{Q}(\xi_p)$ and of the Frobenius automorphism σ_q in $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$. The latter acts $\xi \mapsto \xi^q$ on roots of unity, hence corresponds to the residue class of q under the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \simeq (\mathbb{F}_p)^*$.

Clearly $\sigma_q(\tau) = \pm\tau$ (this being true for any automorphism of $\mathbb{Q}(\xi_p)$ since p^* is rational) and $\sigma_q(\tau) = \tau$ if and only if σ_q restricts to the identity in the Galois group of $\mathbb{Q}(\tau)$. By the Galois correspondence this Galois group is the unique quotient of order two of the cyclic group $\mathbb{F}_p^*$, the kernel of which consists of all squares in $\mathbb{F}_p^*$. Hence σ_q restricts to the identity if and only if q is a square mod p, that is, we have $\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau$.

On the other hand, $\sigma_q(\tau) \equiv \tau^q \mod q$. Hence in the ring A/qA (which contains the field $\mathbb{F}_q$) we have the equality

$$\sigma_q(\tau) = \tau^{q-1}\tau = (p^*)^{(q-1)/2}\tau = (\frac{p^*}{q})\tau$$

and we are done, since $\tau \neq 0$ in A/pA. Indeed if $\tau = aq$ with $a \in A$, taking norms, one gets the contradiction $(p^*)^{\phi(n)} = N(a)^2 q^{2\phi(n)}$.

❑

Linearly disjoint fields and composites

In this section let $K \subseteq \Omega$ be a field extension and suppose given two finite, separable subextensions L and M, that is two subfields of Ω both containing K and both finite and separable over K. The *composite of L and M*—denoted by LM— is the *smallest* subfield of Ω containing both of the fields L and M.

In geometry if you study one space X and are lucky enough to be able to split it in a direct product $Y \times Z$, where the two factors Y and Z are well known, then you know as much about X as about the two factors. This in contrast to having a just fibration (that is, a nice map) $X \to Y$ with fibres Z, where the interplay between properties of X the spaces Y and Z are much complicated.

In the worlds of fields, a tower $K \subseteq L \subseteq LM$ is analogous to a fibration, and we seek a condition that makes the tower as friendly a direct product. The answer is the notion of two subfields being *linearly disjoint*, which we develop in this paragraph.

There is ring-homomorphism $L \otimes_K M$ into Ω defined by sending the decomposable tensor $x \otimes y$ to xy and then extending this to the whole of $L \otimes_K M$ by bilinearity. The image of this map is a subring of Ω of finite dimension over K. And—as any finite ring extension of K which is an integral domain, is a field—we the image is a field. Clearly it contains both L and M, and therefore it is contained in any field containing both L and M. Thus it is equal to the composite LM. What we just argued for, is the first part of the following lemma

Lemma 8 *The composite of L and M is the image of the map $L \otimes_K M \to \Omega$ given by $x \otimes y \mapsto xy$. The degree of the composite field satisfies $[LM : K] \leq [L : K][M : K]$.*

The second part follows from the first since $\dim_K L \otimes_K M = \dim_K L \dim_K M$.

If $\{\alpha_i\}$ and $\{\beta_j\}$ are basises for L and M over K, the products $\alpha_i \beta_j$ form a generating set of the composite LM over K. In general there certainly will be dependencies, so that strict inequality holds, and the map induces by $x \otimes y \mapsto xy$ will not be injective, a naive example being the case that $M = L$. Then the composite equals L, but the space $L \otimes_K L$ is of dimension $[L : K]^2$. Along this line whenever the intersection $L \cap M$ differs from K, the fields L and M are not linearly disjoint over K. Indeed, assume that $x \in K \cap M$ is an element not lying in K. Then $x \otimes 1$ and $1 \otimes x$ are different elements in the tensor product, but of course they are mapped to the same element, namely x.

We say that the two fields L and M are *linearly disjoint over K* if this map is injective, *i.e.,* if the composite LM is isomorphic to the tensor product $L \otimes_K M$. Equivalently, L and M are linearly disjoint if the degree $[LM : K]$ is equal to the product $[L : K][M : K]$.

