Math 430 Tom Tucker
NOTES FROM CLASS 10/25

We will want to work with norms of ideals in a bit. There is one more thing to prove about norms first. First recall a lemma from last time.

Lemma 15.1. *Let L be a separable (not necessarily Galois) field extension of K of degree n, let M be the Galois closure of L over K, and let $G = \mathrm{Gal}(M/L)$. Let H_L be the subgroup of G that acts trivially on L and let $H\backslash G$ be a complete set of left coset representatives for G over H. Then, for any $y \in L$, we have*

$$T_{L/K}(y) = \sum_{\sigma \in H\backslash G} \sigma(y)$$

and

$$\mathrm{N}_{L/K}(y) = \prod_{\sigma \in H\backslash G} \sigma(y)$$

Proposition 15.2. *Let $K \subseteq E \subseteq L$ be finite seprable extension of K. Then, for any $y \in L$, we have*

$$\mathrm{N}_{L/K}(y) = \mathrm{N}_{E/K}(\mathrm{N}_{L/E}(y)).$$

Proof. Let M be a Galois extension of K that contains L and let $G = \mathrm{Gal}(M/K)$. Let H_E and H_L be the subgroups of G that act identically on E and L respectively. Note that H_E is the Galois group for M over E. Let $\tau_1, \dots, \tau_s$ represent the cosets $H_E\backslash G$ and $\gamma_1, \dots, \gamma_t$ represent the cosets $H_L\backslash H_E$, then the $\tau_i\gamma_j$ represent the cosets $H_L\backslash G$. Therefore,

$$\mathrm{N}_{L/K}(y) = \prod_{i,j}(\tau_i\gamma_j)(y) = \prod_{i=1}^{s} \tau_i(\prod_{j=1}^{t} \gamma_j(y)) = \mathrm{N}_{E/K}(\mathrm{N}_{L/E}(y)).$$

□

One more thing to prove before getting to norms of ideals.

Proposition 15.3. *Let B be a Dedekind domain with finitely many maximal ideals $\mathfrak{p}$. Then B is a principal ideal domain.*

Proof. It will suffice to show that every maximal ideal $\mathfrak{p}$ of B is principal. Let $\mathfrak{p}$ be a maximal ideal of B and let $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ be the other maximal ideals of B and let

$$I = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Then $\mathfrak{p}^2 + I = 1$. Since $\mathfrak{p} \neq \mathfrak{p}^2$ (by unique factorization), there is some $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. By Chinese Remainder Theorem, we may choose γ such that γ is congruent to 1 modulo I and congruent to a modulo $\mathfrak{p}^2$. Then the only possible factorization of (γ) is $(\gamma) = \mathfrak{p}$. □

Norms of ideals. Back on our usual set-up A Dedekind with field of fractions K, L a finite seprable extension of K of degree n, B the integral closure of A in L. We'll also want $A/\mathfrak{p}$ to be perfect for every maximal ideal $\mathfrak{p}$. We have already defined the norm $\mathrm{N}_{L/K} : L \longrightarrow K$; it sends B to A (since all the coefficients of the minimal polynomial of an integral element are integral). When it is clear what field we are working over we will omit the L/K subscript.

Definition 15.4. For any ideal $I \subset B$, we define the ideal $\mathrm{N}(I)$ to be the A-ideal generated by all $\mathrm{N}(x)$ for $x \in I$.

Properties of the norm (8.1 on p. 42)

Proposition 15.5. *The norm map has the following properties*

(1) $\mathrm{N}(By) = A\,\mathrm{N}(y)$ *for any* $y \in B$.
(2) *If* $S \subset A$ *is a multiplicative subset not containing 0, and* I *is an ideal of* B*, then* $\mathrm{N}(S^{-1}BI) = S^{-1}A\,\mathrm{N}(I)$.
(3) $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$*, for any ideals* I *and* J *of* B.

