Math 531 Tom Tucker
NOTES FROM CLASS 10/25

Theorem 24.1. *The polynomial $\Phi_q(X)$ is irreducible and is therefore the minimal monic for ξ_q.*

Proof. $\Phi_q(1) = 1 + 1^2 + \cdots + 1^{p-1} = p$. Also

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

where u_k and u are units and ϕ is the Euler ϕ-function. Similarly, for any k such that $(k,q) = 1$. We have $v(1-\xi_q)^{\phi(q)} = p$ 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 24.2.

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

Now, we want to calculate the discriminant $\Delta(\Phi_q)$. We'll want the following Lemma.

Lemma 24.3. *Let F and G be two monic polynomials over a field K. Let*

$$F(X) = \prod_{i=1}^{m} (X - \alpha_i)$$

and

$$G(X) = \prod_{j=1}^{n} (X - \beta_j).$$

Then

$$\Delta(FG) = \Delta(F)\cdot\Delta(G)\cdot\prod_{i=1}^{m} G(\alpha_i)^2.$$

Proof. Since

$$F(X)G(X) = \prod_{i=1}^{m}(X-\alpha_i)\prod_{j=1}^{n}(X-\beta_j),$$

we see that

$$\Delta(FG) = \prod_{i<k}(\alpha_i-\alpha_k)^2\prod_{j<\ell}(\beta_j-\beta_\ell)^2\prod_{i,j}(\alpha_i-\beta_j)^2. \tag{1}$$

For any fixed i, we have

$$\prod_{j=1}^{n}(\alpha_i - \beta_j)^2 = G(\alpha_i)^2.$$

Thus (1) becomes

$$\Delta(FG) = \Delta(F) \cdot \Delta(G) \cdot \prod_{i=1}^{m} G(\alpha_i)^2,$$

as desired. □

Theorem 24.4. *Let $q = p^a > 2$. Then*

$$\Delta(\Phi_q) = \pm p^{p^{a-1}(ap-a-1)}$$

with the minus-sign if and only if $p \equiv 3 \pmod 4$.

Proof. We'll apply the previous Lemma to $F(X) = (X^{p^{a-1}} - 1)$ and $G(X) = \Phi_q(X)$. Then $F(X)G(X) = (X^{p^a} - 1)$. We know then (from homework) that

$$\Delta(F(X)G(X)) = (-1)^{p^a(p^a-1)/2}(p^a)^{p^a}.$$

and

$$\Delta(F(X)) = (-1)^{p^{a-1}(p^{a-1}-1)/2}(p^{a-1})^{p^{a-1}}.$$

We also know that the roots α of F all satisfy $\alpha^{p^{a-1}} = 1$, so

$$\prod_{\substack{\alpha \\ F(\alpha)=0}} \Phi_q(\alpha) = 1 + \alpha^{p^{a-1}} + \cdots + \alpha^{p^{a-1}(p-1)}$$

$$= \prod_{\substack{\alpha \\ F(\alpha)=0}} p = p^{p^{a-1}}.$$

So, we know then that

$$\Delta(\Phi_q(X)) = \frac{(-1)^{p^a(p^a-1)/2}(p^a)^{p^a}}{(p^{2(p^{a-1})})\left((-1)^{p^{a-1}(p^{a-1}-1)/2}(p^{a-1})^{p^{a-1}}\right)}.$$

Now, we simply calculate the powers of (-1) and p that appear. The power of p will be

$$ap^a - 2p^{a-1} - (a-1)p^{a-1} = p^{a-1}(ap - 2 - a + 1) = p^{a-1}(ap - a - 1),$$

as desired. The power of (-1) will be

$$p^a(p^a-1)/2 - p^{a-1}(p^{a-1}-1)/2,$$

which is odd when $p \equiv 3 \pmod 4$, even when $p \equiv 1 \pmod 4$, and even when $p = 2$ and $a \geq 2$. □

Theorem 24.5. *The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\xi_q)$ is $\mathbb{Z}[\xi_q]$.*

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. $\square$

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

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

When $p = 2$, $\left(\frac{a}{2}\right) = 1$ for any odd a. 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) $\left(\frac{a}{p}\right) = 1$ if and only if the order of $a \pmod{p}$ divides $(p - 1/2)$.

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.

Continuing with quadratic reciprocity...

From now on, p and q are distinct primes. Let's also assume that q is odd. Quadratic reciprocity relates $\left(\frac{p}{q}\right)$ with $\left(\frac{q}{p}\right)$. It says that for p and q odd we have

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

What has this got to do with cyclotomic fields? The first fact is that $\left(\frac{p}{q}\right) = 1$ if and only if $x^2 - p$ factors mod q. When $p \equiv 1 \pmod{4}$, and $B = \mathbb{Z}[\sqrt{q}]$, this is the same thing as saying that

$$pB = \mathcal{Q}_1 \mathcal{Q}_2$$

(one prime for each factor). Why is this helpful? Because $\mathbb{Q}(\xi_q)$ contains a unique quadratic field.