Proposition 9 *Let $K \subseteq \Omega$ be a field extension and let $K \subseteq L \subseteq \Omega$ and $K \subseteq M \subseteq \Omega$ be two finite subextensions. The following five statements are equivalent.*

- ☐ *The fields L and M are linearly disjoint over K.*
- ☐ $[LM : K] = [L : K][M : K]$
- ☐ $[L : K] = [LM : M]$
- ☐ *There is one K-basis for L which is an M-basis for LM.*
- ☐ *Any K-basis for L is an M-basis for LM.*

PROOF: The first point in the proof is the inequality

$$\dim L \otimes_K M = [L : K][M : K] \geq [LM : K] = [LM : M][M : K],$$

from which it follows that L and M are linearly disjoint if and only if $[LM : M] = [L : K]$.

Secondly, any K-basis for L form a generating set for LM over M since elements of LM are sums $\sum \alpha_i\beta_i$ with $\alpha_i \in L$ and $\beta_i \in M$. This generating set is a basis for LM over M if and only if $[LM : M] = [L : K]$. ❑

PROBLEM 15. This exercise exhibits an example of two extensions of $\mathbb{Q}$ with intersection equal $\mathbb{Q}$, but which are not linearly disjoint. Let $\alpha = \epsilon\sqrt[3]{2}$ and $\beta = \epsilon^{-1}\sqrt[3]{2}$ where ϵ is a primitive cube root of unity.

a) Show that $\alpha^2 + \alpha\beta + \beta^2 = 0$.

b) Show that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.

c) Show that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are not linearly disjoint over $\mathbb{Q}$. What is the composite of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$? HINT: Take a look at the root field of $x^3 - 2$?

✸

Dedekind rings in linearly disjoint extensions

Let A be a Dedekind ring with field of fractions K and assume that L and M are linearly disjoint extensions of K contained in some "big" extension Ω of K. We let A_L and A_M stand for the integral closure of A in L and M respectively, and A_{LM} denotes the integral closure of A in the composite field LM. Clearly the composite ring A_LA_M—that is, the smallest subring of Ω containing bot A_L and A_M—is contained in A_{LM}.

In this paragraph we explore the relations between these integral closures and their invariants, *i.e.,* their discriminants, with the emphasis on the question when $A_LA_M = A_{LM}$. Linearly disjointness is a must for such an equality, if that does not hold, not even the dimensions match. However it is not sufficient.In addition one needs that the discriminants are disjoint.

We continue working with two linearly disjoint extensions L and M of K.

Any integral basis $\mathcal{B}$ for L over K—that is a K-basis for L whose elements all are in A— is a basis for LM over M contained in A_LA_M. The matrix for the map ρ_x in the basis $\mathcal{B}$ is the same whether we regard ρ_x as a map from L to L or a map from LM to LM. The characteristic polynomial of the to multiplication map are therefore the same, and in particular

it holds that $\mathrm{tr}_{LM/M}(\beta) = \mathrm{tr}_{L/K}(\beta)$. Hence the discriminant $\Delta_{\mathcal{B}}$ of the K-basis $\mathcal{B}$ of L is the same as the discriminant of $\mathcal{B}$ regarded as an M-basis for LM, and $\Delta_{\mathcal{B}}A_{LM} \subseteq A_LA_M$ by proposition 25 on page 25 in *Discriminants*. Varying the integral basis $\mathcal{B}$ for L over K (recall that the discriminant ideal is generated by the discriminants of the all the integral basises), we have proven

Lemma 9 *With notation above*

$$\delta_{A_L/A}A_{LM} \subseteq A_LA_M.$$

Proposition 10 *Assume that the discriminants $\delta_{A_L/A}$ and $\delta_{A_M/A}$ are relatively prime. Then $A_L A_M = A_{LM}$.*

PROOF: Since $\delta_{A_L/A}$ and $\delta_{A_M/A}$ are supposed to be relatively prime, we have the equality $A = \delta_{A_L/A} + \delta_{A_M/A}$ which when multiplied with A_{LM} and combined with lemma 9 above, gives $A_{LM} = \delta_{A_L/A} A_{LM} + \delta_{A_M/A} A_{LM} \subseteq A_L A_M$. The other inclusion is trivial. ❏

