

Problem Set #4

What do we mean by ‘understanding’ something? We can imagine that this complicated array of moving things which constitutes ‘the world’ is something like a great game being played by the gods, and we are observers of the game. We do not know what the rules of the game are; all we are allowed to do is to watch the playing. Of course, if we watch long enough, we may eventually catch on to a few of the rules.

Our usual conventions remain in force: Throughout, D denotes a squarefree integer, $D \neq 1$, and $\mathcal{O}_D = \mathbf{Z}[\tau] = \mathbf{Z} + \mathbf{Z}\tau$, where $\tau = \sqrt{D}$ when $D \equiv 2, 3 \pmod{4}$, $\tau = \frac{1+\sqrt{D}}{2}$ when $D \equiv 1 \pmod{4}$.

EXPECTED RAMIFICATIONS

0. Let Δ be the discriminant of the polynomial $m(x)$ appearing in class (and in the last HW), so that $\Delta = 4D$ if $D \equiv 2, 3 \pmod{4}$ and $\Delta = D$ if $D \equiv 1 \pmod{4}$. Then a rational prime p ramifies in $\mathcal{O}_D$ if and only if $p \mid \Delta$.

CIRCULAR REASONING

1. In class, we stated the following version of Dirichlet’s Approximation Lemma:

Let $\alpha \in \mathbf{R}$. For every $Q \in \mathbf{Z}^+$, there is a positive integer $q \leq Q$ with $\|q\alpha\| \leq \frac{1}{Q+1}$.

(Here $\|x\|$ denotes the distance from x to the nearest integer.)

Prove this by viewing $0\alpha, 1\alpha, \dots, Q\alpha$ as elements of the group $\mathbf{R}/\mathbf{Z}$, identified with a circle of circumference 1, and looking at close neighboring points.

’NITS TO PICK

2. $\epsilon \in \mathcal{O}_D$ is a unit $\iff N(\epsilon) = \pm 1$.
3. Suppose $D < 0$. Then $\mathcal{O}_D^\times = \{\pm 1\}$ unless $D = -1$ or $D = -3$. If $D = -1$, then $\mathcal{O}_D^\times$ consists of the four fourth roots of unity. If $D = -3$, then $\mathcal{O}_D^\times$ consists of the six sixth roots of unity.
4. Verify the following naive algorithm for finding the “fundamental unit” of $\mathcal{O}_D$, when $D > 0$: Test $v = 1, 2, 3, \dots$ successively until one of $Dv^2 \pm 4$ is a square. Choosing the $-$ sign whenever there is a choice, write $u^2 = Dv^2 \pm 4$. Put $\epsilon_0 = \frac{1}{2}(u + v\sqrt{D})$. Then $\mathcal{O}_D^\times = \{\pm \epsilon_0^m : m \in \mathbf{Z}\}$.
Use this to determine the fundamental unit when $1 < D \leq 19$.
5. Suppose $n > 2$ and $D = n^2 + 1$ is squarefree. Then $\mathcal{O}_D^\times = \{\pm \epsilon_0^m : m \in \mathbf{Z}\}$ for $\epsilon_0 = n + \sqrt{n^2 + 1}$.
6. If p is a rational prime with $p \equiv 3 \pmod{4}$, then the fundamental unit $\epsilon_0 \in \mathcal{O}_p^\times$ has $N(\epsilon_0) = 1$.
7. (taken from Ireland and Rosen; compare with Problem #6) Let p be a rational prime with $p \equiv 1 \pmod{4}$. We (will) know from class that it is possible to find positive integers a, b with $a^2 - pb^2 = 1$. Among all such pairs, choose one where b is as small as possible.

- a) a is odd.
- b) $a \pm 1 = 2u^2$, $a \mp 1 = 2pv^2$, $2uv = b$,
- c) $u^2 - pv^2 = \pm 1$.
- d) the $-$ sign holds in part (c).
- e) if $\epsilon_0 \in \mathcal{O}_p^\times$ is the fundamental unit of $\mathcal{O}_p$, then $N(\epsilon_0) = -1$.

CIVILIZATION AND ITS DISCONTENTS

8. Let R be a domain. Say R has a civilized ideal theory if the following two conditions hold:
- (i) The nonzero ideals of R comprise a Unique Factorization Monoid under multiplication.
 - (ii) TO DIVIDE IS TO CONTAIN: If I, J are nonzero ideals of R , then $I \mid J$ if and only if $I \supseteq J$.

We showed in class that $\mathcal{O}_D$ has a civilized ideal theory.

- a) Suppose the domain R has a civilized ideal theory. Let K be the fraction field of R . If $\alpha \in K$ is a root of a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$, then $\alpha \in R$. (Compare with HW #2, 9(a).)

Again, imitate the proof of the rational root test. The case $\alpha = 0$ is immediate. Otherwise, write $\alpha = r/s$ where r, s are nonzero elements of R , and show that every atom divides the ideal (r) at least as many times as it divides the ideal (s) .

- b) Let $L = \mathbf{Q}[\sqrt{D}]$. If R is a subring of L not contained in $\mathbf{Q}$, and R has a civilized ideal theory, then $R \supseteq \mathcal{O}_D$. (Compare with HW #2, 9(b).)

This is one reason we have been so fixated on $\mathcal{O}_D$: it is the smallest candidate for a well-behaved subring of L with fraction field L !

THE LABOR OF DIVISION

9. (Motzkin; Dubois and Steger) Say that a domain R admits a division algorithm if the following holds: There is a size function $\phi: R \setminus \{0\} \rightarrow \mathbf{Z}^+ \cup \{0\}$ such that for every pair of $a, b \in R$, with $b \neq 0$, there are $q, r \in R$ with

$$a = bq + r \quad \text{and either } r = 0 \text{ or } \phi(r) < \phi(b).$$

In Homework #3, you determined all squarefree $D < 0$ for which $\mathcal{O}_D$ admits a division algorithm with the norm as the size function. These are exactly

$$D = -1, -2, -3, -7, -11. \quad (*)$$

Now we ask which $\mathcal{O}_D$, with squarefree $D < 0$, admit *some* division algorithm (possibly having nothing to do with the norm!).

Suppose $\mathcal{O}_D$ admits a division algorithm with size function ϕ .

- a) Among all nonzero, nonunit $\alpha \in \mathcal{O}_D$, select one for which $\phi(\alpha)$ is as small as possible. Then every residue class in $\mathcal{O}_D/(\alpha)$ is represented by an element of $\mathcal{O}_D^\times \cup \{0\}$.
- b) For squarefree $D < 0$ not belonging to the list (*), $\#(\mathcal{O}_D^\times \cup \{0\}) = 3$.
- c) For squarefree $D < 0$ not on the list (*), every nonzero nonunit $\beta \in \mathcal{O}_D$ has $N\beta > 3$.
- d) For squarefree $D < 0$, whenever $\mathcal{O}_D$ has a division algorithm, it has one with the norm as size function.

For example, there is no division algorithm *at all* on the ring $\mathcal{O}_{-19}$.