

Problem Set #5: A Very Nice Cake Shop

The class group is a bitter group and a sweet group. It is bitter because when it is non-trivial it makes a mess. It is sweet because it makes things interesting.

a bitter group



a sweet group



There is a cake shop in Belmont, which is north of Chicago. The class group is the same as this cake shop; it is a very nice cake shop.

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 $D \equiv 2, 3 \pmod{4}$, and $\tau = \frac{1+\sqrt{D}}{2}$ when $D \equiv 1 \pmod{4}$.

EASY PIECES?

These problems are intended as definition chases, understanding checks, applications of known theorems, and/or straightforward generalizations of familiar arguments.

0. Let p be a prime number. In every Ring R of size p , the distinct elements are $1, 1 + 1, \dots, 1 + 1 + \dots + 1$ (p times), and R is isomorphic to $\mathbf{Z}_p$.

Furthermore: All this is true even if we omit commutativity from our axiom list for a Ring.

1. Recall that $I, J \in \text{Id}(\mathcal{O}_D)$ are said to be dilation equivalent if $I = \lambda J$ for some nonzero $\lambda \in \mathbf{Q}[\sqrt{D}]$; in this case, we write $I \sim J$. Prove that if $I_1 \sim I_2$ and $J_1 \sim J_2$, then $I_1 J_1 \sim I_2 J_2$. This shows that our definition of multiplication in $\text{Cl}(\mathcal{O}_D)$ is well-defined.
2.
 - a) For each $B > 0$, there are only finitely many nonzero prime ideals P of $\mathcal{O}_D$ with $\|P\| \leq B$.
 - b) For each $B > 0$, there are only finitely many nonzero ideals I of $\mathcal{O}_D$ with $\|I\| \leq B$.
3. (Finiteness of the class group)
 - a) There is a constant $C = C(D)$ for which the following holds: Whenever $I \in \text{Id}(\mathcal{O}_D)$, there is a nonzero $\alpha \in \mathcal{O}_D$ and a $J \in \text{Id}(\mathcal{O}_D)$ such that $(\alpha) = IJ$ and $\|J\| \leq C$.
 - b) Every nonzero ideal I of $\mathcal{O}_D$ satisfies $[I] = [J]^{-1}$ for some $J \in \text{Id}(\mathcal{O}_D)$ with $\|J\| \leq C$.
 - c) $\text{Cl}(\mathcal{O}_D)$ is finite.
4. Show that $y^2 = x^3 - 5$ has no solutions $x, y \in \mathbf{Z}$, this time for real!

CLASS *not* DISMISSED

Below, $\Delta = \Delta(D)$ denotes the discriminant of the polynomial $m(x)$ discussed in class, so that $\Delta = D$ if $D \equiv 1 \pmod{4}$, $\Delta = 4D$ if $D \equiv 2, 3 \pmod{4}$.

If P is a prime ideal of $\mathcal{O}_D$ containing the prime p of $\mathbf{Z}$, we say P lies above p , and (correspondingly) that p lies below P . Thus: inert or ramified primes p lie below precisely one prime ideal of $\mathcal{O}_D$, while split primes p lie below two distinct prime ideals.

5. If $D < 0$ and each prime $p \leq \sqrt{|\Delta|/3}$ lies below only principal prime ideals, then every ideal of $\mathcal{O}_D$ is principal.

We will do this in class for $D \equiv 1 \pmod{4}$. Your task is to treat the case $D \equiv 2, 3 \pmod{4}$.

6. If $D > 0$ and each prime $p \leq \sqrt{\Delta/5}$ lies below only principal prime ideals, then every ideal of $\mathcal{O}_D$ is principal.
7. (a strengthening of the last two exercises) Prove that the class group $\text{Cl}(\mathcal{O}_D)$ is generated by the classes $[P]$ of the prime ideals P lying above rational primes

$$p \leq \begin{cases} \sqrt{|\Delta|/3} & \text{if } D < 0, \\ \sqrt{\Delta/5} & \text{if } D > 0. \end{cases}$$

8. Use the last exercise to determine the class groups of $\mathcal{O}_{14}$, $\mathcal{O}_{-23}$, $\mathcal{O}_{82}$. “Determine” means “give a familiar group that the class group is isomorphic to”.

Suggestions for -23 and 82 : For -23 , think deeply about the prime ideal factorization of $(\frac{3+\sqrt{-23}}{2})$. The case of 82 is more difficult. Start by considering $(10 + \sqrt{82})$. At some point, you will need to show that the (unique) prime ideal P above 2 is nonprincipal. For this, suppose P is principal, say $P = (\alpha)$. Then $(2) = P^2 = (\alpha^2)$, so $\alpha^2 = 2\epsilon$ for some unit $\epsilon \in \mathbf{Z}[\sqrt{82}]$ of norm 1 , with $\epsilon > 0$. Using that the fundamental unit $9 + \sqrt{82}$ in $\mathbf{Z}[\sqrt{82}]$ has norm -1 , deduce ϵ is a square in $\mathbf{Z}[\sqrt{82}]$, and then that $\sqrt{2} \in \mathbf{Q}[\sqrt{82}]$ — absurd!

A 'PORT IN THE STORM

Let G be a finite abelian group. The Davenport constant of G is the smallest positive integer d possessing the following property:

Whenever $g_1, g_2, g_3, \dots, g_d$ is a sequence of d (not necessarily distinct!) elements of G , there is a (nonempty) subsequence multiplying to the identity.

We denote the Davenport constant of G by $\text{Dav } G$.

9. $\text{Dav } G$ is well-defined. In fact, $\text{Dav } G \leq \#G$ (the cardinality of G). Equality holds for $\mathbf{Z}_m$.
10. If $\#G > 2$, then $\text{Dav } G > 2$.
11. The Fundamental Theorem of Finite Abelian Groups asserts that every finite abelian group G is isomorphic to a group of the form

$$\mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_k}, \quad m_1, \dots, m_k \in \mathbf{Z}^+,$$

where the operation is componentwise addition. (Ask your counselor if you haven't seen this!) If G admits this decomposition, then $\text{Dav } G \geq 1 + (m_1 - 1) + \cdots + (m_k - 1)$.

12. For every finite abelian group G , we have $\text{Dav } G \geq \frac{\log(2 \cdot \#G)}{\log 2}$. In particular, $\text{Dav } G \rightarrow \infty$ whenever $\#G \rightarrow \infty$.