Proposition 11 *Let K be the fraction field of the Dedekind ring A. Let L and M be finite, separable and linearly disjoint field extensions of K of degree n and m. Let the integral closure of A in L and M be respectively A_L and A_M.*

Assume that the discriminants $\delta_{A_L/A}$ and $\delta_{A_M/A}$ are relatively prime. Then they satisfy.

$$\delta_{BC/A} = \delta_{B/A}^m \delta_{C/A}^n.$$

Let $\mathcal{B}$ and $\mathcal{C}$ be basises for respectively L and M over K, we introduce the *ad hoc* notation $\mathcal{B} \otimes \mathcal{C}$ denote the basis of $L \otimes_K M$ whose elements are the products of the elements from $\mathcal{B}$ and $\mathcal{C}$.

Lemma 10 $\Delta_{\mathcal{B}\otimes\mathcal{C}} = \Delta_{\mathcal{B}}^m \Delta_{\mathcal{C}}^n$

PROOF: The proof relays on the fact that the discriminant of a basis equals the determinant of the transition matrix between the basis and the dual basis, as shown in lemma 13 on page 40 in *Discriminants*.

Let $\mathcal{B}$ be $\{x_1, \ldots, x_n\}$ and let $\{x_1, \ldots, x_n'\}$ be the dual basis. Let $\mathcal{C}$ be $\{y_1, \ldots, y_m\}$ and let $\{y_1', \ldots, y_m'\}$ be the dual basis. We claim that $\{x_i' y_j'\}$ is the dual basis of $\{x_i y_j\}$. Indeed, using the linearity and the functoriality of the trace in towers, on obtains

$$\begin{aligned} &\mathrm{tr}_{LM/K}(x_i y_j x_k' y_l') = \mathrm{tr}_{L/K}(\mathrm{tr}_{LM/L}(x_i y_j x_k' y_l')) = \mathrm{tr}_{L/K}(x_i x_k' \,\mathrm{tr}_{LM/L}(y_j y_l')) = \\ &= \mathrm{tr}_{L/K}(x_i x_k')(\mathrm{tr}_{LM/L}(y_j y_l')) \overset{\diamondsuit}{=} \mathrm{tr}_{L/K}(x_i x_k') \,\mathrm{tr}_{M/K}(y_j y_l') = \delta_{ik}\delta_{jl} \end{aligned}$$

where the equality marked $\diamondsuit$ holds since $\mathrm{tr}_{LM/L}(\beta) = \mathrm{tr}_{M/K}(\beta)$ for any element $\beta \in M$ as $LM = L \otimes_K M$.

The transition matrix between the basises $\{x_i y_j\}$ and $\{x_i' y_j'\}$ is the tensor product—or the Kronecker product as many call it—of the the transition matrix V between $\{x_i\}$ and $\{x_i'\}$ and the one, W, between $\{y_j\}$ and $\{y_j'\}$. One has

$$\Delta_{\mathcal{B}\otimes\mathcal{V}} = \det V \otimes W = \det V^m \otimes \det W^n = \Delta_{\mathcal{B}}^m \Delta_{\mathcal{C}}^n$$

❏

PROOF OF THE PROPOSITION: First of all, by localizing, we may assume that A is a principal ideal domain. Chose A-basises $\mathcal{B}$ for A_L and $\mathcal{C}$ for A_M. Then the discriminants $\Delta_{\mathcal{B}}$ and $\Delta_{\mathcal{C}}$ are generators for the (principal) discriminant ideals $\delta_{A_L/A}$ and $\delta_{A_M/A}$.

By proposition 10 we know that $A_{LM} = A_L A_M$, and hence $\mathcal{B} \otimes \mathcal{C}$ is an A-basis for A_{LM}, and the discriminant of the basis $\mathcal{B} \otimes \mathcal{C}$ is a generator for the discriminant ideal $\delta_{A_{LM}/A}$. The proposition then follows from Lemma 10 above. ❑