Math 4527 (Number Theory 2)

Lecture #34 of 37 $\sim$ April 14, 2021

Computing Ideal Class Groups

- Computing Ideal Class Groups
- Minkowski's Bound

This material represents §9.2.1-9.2.2 from the course notes.

Reminders, I

Recall Minkowski's convex-body theorem:

Theorem (Minkowski's Theorem for General Lattices)

Let Λ be any lattice in $\mathbb{R}^n$ whose fundamental domain has volume V. If B is any open convex centrally-symmetric region in $\mathbb{R}^n$ whose volume is $> 2^n V$, then B contains a nonzero point of Λ.

Also recall the class group:

Definition

Let $R = \mathcal{O}_{\sqrt{D}}$ be a quadratic integer ring. The <u>ideal class group</u> is the set of ideal classes (where $I \sim J$ if $(a)I = (b)J$ for some nonzero a, b) of $\mathcal{O}_{\sqrt{D}}$ under multiplication.

Reminders, II

The ideal class group of $\mathcal{O}_{\sqrt{D}}$ *is* always a finite abelian group:

Theorem (Properties of the Class Group)

Suppose $R = \mathcal{O}_{\sqrt{D}}$ is a quadratic integer ring and let $[I]$ denote the ideal class of an ideal I of R. Then the following are true:

1. *If I is a nonzero ideal of R, then I contains a nonzero element α such that $N(\alpha) \leq (|D| + 1)N(I)$.*
2. *Every ideal class of R contains an ideal J such that $N(J) \leq |D| + 1$.*
3. *The ideal class group of $\mathcal{O}_{\sqrt{D}}$ is finite.*

Computing Class Groups, I

Item (2) in the proposition on the last slide gives us an explicit way to calculate the ideal class group of $\mathcal{O}_{\sqrt{D}}$.

- Explicitly, we need only compute all of the possible prime ideals having norm at most $D+1$, and then determine the resulting structure of these ideals under multiplication.

The cardinality of the class group also has a name:

Definition

If D is a squarefree integer not equal to 1, the <u>class number</u> of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ is the order of the ideal class group of $\mathcal{O}_{\sqrt{D}}$. The class number is often written as $h(D)$.

- The class number of $\mathcal{O}_{\sqrt{D}}$ is equal to 1 if and only if $\mathcal{O}_{\sqrt{D}}$ is a PID. A larger class number corresponds to having more inequivalent types of non-unique factorizations.

Computing Class Groups, II

<u>Example</u>: Show that the class group of $\mathbb{Z}[\sqrt{2}]$ is trivial and deduce that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain.

Computing Class Groups, II

<u>Example</u>: Show that the class group of $\mathbb{Z}[\sqrt{2}]$ is trivial and deduce that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain.

- From the proposition, we know that any ideal class contains an ideal J of norm at most 3.
- Then the only possible prime divisors of the norm are 2 and 3, so the only possible prime ideal divisors of J are the primes lying above 2 and 3.
- Using the Dedekind-Kummer factorization theorem shows that in $\mathbb{Z}[\sqrt{2}]$ we have $(2) = (\sqrt{2})^2$ while the ideal (3) is inert and has norm 9, and so the only possible ideals J are (1), of norm 1, and $(\sqrt{2})$, of norm 2.
- Since both of these ideals are principal, we conclude that every ideal of $\mathbb{Z}[\sqrt{2}]$ is principal and so $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain.

Computing Class Groups, III

Example: Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

Computing Class Groups, III

Example: Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

- From the proposition, we know that any ideal class contains an ideal J of norm at most 6.
- Then the only possible prime divisors of the norm are 2, 3, and 5 so the only possible prime ideal divisors of J are the primes lying above 2, 3, and 5.
- Using the Dedekind-Kummer factorization theorem (or appealing to our analysis from earlier) shows that in $\mathbb{Z}[\sqrt{-5}]$ we have $(2) = (2, 1+\sqrt{-5})^2$, $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, and $(5) = (\sqrt{-5})^2$.
- Thus, the possible prime ideals dividing J are $I_2 = (2, 1+\sqrt{-5})$ of norm 2, $I_3 = (3, 1+\sqrt{-5})$ and $I_3' = (3, 1-\sqrt{-5})$ both of norm 3, and $I_5 = (\sqrt{-5})$ of norm 5.

