Minicourse on Quadratic Reciprocity: Supplementary Problems

Dr. Aaron Michael Silberstein
Sài Gòn, August 2013

1 Finite Fields

1. (Rabin’s irreducibility test). Let \( f(x) \in \mathbb{F}_p[x] \). Prove that \( f(x) \) is irreducible if and only if it divides \( x^{p^{(\deg f)}} - x \) but not \( x^{p^{(nk)}} - x \) for any \( k \mid \deg f \).

2. Let \( f \in K[x] \) for a field. Prove that \( (f(x), f'(x)) = 1 \) if and only if \( f \) is squarefree in \( L[x] \) for every field \( L \) containing \( K \).

3. Let \( f(x) \in \mathbb{F}[x] \) for some finite field \( \mathbb{F} \). Prove that if \( f \) is squarefree in \( \mathbb{F}[x] \) then \( f \) is squarefree in every extension of \( \mathbb{F} \). Prove that this is not true when I make \( \mathbb{F} = \mathbb{F}(t) \) for a finite field \( F \). We say that finite fields are perfect.

2 Uchida’s Theorem

This theorem appeared in the Osaka Journal of Mathematics, No. 14 (1977), pp. 155-157. Let \( R \) be a Dedekind domain — that is, \( R \) is an integral domain in which every prime ideal is maximal. Let \( K \) be the field of fractions of \( R \), and let \( L \) be a finite extension of \( K \). For each \( \alpha \in L \) we let \( \mu_\alpha(x) \) be its monic minimal polynomial over \( K \); we call \( \alpha \) \( R \)-integral if and only if \( \mu_\alpha(x) \in R[x] \). The integral closure \( M \) of \( R \) in \( L \) is the set of all \( R \)-integral elements of \( L \). We say that \( M = R[\beta] \) if every element of \( M \) can be written as a polynomial with \( R \)-coefficients in \( R \).

Recall that \( M \) is an \( R \)-module of rank \([L : K]\).

1. Let \( m \) be a maximal ideal of \( R[X] \). Prove that if \( m \) contains a monic polynomial, then \( m \) is of the form \( m = (p, f(X)) \) where \( p \) is a prime ideal of \( R \) and \( f(X) \) is an integral polynomial irreducible mod \( p \).

2. Let \( \alpha \in M \). Suppose there is a maximal ideal \( m \) of \( R[X] \) such that \( \mu_\alpha \in m^2 \). Using the above lemma, \( m = (p, f(X)) \) for some \( f \in R[X] \). Show that there exists \( t(X) \in R[X] \) and \( p \in p \) such that \( f(\alpha)t(\alpha)/p \in M \) but \( f(\alpha)t(\alpha)/p \notin R[\alpha] \).
3. Prove the converse: if $\mu_\alpha \notin m^2$ for any maximal ideal $m \subseteq R[x]$, then $R[\alpha] = M$ (hint: prove that every maximal ideal is invertible).

4. Use this to prove that the ring of integers in $\mathbb{Q}[\zeta_n]$ is exactly $\mathbb{Z}[\zeta_n]$. 