

ALGEBRAIC NUMBER THEORY W4043

1. HOMEWORK, WEEK 1, DUE SEPTEMBER 13

1. Compute the Legendre symbols

$$\left(\frac{7}{13}\right), \left(\frac{13}{7}\right), \left(\frac{23}{19}\right), \left(\frac{19}{23}\right).$$

Show that they verify quadratic reciprocity.

2. Find a cyclic generator of the multiplicative group of \mathbb{F}_p when $p = 17$ and $p = 23$. Explain how you found the generator. (Trial and error is a possible explanation, but there are better ways.)

3. A *quadratic field* is an extension of \mathbb{Q} of degree 2. Let $d \in \mathbb{Z}$ and assume d is not a square in \mathbb{Q} . Let $\sqrt{d} \in \mathbb{C}$ be a square root of d , and define $\mathbb{Q}(\sqrt{d})$ to be the subfield of \mathbb{C} consisting of elements of the form $\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ (you may want to verify that $\mathbb{Q}(\sqrt{d})$ is a field if you haven't seen this previously).

- (a) Prove that $\mathbb{Q}(\sqrt{d})$ is a quadratic field. Show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some integer d . Show that $\mathbb{Q}(\sqrt{d})$ is a Galois extension of \mathbb{Q} and determine its Galois group, indicating the action of non-trivial elements of $\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ on the typical element $a + b\sqrt{d}$.

- (b) Let d and d' be two integers that are not squares in \mathbb{Q} . Show that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ if and only if d/d' is a square in \mathbb{Q} . Use this result to give a complete (infinite) list of all quadratic fields.

- (c) Let $P(x) = ax^2 + bx + c \in \mathbb{Z}[x]$, with $a \neq 0$, and assume P is irreducible in $\mathbb{Q}[x]$. Let $\Delta = b^2 - 4ac$ be the discriminant of P . Show that $\mathbb{Q}(\sqrt{\Delta})$ is a splitting field for P . What are the possible values of Δ modulo 4?

- (d) Conversely, let $d \in \mathbb{Z}$ be a square-free integer (in other words, if p is a prime dividing d then p^2 does not divide d). Find a monic polynomial $Q \in \mathbb{Z}[x]$ with splitting field $\mathbb{Q}(\sqrt{d})$. If $d \equiv 1 \pmod{4}$ show that Q can be taken to have discriminant d ; if $d \equiv 2 \pmod{4}$ or $d \equiv 3 \pmod{4}$ show that Q can be taken to have discriminant $4d$.