Proof. 1. We know the norm map is multiplicative since the determinant of matrices is. Since $\mathrm{N}(B) \subset A$, it follows that $\mathrm{N}(By) \subset A\,\mathrm{N}(y)$. Also, $\mathrm{N}(y) \subset \mathrm{N}(By)$, so $A\,\mathrm{N}(y) \subset \mathrm{N}(By)$, so $\mathrm{N}(By) = A\,\mathrm{N}(y)$.

2. For any $y \in S^{-1}BI$, we can write $y = x/s$ for $x \in I$ and $s \in S$. Then $\mathrm{N}(y) = \mathrm{N}(x/s) = \mathrm{N}(x)/s^n \in S^{-1}A\,\mathrm{N}(I)$, so $\mathrm{N}(S^{-1}BI) \subseteq S^{-1}A\,\mathrm{N}(I)$. On the other hand, $S^{-1}A\,\mathrm{N}(I)$ is generated as an $S^{-1}A$-module by $\mathrm{N}(I)$, and $\mathrm{N}(I) \subseteq \mathrm{N}(S^{-1}BI)$, so we have $S^{-1}A\,\mathrm{N}(I) \subseteq \mathrm{N}(S^{-1}BI)$.

3. This is surprisingly difficult, since we the norm is not additive. On the other hand, since any ideal of A is determined by its localizations at all the maximal $\mathfrak{p}$ of A, it will suffice to show that $A_\mathfrak{p}\,\mathrm{N}(I)A_\mathfrak{p}\,\mathrm{N}(J) = A_\mathfrak{p}\,\mathrm{N}(IJ)$. From 2, this means we only have to show that

$$\mathrm{N}(S^{-1}BI)\,\mathrm{N}(S^{-1}BJ) = \mathrm{N}(S^{-1}BIJ).$$

Since there are finitely many primes $\mathfrak{q} \in B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$, the ring $S^{-1}B$ has finitely many primes, hence is a principal ideal domain. So we write $S^{-1}Bx = S^{-1}BI$ and $S^{-1}By = S^{-1}BJ$. Then we have

$$\begin{aligned}\mathrm{N}(S^{-1}BI)\,\mathrm{N}(S^{-1}BJ) &= \mathrm{N}(S^{-1}Bx)\,\mathrm{N}(S^{-1}By)\\ &= \mathrm{N}(S^{-1}Bxy) = \mathrm{N}(S^{-1}BIJ),\end{aligned}$$

and we are done. ∎

Now, we want to figure out what the norm of a prime ideal in B is. We begin with a simple observation.

Lemma 15.6. *Let $\mathfrak{q} \cap A = \mathfrak{p}$ for $\mathfrak{q}$ a maximal ideal of B. Then* $\mathrm{N}(\mathfrak{q})$ *is a power of* $\mathfrak{p}$.

Proof. First of all, we know that $\mathrm{N}(\mathfrak{q})$ cannot be all of A since writing $\mathrm{N}(y)$ is a power of $y_1 \cdots y_m$ where the y_i are the conjugates of y, one of which is y itself. Thus $\mathrm{N}(y) \subseteq \mathfrak{q}$, so $\mathrm{N}(y) \subseteq \mathfrak{q} \cap A = \mathfrak{p}$. Since $\mathfrak{p} \subseteq \mathfrak{q}$ and $\mathrm{N}(a) = a^n$ ($n = [L : k]$, as usual), $\mathrm{N}(\mathfrak{q})$ contains a^n for every $a \in \mathfrak{p}$. So $N(\mathfrak{q})$ contains $\mathfrak{p}^n$. Thus, it cannot be contained in any maximal ideal other than $\mathfrak{p}$, since $\mathfrak{p}^2$ is prime to any maximal ideal other than $\mathfrak{p}$, and our proof is complete. □

Lemma 15.7. *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 15.8. *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 $f = [B/\mathfrak{q}_i : A/\mathfrak{p}] = f$. 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 $f = [B/\mathfrak{q} : A/\mathfrak{p}]$. $\square$

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. More on this next time.