Exercise sheet 4
Quadratic residues and class groups

Exercise 1. [Quadratic reciprocity for the prime 2]

We define $G = e^{i\pi/4} + e^{-i\pi/4}$ for p an odd prime number.

(a) Prove that $G = \sqrt{2}$, and deduce that $G \cdot 2^{(p-1)/2} \equiv e^{i\pi p/4} + e^{-i\pi p/4} \mod p$ (in which number ring ?).

(b) Use this equality to obtain the value of $2^{(p-1)/2}$ modulo p in terms of the congruence of p modulo 8.

(c) Give finally the formula for the Legendre symbol $\left(\frac{2}{p}\right)$.

Exercise 2. [Jacobi symbol]

For $a \in \mathbb{Z}$ and $b = \prod_i p_i^{r_i}$ coprime (and the latter being odd and positive), one defines the *Jacobi symbol of a modulo b* by

$$\left(\frac{a}{b}\right) := \prod_i \left(\frac{a}{p_i}\right)^{r_i}.$$

(a) Give an example for which $\left(\frac{a}{b}\right) = 1$ but a is not square modulo b.

(b) Prove that $\left(\frac{a}{b}\right)$ only depends on the congruence class of a modulo b, and is multiplicative in a and in b.

(c) Compute $\left(\frac{-1}{b}\right)$ and $\left(\frac{2}{b}\right)$ in terms of the congruence classes of b modulo 4 and 8.

(d) Prove that for every a, b positive, odd and coprime, one has the same reciprocity formula

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$$

as for the Legendre symbol.

(e) Use it to devise an algorithm to compute efficiently the Jacobi symbol (hence also the Legendre symbol).

(f) Compute the Jacobi symbols $\left(\frac{7}{15}\right), \left(\frac{12}{43}\right), \left(\frac{13}{53}\right), \left(\frac{10}{99}\right)$.

Exercise 3. [Jacobi symbol and quadratic fields]

Fix $d \in \mathbb{Z}$, $d \neq 0, 1$ squarefree and $K = \mathbb{Q}(\sqrt{d})$.

(a) Recall how an odd prime p decomposes in K in terms of the Legendre symbol $\left(\frac{d}{p}\right)$.

(b) If d is odd, use the reciprocity formula to write it in terms of the Jacobi symbol $\left(\frac{p}{d}\right)$ and the congruence of p modulo 4.

(c) Use similar arguments in the cases $p = 2$ or d even.

(d) Give a complete description of the situation for some d, e.g. $d = -15, -7, 6, 11$.

Exercise 4. [Computation of some class groups]

Fix $d \in \mathbb{Z}$, $d \neq 0, 1$ squarefree and $K = \mathbb{Q}(\sqrt{d})$.

(a) With the usual $\mathbb{Z}$-basis of $\mathcal{O}_K$, compute the constant G appearing in the proof of finiteness of the class group (depending on the congruence of d modulo 4 and the sign of d).

(b) Recall why $\mathrm{Cl}\,\mathcal{O}_K$ is generated by the prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p}) \leq G$.

(c) Deduce that for $d = -2, -3, -7$, the ring $\mathcal{O}_K$ is principal.

(d) Now, we fix $K = \mathbb{Q}(\sqrt{6})$. Prove that $(2, \sqrt{6})$ is the unique prime ideal above 2 and that it is not principal. Prove the same for $(3, \sqrt{6})$, and that $(2, \sqrt{6})(3, \sqrt{6})$ is principal.

(e) Prove that the prime numbers 7 and 11 are inert in $\mathbb{Q}(\sqrt{6})$, while 5 is totally split.

(f) Using all these considerations, prove that the class group of $\mathbb{Z}[\sqrt{6}]$ is $\mathbb{Z}/2\mathbb{Z}$.