Math 531 Tom Tucker
NOTES FROM CLASS 10/29

Theorem 25.1. *Let q be an odd prime.* $\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}$.

Proof. We'll continue to work in $\mathbb{Z}[\xi_q]$. The corollary about orders mod p still applies, so all we need to do is figure out when 2 splits into an even number of primes in $\mathbb{Z}[\xi_q]$. To check how $2R_E$ factors, for E the unique quadratic extension of in $\mathbb{Z}[\xi_q]$, we'll have to work with

$$\alpha = \frac{1+\sqrt{\epsilon(q)q}}{2}$$

instead of $\sqrt{\epsilon(q)q}$, since $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ is not integrally closed when localized at 2. The minimal polynomial for α is

$$x^2 - x + \frac{1-\epsilon(q)q}{4}.$$

We can check that this splits into linear factors over 2 if and only if $\frac{1-\epsilon(q)q}{4} \equiv 0 \pmod 2$. We check that when $\epsilon(q) = 1$, this means that $q \equiv 1 \pmod 8$ and that when $\epsilon(q) = -1$, this means that $q \equiv 7 \pmod 8$. Thus $\left(\frac{2}{q}\right) = 1$ if and only if $q \equiv 7 \pmod 8$ or $q \equiv 1 \pmod 8$. This is equivalent to saying that $(q^2-1)/8 \equiv 0 \pmod 2$, and we are done. □

************ One more thing before finishing up cyclotomic fields.

Theorem 25.2. *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 $\mathbb{Q}$.*

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 last week's homework #4, 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. 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 the degree of $\mathbb{Q}[\xi_m]$ over $\mathbb{Q}[\xi_{m'}]$ is $\phi(q)$ by the inductive hypothesis. To prove it suffices to show that $\Phi_q(X)$ is irreducible over $\mathbb{Z}[\xi_{m'}]$.

To calculate the degree of $\mathbb{Q}[\xi_m]$ it will suffice to show that the degree of $\mathbb{Q}[\xi_m]$ over $\mathbb{Q}[\xi_{m'}]$ is $\phi(q)$ by the inductive hypothesis. If $q = p^a$, we know that $p\mathbb{Z}[\xi_q]$ factors as $\mathbb{Z}[\xi_q](1-\xi_q)^{\phi(q)}$. Thus,

$$p\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_q](1-\xi_q)^{\phi(q)}\mathbb{Z}[\xi_m] = I^{\phi(q)},$$

for some ideal I of $\mathbb{Z}[\xi_m]$.

We also know that since $\Delta(\mathbb{Z}[\xi_{m'}]/\mathbb{Z})$ is prime to p, we have

$$p\mathbb{Z}[\xi_{m'}] = \mathcal{Q}_1 \cdot \mathcal{Q}_t$$

for distinct coprime $\mathcal{Q}_i$. It follows that for each $\mathcal{Q}_i$ we must have $\mathcal{Q}_i\mathbb{Z}[\xi_m] = \mathcal{M}_i^{\phi(q)}$ for some prime $\mathcal{M}_i$ in $\mathbb{Z}[\xi_m]$. This means that

$$[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_{m'})] \geq \phi(q).$$

Since $[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_{m'})] \leq \phi(q)$, this means that

$$[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_{m'})] = \phi(q),$$

as desired. $\square$