Math 430 Tom Tucker
NOTES FROM CLASS 10/21

**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 $H = H_L$ be the subgroup of $G$ that acts trivially on $L$ and let $H\backslash G$ be a complete set of 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*

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

*Proof.* Let $y_1, \ldots, y_m$ be the conjugates of $y$. Then we know that

$$\mathrm{T}_{L/K}(y) = [L : K(y)] \left( \sum_{i=1}^{m} y_i \right)$$

and

$$\mathrm{N}_{L/K}(y) = \left( \prod_{i=1}^{m} y_i \right)^{[L:K(y)]}$$

(since the characteristic polynomial of $y$ must be a power of the minimal polynomial of $y$ and for the degrees to match up that power must be $[L : K(y)]$).

Now, let $H_y$ be the subgroup of $G$ that acts identically on $K(y)$. Then $H$ is a subgroup of $H_y$ and $H\backslash G$ will contain will contain $[H_y : H] = [L : K(y)]$ copies of $H_y\backslash G$.

Then

$$\begin{aligned} \sum_{\sigma \in H\backslash G} \sigma(y) &= [L : K(y)] \sum_{\sigma \in H_y\backslash G} \sigma(y) \\ &= [L : K(y)] \left( \sum_{i=1}^{m} y_i \right) = \mathrm{T}_{L/K}(y), \end{aligned}$$

and

$$\begin{aligned} \prod_{\sigma \in H\backslash G} \sigma(y) &= \prod_{\sigma \in H_y\backslash G} \sigma(y)^{[L:K(y)]} \\ &= \left( \prod_{i=1}^{m} y_i \right)^{[L:K(y)]} = \mathrm{N}_{L/K}(y)^{[L:K(y)]}, \end{aligned}$$

as desired. $\square$

**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 $\tau_1, \ldots, \tau_s$ represent the cosets $H_E \backslash G$ and $\gamma_1, \ldots, \gamma_t$ 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 maxima ideal of $B$ and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be the other maximal ideals of $B$. Then $\mathfrak{p}^2 \neq \mathfrak{p}$ by unique factorization of ideals, so there is a $\beta \in \mathfrak{p} \setminus \mathfrak{p}^2$. . We have that $\mathfrak{p}^2, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ are all coprime so we may apply the Chinese remainder theorem to find an $\alpha$ that is congruent to $\beta$ mod $\mathfrak{p}^2$ and congruent to 1 mod all the $\mathfrak{q}_i$. Then $B\alpha = \mathfrak{p}$. □

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.

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

**Proposition 15.4.** *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 $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ 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 $\gamma$ such that $\gamma$ is congruent to 1 modulo $I$ and congruent to $a$ modulo $\mathfrak{p}^2$. Then the only possible factorization of $(\gamma)$ 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 15.5.** 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 15.6.** *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 15.7.** *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. $\square$