Math 430 Tom Tucker
NOTES FROM CLASS 10/27

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 16.1. *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 (mod 4) and $N(\mathfrak{q}) = p^2$ if p is congruent to 3 (mod 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

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

More generally we define the m-th cyclotomic polynomial as

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

Recall the Euler ϕ-function given by

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

(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 16.2. *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

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

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. □

The following is obvious now.

Corollary 16.3.

$$[\mathbb{Q}(\xi_q) : \mathbb{Q}] = \phi(q) = p^{a-1}(p-1).$$

Theorem 16.4. *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\xi_q)$ is $\mathbb{Z}[\xi_q]$. Furthemore, p ramifies completely in $\mathbb{Q}(\xi_q)$.*

Proof. Since $\Delta(\mathbb{Z}[\xi_q]/\mathbb{Z})$ is a power of p, the only primes in $\mathbb{Z}[\xi_q]$ that could fail to be invertible are those lying over p. On the other hand, by the Kummer theorem, the only prime lying over p in $\mathbb{Z}[\xi_q]$ is $(p, \xi_q - 1)$ since $\Phi_q(X)$ divides $(X^q - 1) \equiv (X-1)^q \pmod p$. We know that

$$(\xi_q - 1) \cdot \prod_{\substack{1<k<q \\ (k,q)=1}} (\xi_q^k - 1) = p,$$

and of course $(\xi_q^k - 1)$ is in $\mathbb{Z}[\xi_q]$ for any k, so

$$(p, \xi_q - 1) = (\xi_q - 1)$$

and is therefore principle and hence invertible. Since $(\xi_q - 1)$ has residue field $\mathbb{Z}/p\mathbb{Z}$ is the only prime that lies over p it follows that p ramifies completley in $\mathbb{Z}[\xi_q]$. □

Theorem 16.5. *Let m be any positive integer. Then $\mathbb{Z}[\xi_m]$ is Dedekind and the field $\mathbb{Q}(\xi_m)$ is Galois of degree of $\phi(m)$ over $\mathbb{Q}$. Thus, $\Phi_m(X)$ is irreducible over $\mathbb{Q}$ for all m.*

Proof. It is obvious that $\mathbb{Q}(\xi_m)$ is Galois. Indeed, $\xi_m^m = 1$ implies $\sigma(\xi_m)^m = 1$ for any conjugate $\sigma(\xi_m)$ of ξ_m. But every root of $x^m - 1 = 0$

is a power of ξ_m so is in $\mathbb{Q}(\xi_m)$. Hence, $\mathbb{Q}(\xi_m)$ is the splitting field for the minimal monic of ξ_m and is therefore Galois.

We will show that $\mathbb{Z}[\xi_m]$ is Dedekind and that $\mathbb{Q}(\xi_m)$ has degree$\phi(m)$ over $\mathbb{Q}$ by induction on the number r of distinct prime factors p of m. We have already treated the case $r = 1$. Then writing $m = m'q$ where m' has $r-1$ distinct prime factors and q is a prime power (which is prime to m'). The discriminant of $\mathbb{Z}[\xi'_m]$ divides $(m')^{m'}$ (the discriminant of $x^{m'} - 1$) so is prime to the discriminant of $\mathbb{Z}[\xi_q]$ (since $(m', q) = 1$). By this week's homework #5, it follows that $\mathbb{Z}[\xi_q, \xi_{m'}]$ is Dedekind, since $\mathbb{Z}[\xi'_m]$ and $\mathbb{Z}[\xi_q]$ are Dedekind by the inductive hypothesis and have coprime discriminants. Since ξ_m^q is a primitive m'-th root of unity and $\xi_m^{m'}$ is primitive q-th root of unity,

$$\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_q, \xi_{m'}],$$

so $\mathbb{Z}[\xi_m]$ is Dedekind.

To calculate the degree of $\mathbb{Q}(\xi_m)$ it will suffice to show that $\mathbb{Q}(\xi_q)$ and $\mathbb{Q}(\xi_{m'})$ are disjoint over $\mathbb{Q}$, since that means that the degree of $\mathbb{Q}(\xi_m)$ is the product of the degrees of $\mathbb{Q}(\xi_q)$ and $\mathbb{Q}(\xi_{m'})$, and $\phi(m) = \phi(q)\phi(m')$ since m' and q are relatively prime. Now p ramifies completely in $\mathbb{Q}(\xi_q)$, and not at all in $\mathbb{Q}(\xi_m)$ so $\mathbb{Q}(\xi_q) \cap \mathbb{Q}(\xi_{m'}) = \mathbb{Q}$, as desired, by a previous homework problem.

To see that $\Phi_m(X)$ is irreducible over $\mathbb{Q}$ for all m we simply note that $\deg \Phi_m(X) = \phi(m) = [\mathbb{Q}(\xi_m) : \mathbb{Q}]$. $\square$

Now quadratic reciprocity.

We can use cyclotomic fields to prove the quadratic reciprocity theorem. Recall the definition the quadratic residue symbol for a prime p. It is defined for an integer a coprime to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & : \ a \text{ is square} \pmod p \\ -1 & : \ a \text{ is not a square} \pmod p \end{cases}$$

From now on, p and q are distinct odd primes (there is also a form of quadratic reciprocity when one of them is 2, but we will not treat it). Quadratic reciprocity relates $\left(\frac{p}{q}\right)$ with $\left(\frac{q}{p}\right)$. It says that for p and q odd we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}}.$$

When p is odd and $(a, p) = 1$, we have

(1) $\left(\frac{a}{p}\right) = a^{(p-1)/2}$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;

(4) $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\mathrm{ord}(a)}}$, where $\mathrm{ord}_p(a)$ denotes the order of $a \pmod p$.

Properties 2, 3, and 4 follow immediately from 1. Property 1 follows from the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ has a primitive root θ and a is square mod p if and only if $a = \theta^r$ for some even r. Now, $(\theta^r)^{(p-1)/2} = 1$ if r is even and -1 is r is odd, so we are done.

We will give a simple proof of quadratic reciprocity by factoring p in $\mathbb{Z}[\xi_q]$.

Lemma 16.6. *The field $\mathbb{Q}(\xi_q)$ contains exactly one quadratic field. It is $\mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$.*

Proof. The field $\mathbb{Q}(\xi_q)$ is Galois since all the conjugates of ξ_q are powers of ξ_q and hence Φ_q splits completely in $\mathbb{Q}(\xi_q)$. It is clear that the Galois group is $(\mathbb{Z}/a\mathbb{Z})^*$ which is cyclic of even order, so there is exactly one subgroup of index 2, and one subfield of degree 2. Since $\mathbb{Q}(\xi_q)$ only ramifies at p, this quadratic field cannot ramify at 2, so it must have discriminant divisible only by q. There are only two possibilities $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. By checking the ramification at 2, we see that if $q \equiv 1 \pmod 4$ it is $\mathbb{Q}(\sqrt{q})$, if $q \equiv 3 \pmod 4$, then $-q \equiv 1 \pmod 4$, so it must be $\mathbb{Q}(\sqrt{-q})$. $\square$