Computing Class Groups, IV

Example: Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

Computing Class Groups, IV

Example: Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

- As we have previously shown, the ideal I_2 is not principal, so since $I_2^2 = (2)$ we see that $[I_2]$ is an element of order 2 in the class group.
- We have also previously shown that $I_2 I_3 = (1 + \sqrt{-5})$, so $[I_3] = [I_2]^{-1} = [I_2]$, and then since $I_3 I_3' = (3)$ we see $[I_3'] = [I_2]$ as well.
- Thus, since I_5 is principal, we see that all of the nonprincipal ideals lie in the same class (namely, the class $[I_2]$) and so the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

Computing Class Groups, V

<u>Example</u>: Determine the class group of $\mathbb{Z}[\sqrt{6}]$ and decide whether it is a principal ideal domain.

Computing Class Groups, V

Example: Determine the class group of $\mathbb{Z}[\sqrt{6}]$ and decide whether it is a principal ideal domain.

- From the proposition, we know that any ideal class contains an ideal J of norm at most 7.
- Then the only possible prime divisors of the norm are 2, 3, 5, and 7, so the only possible prime ideal divisors of J are the primes lying above 2, 3, 5, and 7.
- Using the Dedekind-Kummer factorization theorem shows that in $\mathbb{Z}[\sqrt{6}]$ we have $(2) = (2, \sqrt{6})^2$, $(3) = (3, \sqrt{6})^2$, $(5) = (5, 1 + \sqrt{6})(5, 1 - \sqrt{6})$, and (7) is inert.
- Thus the possible prime ideals dividing J are $I_2 = (2, \sqrt{6})$ of norm 2, $I_3 = (3, \sqrt{6})$ of norm 3, and $I_5 = (5, 1 + \sqrt{6})$ and $I_5' = (5, 1 - \sqrt{6})$ both of norm 5. (Note that $I_7 = (7)$ cannot divide J since its norm is 49.)

Computing Class Groups, VI

<u>Example</u>: Determine the class group of $\mathbb{Z}[\sqrt{6}]$ and decide whether it is a principal ideal domain.

- In fact we can see I_2 is principal, since it contains $2-\sqrt{6}$ and both 2 and $\sqrt{6}$ are divisible by $2-\sqrt{6}$.
- Likewise, I_3 is principal since it contains $3-\sqrt{6}$ and both 3 and $\sqrt{6}$ are divisible by $3-\sqrt{6}$, and also I_5 (hence also its conjugate I_5') is principal since $1+\sqrt{6}$ divides 5.
- Thus, no matter what the ideal J is, it is principal, and so the class group of $\mathbb{Z}[\sqrt{6}]$ is $\boxed{\text{trivial}}$, and $\mathbb{Z}[\sqrt{6}]$ is a PID.

Minkowski's Bound, I

Our ability to compute the class group of $\mathcal{O}_{\sqrt{D}}$ relies upon being able to get a good estimate on the norm of the smallest nonzero element in an ideal I.

- If D is negative, then the elements of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ naturally form a lattice in the complex plane. Then any nonzero ideal I will form a sublattice, to which we can then apply Minkowski's convex-body theorem to obtain an element of small norm.
- If D is positive, we will have to take a slightly different approach to embed $\mathcal{O}_{\sqrt{D}}$ into $\mathbb{R}^2$ as a lattice, but we will be able to do essentially the same thing. The idea in this case is instead to map an element $\alpha \in \mathcal{O}_{\sqrt{D}}$ to the point $(\alpha, \overline{\alpha}) \in \mathbb{R}^2$.

