Math 430 Tom Tucker
NOTES FROM CLASS 10/27

Lemma 16.1. *Suppose that L is Galois over K. Let $\mathfrak{q}$ be maximal in B with $\mathfrak{q} \cap A = \mathfrak{p}$ and let $f = [B/\mathfrak{q} : A/\mathfrak{p}]$. Then* $\mathrm{N}(\mathfrak{q}) = \mathfrak{p}^f$.

Proof. Since we know that $\mathrm{N}(\mathfrak{q})$ is a power of $\mathfrak{p}$, it suffices to show that $A_{\mathfrak{p}} \mathrm{N}(\mathfrak{q}) = \mathfrak{p}^f$, which is equivalent to showing that $\mathrm{N}(S^{-1}B\mathfrak{q}) = \mathfrak{p}^f$, where $S = A \setminus \mathfrak{p}$. We write

$$\mathrm{N}(\mathfrak{q}) = \mathfrak{p}^\ell.$$

So it suffices to show this for $A = A_{\mathfrak{p}}$ and $B = S^{-1}B$. In this case, B is a principal ideal domain and we may write $\mathfrak{q} = B\pi$. Now, letting $G = \mathrm{Gal}(L/K)$, we see that

$$B\,\mathrm{N}(\mathfrak{q}) = B\,\mathrm{N}(B\pi) = \prod_{\sigma \in G} B\sigma(\pi) = B \prod_{\sigma \in G} \sigma(\mathfrak{q}).$$

Letting $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be the distinct conjugates of $\mathfrak{q}$, i.e. all the primes of B lying over $\mathfrak{p}$, we see that

$$B\,\mathrm{N}(\mathfrak{q}) = \mathfrak{q}_1^t \cdots \mathfrak{q}_m^t,$$

where $t = n/m$. (since n is the size of G). Now, we know that the relative degrees $[B/\mathfrak{q}_i : A/\mathfrak{p}]$ are all equal to some fixed number f, and likewise all the ramification indices are equal to some fixed e, so we have

$$B\mathfrak{p} = \mathfrak{q}_1^e \cdots \mathfrak{q}_m^e,$$

with $mef = n$, so $e = n/mf$. Thus, $t = f$, and our proof is complete. □

Theorem 16.2. *Let L be any finite separable extension of K and let A and B be a usual. Let $\mathfrak{q}$ be maximal in B with $\mathfrak{q} \cap A = \mathfrak{p}$ and let $f = [B/\mathfrak{q} : A/\mathfrak{p}]$. Then* $\mathrm{N}(\mathfrak{q}) = \mathfrak{p}^f$.

Proof. Let M be the Galois closure of L over K. Let R be the integral closure of B in M, which is also the integral closure of A in M. Let $\mathfrak{m}$ be a maximal ideal of R with $\mathfrak{m} \cap B = \mathfrak{q}$. From the previous Lemma, we know that $\mathrm{N}_{M/L}(\mathfrak{m}) = \mathfrak{q}^{[R/\mathfrak{m}:B/\mathfrak{q}]}$. By the previous Lemma and transitivity of the norm, we know that

$$\mathrm{N}_{L/K}(\mathfrak{q}^{[R/\mathfrak{m}:B/\mathfrak{q}]}) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathfrak{m})) = \mathrm{N}_{M/K}(\mathfrak{m}) = \mathfrak{p}^{[R/\mathfrak{m}:A/\mathfrak{p}]}.$$

Thus

$$\mathrm{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{\frac{[R/\mathfrak{m}:A/\mathfrak{p}]}{[R/\mathfrak{m}:B/\mathfrak{q}]}} = \mathfrak{p}^f,$$

where $f = [B/\mathfrak{q} : A/\mathfrak{p}]$. □

Now, a quick beginning to cyclotomic fields. All of this is over $\mathbb{Q}$. We will use the following notation a lot: ξ_m is called a *primitive root of unity* if $\xi^m = 1$ and $\xi^n \neq 1$ for all $1 \leq n < m$.

We let $\Phi(x)$ denote the polynomial $(x^p - 1)/(x-1)$. It is easily seen that $\Phi(x+1)$ is Eisenstein and therefore irreducible.

