Math 568 Tom Tucker
Notes from Class 11/5

Lemma 16.1. *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 $\mathcal{Q}_1, \ldots, \mathcal{Q}_m$ 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 16.2. *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 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 $\mathbb{Z}$. 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. □

Now, let's begin working with cyclotomic fields. We say that ξ_m is a primitive m-th root of unity if $\xi_m^m = 1$ but $\xi_m^d \neq 1$ for any $d < m$. We define the m-th cyclotomic as
$$\Phi_m(X) = \prod_{\substack{0 < i < m \\ \gcd(i,m)=1}} (X - \xi_m^i).$$
We will show that $\Phi_m(X)$ is irreducible for all m. Note that if $m = p^a$ for p a prime then $\Phi_m(X + 1)$ is Eistenstein so we know it is irreducible already.

Recall the definition:

$$\phi(m) = \#\{i \in \mathbb{Z} \mid 0 < i < m \text{ and } \gcd(i, m) = 1\}$$

Then the degree of Φ_m is $\phi(m)$. Recall that $\phi(p^a) = (p^a - p^{a-1})$ and that $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$ if $\gcd(m_1, m_2) = 1$.

Lemma 16.4. *Let $m = p^a$. Then:*

(i) $\mathbb{Z}[\xi_m]$ *is Dedekind;*
(ii) p *is the only prime that ramifies in* $\mathbb{Z}[\xi_m]$*;*
(iii) $p\mathbb{Z}[\xi_m] = (\xi_m - 1)^{\phi(m)}$.

To see that $\mathbb{Z}[\xi_m]$ id Dedekind recall that p is the only prime that divides $\Delta(\mathbb{Z}[\xi_m]/\mathbb{Z})$ and that the prime lying over p takes the form $(p, \xi_m - 1)$ since $\Phi_m(X)$ is congruent to a $(X-1)^{\phi(m)}$ modulo p. Since $N(\xi_m - 1) = \pm 1$, we see that $(p, \xi_m - 1) = (\xi_m - 1)$ is principal and therefore invertible. We just saw that p is the only prime that divides $\Delta(\mathbb{Z}[\xi_m]/\mathbb{Z})$ so p is the only prime that can ramify in $\mathbb{Z}[\xi_m]$ and that $p\mathbb{Z}[\xi_m] = (\xi_m - 1)^{\phi(m)}$ as desired.

Theorem 16.5. *For any m, we have $[\mathbb{Q}(\xi_m) : \mathbb{Q}] = \phi(m)$. Thus, Φ_m is irreducible.*

Proof. We proceed by induction on the number of prime factors of m. If m is a prime power then we are done since Φ_m is then Eistenstein. Now, assume m has n prime factors for $n > 1$. We write $m = m'p^a$. Then by induction $[\mathbb{Q}(\xi_{m'}) : \mathbb{Q}] = \phi(m')$ and $[\mathbb{Q}(\xi_{p^a}) : \mathbb{Q}] = \phi(p^a)$. Since $\mathbb{Q}(\xi_{m'})$ and $\mathbb{Q}(\xi_{p^a})$ are Galois, we will thus be done if we can show that $\mathbb{Q}(\xi_{m'}) \cap \mathbb{Q}(\xi_{p^a}) = \mathbb{Q}$. Write $\mathbb{Q}(\xi_{m'}) \cap \mathbb{Q}(\xi_{p^a}) = L$ and let $\mathcal{O}_L$ denote the ring of integers of L. Then $p\mathcal{O}_L = \mathcal{Q}^{[L:\mathbb{Q}]}$ since p ramifies completely in $\mathbb{Q}(\xi_{p^a})$. On the other hand p does not ramify in $\mathbb{Q}(\xi_{m'})$ so $[L : \mathbb{Q}] = 1$, and we are done. $\square$

Theorem 16.6. *For any m, the ring $\mathbb{Z}[\xi_m]$ is Dedekind.*

Proof. Again, we use induction on the number of prime factors of m. If m is a prime power, we are done by Lemma 16.4. Now we treat the inductive step. Let $\mathcal{M}$ be a prime in $\mathbb{Z}[\xi_m]$ and let $p\mathbb{Z} = \mathcal{M} \cap \mathbb{Z}$. If p doesn't divide m, then $\mathcal{M}$ is invertible, since p is prime to $\Delta(\mathbb{Z}[\xi_m]/\mathbb{Z})$. Otherwise, write $m = m'q^a$ where m' is prime to q and $p \neq q$, and let $\mathcal{P} = \mathcal{M} \cap \mathbb{Z}[xi_{m'}]$. Then $\mathbb{Z}[\xi_{m'}]$ is Dedekind by induction and $\Delta(\mathbb{Z}[\xi_m]/\mathbb{Z}[\xi_{m'}])$ is prime to $\mathcal{P}$, so $\mathcal{M}$ is invertible. Thus, $\mathbb{Z}[\xi_m]$ is Dedekind. $\square$