Minkowski's Bound, II

Now we can define the Minkowski embedding:

Definition

Suppose D is a squarefree integer not equal to 1. We define the *<u>Minkowski embedding</u>* $\varphi : \mathcal{O}_{\sqrt{D}} \to \mathbb{R}^2$ *as follows: if $D < 0$, we map the element $a + b\sqrt{D} \in \mathcal{O}_{\sqrt{D}}$ to $(a, b\sqrt{|D|})$, and if $D > 0$, we map the element $a + b\sqrt{D} \in \mathcal{O}_{\sqrt{D}}$ to $(a + b\sqrt{D}, a - b\sqrt{D})$.*

- It is easy to see that the Minkowski map φ is a homomorphism of additive groups (i.e., it is $\mathbb{Z}$-linear).
- Thus, the image of $\mathcal{O}_{\sqrt{D}}$ will be a 2-dimensional lattice spanned by the vectors $\varphi(1)$ and $\varphi(\omega)$, where ω is a generator of $\mathcal{O}_{\sqrt{D}}$.

Minkowski's Bound, III

The image of $\mathcal{O}_{\sqrt{D}}$ will be a 2-dimensional lattice Λ in $\mathbb{R}^2$.

- If $D < 0$, the Minkowski embedding is simply the result of identifying the elements of $\mathcal{O}_{\sqrt{D}}$ as points in the complex plane.
- For $D < 0$, the lattice is spanned by $\varphi(1) = (1, 0)$ and $\varphi(\omega)$, which is either $(0, \sqrt{|D|})$ or $(1/2, \sqrt{|D|}/2)$ according to whether $D \equiv 2, 3$ or $D \equiv 1 \pmod 4$.
- If $D > 0$, the lattice is spanned by the linearly-independent vectors $\varphi(1) = (1, 1)$ and $\varphi(\omega) = (\omega, \overline{\omega})$, which is either $(\sqrt{D}, -\sqrt{D})$ or $(\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2})$.

Minkowski's Bound, IV

In order to apply Minkowski's theorem, we need to compute the volume of the fundamental domain of the lattice. This turns out to be most easily written in terms of the discriminant Δ, which I introduced on the last homework:

Definition

If $\mathcal{O}_{\sqrt{D}}$ is a quadratic integer ring, the discriminant of $\mathcal{O}_{\sqrt{D}}$ is defined to be $\Delta = \begin{cases} 4D & \text{if } D \equiv 2,3 \text{ (mod 4)} \\ D & \text{if } D \equiv 1 \text{ (mod 4)} \end{cases}$.

Minkowski's Bound, V

Now we can give Minkowski's bound:

Theorem (Minkowski's Bound)

Suppose D is a squarefree integer not equal to 1, let Δ be the discriminant of $\mathcal{O}_{\sqrt{D}}$, and let $\varphi : \mathcal{O}_{\sqrt{D}} \to \mathbb{R}^2$ be the Minkowski embedding with $\Lambda = \varphi(O_{\sqrt{D}})$. Then the following hold:

1. *The fundamental domain for Λ has area* $\begin{cases} \sqrt{\Delta} & \text{if } D > 0 \\ \frac{1}{2}\sqrt{|\Delta|} & \text{if } D < 0 \end{cases}$.
2. *If $I \neq 0$ and $\Lambda_I = \varphi(I)$, the fundamental domain for Λ_I has area equal to $N(I)$ times the fundamental domain for Λ.*
3. *Every nonzero ideal I of R contains a nonzero element α with* $|N(\alpha)| \leq \mu \cdot N(I)$, *where* $\mu = \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}$.
4. *Every ideal class has an ideal with norm* $\leq \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}$.

Minkowski's Bound, VI

1. The fundamental domain for Λ has area $\begin{cases} \sqrt{\Delta} & \text{if } D > 0 \\ \frac{1}{2}\sqrt{|\Delta|} & \text{if } D < 0 \end{cases}$.

Proof:

- The area of the fundamental domain equals the determinant of $\varphi(1)$, $\varphi(\omega)$, where ω is a generator for $\mathcal{O}_{\sqrt{D}}$.
- If $D < 0$, we have $\varphi(1) = (1, 0)$ and $\varphi(\omega) = (\mathrm{Re}(\omega), \mathrm{Im}(\omega))$ is either $(0, \sqrt{|D|})$ or $(1/2, \sqrt{|D|}/2)$ according to whether $D \equiv 2, 3$ or $D \equiv 1 \pmod 4$. The determinant is $\sqrt{|D|}$ or $\sqrt{|D|}/2$ respectively, and this equals $\sqrt{|\Delta|}/2$.
- If $D > 0$, we have $\varphi(1) = (1, 1)$ and $\varphi(\omega) = (\omega, \overline{\omega})$ is either $(\sqrt{D}, -\sqrt{D})$ or $(\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2})$. Then the determinant is $2\sqrt{D}$ or $\sqrt{D}$ respectively, and this equals $\sqrt{\Delta}$.