Before we continue with generalities about cyclotomic fields, a quick example with norms in the Gaussian integers.

An easy application. Which positive numbers m can be written as $a^2 + b^2$ for integers a and b?

Theorem 16.3. *A positive integer m can be written as $a^2 + b^2$ for integers a and b if and only if every prime $p \mid m$ such that $p \equiv 3 \pmod 4$ appears to an even power in the factorization of m.*

Proof. Let $B = \mathbb{Z}[i]$. Then $\mathrm{N}(a+bi) = a^2 + b^2$, for $a, b \in \mathbb{Z}$. Since B is a principal ideal domain, a positive integer $m = \mathrm{N}(a+bi)$ for some $a + bi \in B$ if and only if $(m) = \mathrm{N}(I)$ for some ideal I of B. Every ideal of B factors into prime ideals $\mathfrak{q}$. For each $\mathfrak{q}$ with $\mathfrak{q} \cap \mathbb{Z} = p$, we have $N(\mathfrak{q}) = (p)$ if p is not congruent to $3 \pmod 4$ and $N(\mathfrak{q}) = p^2$ if p is congruent to $3 \pmod 4$. Thus the possible norms of ideals of B are simply the integers m such that every prime $p \mid m$ such that $p \equiv 3 \pmod 4$ appears to an even power in the factorization of m. $\square$

Now, back to cyclotomic fields. Let $q = p^a > 2$. Let

$$\Phi_q(X) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \cdots + X^{p^{a-1}} + 1.$$

Then

$$\Phi_q(X) = \frac{X^q - 1}{X^{p^{a-1}} - 1}.$$

Let ξ_q be a primitive q-th root of unity. Then

$$\Phi_q(X) = \prod_{\substack{1 \leq k < q \\ (k,q)=1}} (X - \xi_q^k).$$

More generally we define the m-th cyclotomic polynomial as

$$\Phi_m(X) = \prod_{\substack{1 \leq k < m \\ (k,m)=1}} (X - \xi_q^k).\}$$

Recall the Euler ϕ-function given by

$$\phi(m) = \#\{k \mid 1 \leq k < m \text{ such that } (k,m) = 1.\}$$

(Here (k, m) is the greatest divisor of m and k.)

Recall the usual properties of ϕ, e.g. $\phi(ab) = \phi(a)\phi(b)$ if a and b are coprime and $\phi(p^a) = p^a - p^{a-1}$.

Theorem 16.4. *The polynomial $\Phi_q(X)$ is irreducible and is therefore the minimal monic for ξ_q.*

Proof. Note that $\Phi_q(1) = 1 + 1^2 + \cdots + 1^{p-1} = p$. Note also that if $\gcd(k, q) = 1$, then $(1 - \xi_q^k)/(1 - \xi_q) = 1 + \xi_q + \cdots + \xi_q^{k-1}$, so is in $\mathbb{Z}[\xi_q]$, and since $\xi_q = \xi_q^{kj}$ for j the inverse of k modulo q, we also have that $(1 - \xi_q)/(1 - \xi_q^k)$ is in $\mathbb{Z}[\xi_q]$. Thus, $(1 - \xi_q^k)/(1 - \xi_q)$ is a unit in $\mathbb{Z}[\xi_q]$. Thus, we have

$$\Phi_q(1) = \prod_{\substack{1 \le k < q \\ (k,q)=1}} (1 - \xi_q^k) = \prod_{\substack{1 \le k < q \\ (k,q)=1}} u_k(1 - \xi_q) = u(1 - \xi_q)^{\phi(q)},$$

where u_k and u are units (in $\mathbb{Z}[\xi_q]$). Similarly, for any k such that $(k, q) = 1$, we have $v(1 - \xi_q^k)^{\phi(q)} = p$ for a unit v. It follows that $(1 - \xi_q^k)$ is not a unit for $(k, q) = 1$. Now, if $\Phi_q(X) = F(X)G(X)$ for polynomials F and G over $\mathbb{Z}$, either $F(1) = \pm 1$ or $G(1) = \pm 1$. But since each is a product of $(1 - \xi_q^k)$ for various k, neither can be a unit, so Φ_q must be irreducible. □