Math 531 Tom Tucker
NOTES FROM CLASS 10/22

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

Lemma 23.1. *Let $\mathcal{Q} \cap A = \mathcal{P}$ for $\mathcal{Q}$ a maximal ideal of B. Then $\mathrm{N}(\mathcal{Q})$ is a power of $\mathcal{P}$.*

Proof. First of all, we know that $\mathrm{N}(\mathcal{Q})$ 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 $\mathrm{N}(y) \subseteq \mathcal{Q}$, so $\mathrm{N}(y) \subseteq \mathcal{Q} \cap A = \mathcal{P}$. Since $\mathcal{P} \subseteq \mathcal{Q}$ and $\mathrm{N}(a) = a^n$ ($n = [L : k]$, as usual), $\mathrm{N}(\mathcal{Q})$ contains a^n for every $a \in \mathcal{P}$. Since for every maximal $\mathcal{P}' \neq \mathcal{P}$ in A, there exists $x \in \mathcal{P}'$ such that $a + x = 1$ for some $a \in \mathcal{P}$, the element $w = (a+x)^n - x^n$ is in $\mathcal{P}'$ and $w + a^n = 1$. Therefore $\mathrm{N}(\mathcal{Q})$ cannot have $\mathcal{P}'$ in its factorization and must be a power of $\mathcal{P}$, as desired. $\square$

Lemma 23.2. *Suppose that L is Galois over K. Let $\mathcal{Q}$ be maximal in B with $\mathcal{Q} \cap A = \mathcal{P}$ and let $f = [B/\mathcal{Q} : A/\mathcal{P}]$. Then $\mathrm{N}(\mathcal{Q}) = \mathcal{P}^f$.*

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

$$\mathrm{N}(\mathcal{Q}) = \mathcal{P}^{\ell}.$$

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

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

Letting $\mathcal{Q}_1, \dots, \mathcal{Q}_m$ be the distinct conjugates of $\mathcal{Q}$, i.e. all the primes of B lying over $\mathcal{P}$, we see that

$$\mathrm{N}(\mathcal{Q}) = \mathcal{Q}_1^{t_1} \cdots \mathcal{Q}_m^{t_m},$$

where the $\sum_{i=1}^{m} t_i = n$. We also know that since $\mathrm{N}(\mathcal{Q})$ is a power of $\mathcal{P}$, and

$$\mathcal{P}B = \mathcal{Q}_1^e \cdots \mathcal{Q}_m^e$$

for some positive integer e, all of the t_i must equal $e\ell$ for ℓ. Thus, we have $m(e\ell) = n$. On the other hand, we know that the relative degrees $[B/\mathcal{Q}_i : A/\mathcal{P}]$ are all equal to some fixed f, so we have

$$n = \sum_{i=1}^{m} ef = mef.$$

This gives $mef = me\ell$, so $\ell = f$, as desired. □

Theorem 23.3. *Let L be any finite separable extension of K and let A and B be a usual. Let $\mathcal{Q}$ be maximal in B with $\mathcal{Q} \cap A = \mathcal{P}$ and let $f = [B/\mathcal{Q}_i : A/\mathcal{P}] = f$. Then* $\mathrm{N}(\mathcal{Q}) = \mathcal{P}^f$.

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 $\mathcal{M}$ be a maximal ideal of R with $\mathcal{M} \cap B = \mathcal{Q}$. From the previous Lemma, we know that $\mathrm{N}_{M/L}(\mathcal{M}) = \mathcal{Q}^{[R/\mathcal{M}:B/\mathcal{Q}]}$. By the previous Lemma and transitivity of the norm, we know that

$$\mathrm{N}_{L/K}(\mathcal{Q}^{[R/\mathcal{M}:B/\mathcal{Q}]}) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathcal{M})) = \mathrm{N}_{M/K}(\mathcal{M}) = \mathcal{P}^{[R/\mathcal{M}:A/\mathcal{P}]}.$$

Thus

$$\mathrm{N}_{L/K}(\mathcal{Q}) = \mathcal{P}^{\frac{[R/\mathcal{M}:A/\mathcal{P}]}{[R/\mathcal{M}:B/\mathcal{Q}]}} = \mathcal{P}^f,$$

where $f = [B/\mathcal{Q} : A/\mathcal{P}]$. □

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

Theorem 23.4. *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 $\mathbb{Z}$. Recall that from Problem 6 #4, we know that Show that $\mathbb{Z}[i]p$ factors as

$$\begin{array}{rcl} \mathcal{Q}^2 & ; & \text{if } p = 2 \\ \mathcal{Q}_1\mathcal{Q}_2 & ; & \text{if } p \equiv 1 \pmod 4 \\ \mathcal{Q} & ; & \text{if } p \equiv 3 \pmod 4), \end{array}$$

where $\mathcal{Q}, \mathcal{Q}_1, \mathcal{Q}_2$ are primes of $\mathbb{Z}[i]$ and $\mathcal{Q}_1 \neq \mathcal{Q}_2$. It follows that there is an ideal $\mathcal{Q}_p$ of B such that $\mathrm{N}(\mathcal{Q}) = \mathbb{Z}p$ if and only if p is not congruent to 3 mod 4. If $p \equiv 3 \pmod 4$, then pB is the only prime lying over p and $\mathrm{N}(pB) = (\mathbb{Z}p)^2$. Factoring m as

$$m = \prod_{\substack{p \not\equiv 3 \pmod 4 \\ p \mid m}} p^{s_i} \prod_{\substack{p \equiv 3 \pmod 4 \\ p \mid m}} p^{t_i}$$

Letting $\mathcal{Q}_p$ be as above, we see that the ideal

$$I = \prod_{\substack{p \not\equiv 3 \pmod 4 \\ p \mid m}} \mathcal{Q}_p^{s_p} \prod_{\substack{p \equiv 3 \pmod 4 \\ p \mid m}} (\mathcal{P}B)^{\frac{t_p}{2}}.$$

Has the property that $\mathrm{N}(I) = \mathbb{Z}m$. On the other hand if I is any ideal of B then $\mathbb{Z}_{(p)} \mathrm{N}(I) = (\mathrm{N}(B_{pB}I))^2$, for any $p \equiv 1 \pmod 4$, so if $\mathbb{Z}m = \mathrm{N}(I)$, then t_p is even. So we are done. $\square$

Now, let's begin working with 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

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

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

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

Lemma 23.5. *For any positive integer k with $(k,q) = 1$, the element*

$$\frac{1-\xi_q^k}{1-\xi_q}$$

is a unit in B.

Proof. Since $(1-\xi_q^k)/(1-\xi_q) = 1 + \xi_q + \cdots + \xi_q^{k-1}$, we see that $(1-\xi_q^k)/(1-\xi_q)$ is in B. Also, there exists a positive integer ℓ such that $k\ell \equiv 1 \pmod q$, so $\xi_q = (\xi_q^k)^\ell$. Hence the inverse of $(1-\xi_q^k)(1-\xi_q)$ which is

$$\frac{1-\xi_q}{1-\xi_q^k} = \frac{1-(\xi_q^k)^\ell}{1-\xi_q^k} = 1 + (\xi_q^k) + \cdots + (\xi_q^k)^{\ell-1}$$

is in B. So $(1-\xi_q^k)/(1-\xi_q)$ is a unit $\square$