Minkowski's Bound, VII

2. If $I \neq 0$ and $\Lambda_I = \varphi(I)$, the fundamental domain for Λ_I has area equal to $N(I)$ times the fundamental domain for Λ.

Proof:

- Let $\Lambda_I = \varphi(I)$ be the image of I, which is a lattice inside $\mathbb{R}^2$ that is a sublattice of $\Lambda = \varphi(\mathcal{O}_{\sqrt{D}})$.
- Since φ is an isomorphism of additive abelian groups that maps $\mathcal{O}_{\sqrt{D}}$ to Λ and I to Λ_I, we see that $\Lambda/\Lambda_I \cong \mathcal{O}_{\sqrt{D}}/I$.
- Taking cardinalities yields $\#(\Lambda/\Lambda_I) = \#(\mathcal{O}_{\sqrt{D}}/I) = N(I)$.
- Geometrically, this means that the fundamental domain for Λ_I consists of $N(I)$ copies of the fundamental domain for Λ. Thus, the fundamental domain for Λ_I has area $N(I)$ times the area of the fundamental domain for Λ, as claimed.

Minkowski's Bound, VIII

3. Every nonzero ideal I of R contains a nonzero element α with $|N(\alpha)| \leq \mu \cdot N(I)$, where $\mu = \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}$.

Proof:

- Let $\Lambda_I = \varphi(I)$. By (1) and (2), the fundamental domain of Λ_I has area $\begin{cases} N(I) \cdot \sqrt{\Delta} & \text{if } D > 0 \\ N(I) \cdot \frac{1}{2}\sqrt{|\Delta|} & \text{if } D < 0 \end{cases}$.
- Now we break into the two cases $D > 0$ and $D < 0$ and apply Minkowski's theorem to an appropriate convex body.

Minkowski's Bound, IX

3. Every nonzero ideal I of R contains a nonzero element α with $|N(\alpha)| \leq \mu \cdot N(I)$, where $\mu = \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}$.

<u>Proof</u> ($D > 0$ case):

- Suppose $D > 0$ and let B be the convex, centrally-symmetric closed set in $\mathbb{R}^2$ defined by $|x_1| + |x_2| \leq N(I)^{1/2}\Delta^{1/4}\sqrt{2}$, which is a square of area $4N(I)\sqrt{\Delta}$.
- By Minkowski's theorem, since the area of B equals 2^2 times the area of the fundamental domain of Λ_I, there necessarily exists some nonzero element $\varphi(\alpha) = (\alpha, \overline{\alpha})$ of Λ_I in B.
- Then $|N(\alpha)| = |\alpha|\,|\overline{\alpha}| \leq \left[\dfrac{|\alpha| + |\overline{\alpha}|}{2}\right]^2 \leq N(I) \cdot \dfrac{1}{2}\sqrt{\Delta}$ where we used the arithmetic-geometric mean inequality. Victory.

Minkowski's Bound, X

3. Every nonzero ideal I of R contains a nonzero element α with $|N(\alpha)| \le \mu \cdot N(I)$, where $\mu = \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}$.

Proof ($D < 0$ case):

- Suppose $D < 0$ and let B be the convex, centrally-symmetric closed set in $\mathbb{R}^2$ defined by $x_1^2 + x_2^2 \le \dfrac{2}{\pi} N(I)\sqrt{|\Delta|}$, which is simply a circle of area $2N(I)\sqrt{|\Delta|}$.
- By Minkowski's theorem, since the area of B equals 2^2 times the area of the fundamental domain of Λ_I, there exists some nonzero element $\varphi(\alpha) = (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$ of Λ_I in B.
- Then $N(\alpha) = \mathrm{Re}(\alpha)^2 + \mathrm{Im}(\alpha)^2$ is the sum of the squares of the coordinates of $\varphi(\alpha)$, which by the hypotheses on B is at most $\dfrac{2}{\pi}\sqrt{|\Delta|} \cdot N(I)$, as claimed.

