PROBLEM SET 1

YIHANG ZHU

Exercise 1. For p an odd prime, let $\zeta \in \bar{\mathbb{F}}_p$ be a primitive 8-th root of unity. Show that $\zeta + \zeta^{-1}$ represents $\sqrt{2}$. Use this to prove $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Exercise 2. Let p be an odd prime. We view the Legendre symbol $(\frac{-1}{p})$ as an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \{\pm 1\}$, where -1 acts on $\mathbb{Q}(i)$ via $i \mapsto -i$. Show that $\sigma a \equiv a^p \mod \mathfrak{p}$ for $a \in \mathbb{Z}[i]$ and any prime factor $\mathfrak{p} \in \mathbb{Z}[i]$ of p. (Recall the different ways p factorizes into prime factors inside $\mathbb{Z}[i]$)

Exercise 3. Prove that a UFD is integrally closed.

Exercise 4. Show that the identity $3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ gives two essentially different factorizations of 21 into irreducible elements in the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$. Therefore $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Exercise 5. In the previous exercise, we saw that unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$ because for instance

$$3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

But we have the factorizations into prime ideals

$$\begin{aligned}
(3) &= (3, \sqrt{-5} + 1)(3, \sqrt{-5} - 1), \\
(7) &= (7, \sqrt{-5} + 3)(7, \sqrt{-5} - 3), \\
(1 + 2\sqrt{-5}) &= (3, \sqrt{-5} - 1)(7, \sqrt{-5} - 3) \\
(1 - 2\sqrt{-5}) &= (3, \sqrt{-5} + 1)(7, \sqrt{-5} + 3).
\end{aligned}$$

Prove these identities.