Minkowski's Bound, XI

4. Every ideal class of R contains an ideal J with
$$N(J) \leq \begin{cases} \frac{1}{2}\sqrt{\Delta} & \text{if } D > 0 \\ \frac{2}{\pi}\sqrt{\Delta} & \text{if } D < 0 \end{cases}.$$

Proof:

- This follows the same way as last week:
- Let $\mathcal{C}$ be an ideal class and let I be any ideal in $\mathcal{C}^{-1}$.
- By (3), there exists a nonzero element $\alpha \in I$ such that $N(\alpha) \leq \mu N(I)$. Because $\alpha \in I$, by the equivalence of divisibility and containment we see that I divides (α) and so $(\alpha) = IJ$ for some ideal J.
- Taking norms yields $N(\alpha) = N(I)N(J)$, so $N(J) = \dfrac{N(\alpha)}{N(I)} \leq \mu$. Finally, taking ideal classes gives $[1] = [(\alpha)] = [I][J]$ so $J \in [I]^{-1} = (\mathcal{C}^{-1})^{-1} = C$, as required.

Minkowski's Bound, XII

Minkowski's bound is quite a lot better than the estimate we obtained earlier.

- The reason is that the constant μ is basically $\sqrt{\Delta} \sim D^{1/2}$, rather than the constant $|D| + 1 \sim D$.
- So, for large D, we have far fewer ideals to examine in order to compute the class group.

We will also remark that, much like everything else we have done, Minkowski's bound on ideal classes holds for general rings of integers of number fields (the proof is similar but more involved, since one must work in $\mathbb{R}^n$).

Computing Class Groups, VI

Example: Determine the class group of $\mathbb{Z}[\sqrt{5}]$.

Computing Class Groups, VI

Example: Determine the class group of $\mathbb{Z}[\sqrt{5}]$.

- Since $5 \equiv 1 \pmod 4$, we have $\Delta = 5$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{1}{2}\sqrt{5} \approx 1.1180 < 2$, so the only nontrivial ideals we need to consider are ideals of norm 2.
- Thus, the class group of $\mathbb{Z}[\sqrt{5}]$ is trivial.

Computing Class Groups, VII

Example (again): Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

Computing Class Groups, VII

<u>Example</u> (again): Show that the class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.

- Since $-5 \equiv 3 \pmod 4$, we have $\Delta = -20$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\dfrac{2}{\pi}\sqrt{20} \approx 2.8471 < 3$, so the only nontrivial ideals we need to consider are ideals of norm 2.
- Since (2) splits as $(2) = (2, 1+\sqrt{-5})^2$, and we have previously shown that $(2, 1+\sqrt{-5})$ is nonprincipal, we conclude that the class group is generated by the nonprincipal ideal $I_2 = (2, 1+\sqrt{-5})$. Since I_2 has order 2 as $I_2^2 = (2)$, the class group has order 2 as claimed.

Computing Class Groups, VIII

Example: Show that the class group of $\mathcal{O}_{\sqrt{-19}}$ is trivial and deduce that it is a principal ideal domain.

Computing Class Groups, VIII

Example: Show that the class group of $\mathcal{O}_{\sqrt{-19}}$ is trivial and deduce that it is a principal ideal domain.

- Since $-19 \equiv 1 \pmod 4$, we have $\Delta = -19$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{19} \approx 2.7750 < 3$, so the only nontrivial ideals we need to consider are ideals of norm 2.
- The minimal polynomial of the generator is $x^2 - x + 5$, which is irreducible modulo 2. Therefore, (2) is inert, and so there are no ideals of norm 2 in $\mathcal{O}_{\sqrt{-19}}$.
- Therefore, the only ideal class is the trivial class, so the class group is trivial and $\mathcal{O}_{\sqrt{-19}}$ is a PID.
- Remark: It can be shown that $\mathcal{O}_{\sqrt{-19}}$ is not Euclidean with respect to any norm (though this is not quite so easy), so it provides an example of a PID that is not a Euclidean domain.

Computing Class Groups, IX

Example: Determine the class group of $\mathbb{Z}[\sqrt{6}]$.

Computing Class Groups, IX

Example: Determine the class group of $\mathbb{Z}[\sqrt{6}]$.

- Since $6 \equiv 2 \pmod 4$, we have $\Delta = 24$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{1}{2}\sqrt{24} \approx 2.4495 < 3$, so there can be no nontrivial ideal classes.
- The minimal polynomial of the generator is $x^2 - 6$, which has a repeated root $r = 0$ modulo 2, so (2) is ramified: $(2) = (2, \sqrt{6})^2$. This ideal $I_2 = (2, \sqrt{6})$ is in fact principal as we saw earlier (it is generated by $2 + \sqrt{6}$).
- Therefore, the only ideal class is the trivial class, so the class group is trivial.

Computing Class Groups, X

Example: Determine the class group of $\mathbb{Z}[\sqrt{10}]$.

Computing Class Groups, X

Example: Determine the class group of $\mathbb{Z}[\sqrt{10}]$.

- Since $10 \equiv 2 \pmod 4$, we have $\Delta = 40$, and so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{1}{2}\sqrt{40} \approx 3.1623 < 4$, so the only nontrivial ideals we need to consider are ideals of norm 2 and norm 3.
- For 2, since $x^2 - 10$ has a repeated root $r = 0$ modulo 2, we see (2) is ramified: $(2) = (2, \sqrt{10})^2$.
- This ideal $I_2 = (2, \sqrt{10})$ is not principal, since any generator would necessarily have norm ± 2, but there are no elements of norm ± 2 since $x^2 - 10y^2 = \pm 2$ has no solutions modulo 5.
- Thus, $[I_2]$ is an element of order 2 in the class group since I_2 is not principal but I_2^2 is.

Computing Class Groups, XI

Example: Determine the class group of $\mathbb{Z}[\sqrt{10}]$.

- For 3, since $x^2 - 10$ has roots ± 1 modulo 3, we see (3) splits: $(3) = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10})$.
- The ideals $I_3 = (3, 1 + \sqrt{10})$ and $I_3' = (3, 1 - \sqrt{10})$ are both nonprincipal, since any generator would necessarily have norm ± 3, but there are no elements of norm ± 3.
- We can then compute $I_3^2 = (9, 3 + 3\sqrt{10}, 11 + 2\sqrt{10})$.
- To test for principality we can look for elements of norm 9, and looking at such elements (e.g., $1 \pm \sqrt{10}$) will reveal this ideal is in fact principal and generated by $(1 + \sqrt{10})$.
- Explicitly, $1 + \sqrt{10} = 9 + (3 + 3\sqrt{10}) - (11 + 2\sqrt{10}) \in I_3^2$ and each generator is divisible by $1 + \sqrt{10}$.
- Then $(I_3')^2 = (1 - \sqrt{10})$, so $[I_3]$ and $[I_3']$ are both ideal classes of order 2 and they are equal.

Computing Class Groups, XII

Example: Determine the class group of $\mathbb{Z}[\sqrt{10}]$.

- It remains to determine the relationship between I_2 and I_3.
- We have $I_2 I_3 = (6, 2 + 2\sqrt{10}, 3\sqrt{10}, 10 + \sqrt{10})$.
- To test for principality we can look for elements of norm 6, and looking at such elements (e.g., $4 \pm \sqrt{10}$) will reveal this ideal is in fact principal and generated by $(4 + \sqrt{10})$, since $4 + \sqrt{10} = (10 + \sqrt{10}) - 6$ and each generator is divisible by $4 + \sqrt{10}$.
- Since $[I_2][I_3] = (1) = [I_2]^2$, we see $[I_2] = [I_3]$.
- Thus, we conclude that there is one nonprincipal ideal class of order 2, so the class group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Summary

We computed some examples of class groups of quadratic integer rings.

We proved Minkowski's bound and use it to compute more examples of class groups of quadratic integer rings.

Next lecture: Binary quadratic forms.