Math 4527 (Number Theory 2)

Lecture #36 of 37 $\sim$ April 15, 2021

Binary Quadratic Forms, Part 2

- Reduced Forms For $\Delta < 0$
- Composition of Quadratic Forms
- The Class Group (Again)

This material represents §9.2.4 from the course notes.

Another Class Group Example, I

Example: Determine the class group of $\mathcal{O}_{\sqrt{-31}}$.

Another Class Group Example, I

Example: Determine the class group of $\mathcal{O}_{\sqrt{-31}}$.

- Since $-31 \equiv 1 \pmod 4$, we have $\Delta = -31$, so Minkowski's bound says that every ideal class of R contains an ideal of norm at most $\frac{2}{\pi}\sqrt{31} \approx 3.5445 < 4$, so the only nontrivial ideals we need to consider are ideals of norm 2 and 3.
- The minimal polynomial of $\omega = \frac{1+\sqrt{-31}}{2}$ is $x^2 - x + 8$.
- For (3) we see the polynomial $x^2 - x + 8$ is irreducible modulo 3, so (3) is inert of norm 9 and it does not yield a nontrivial element of the class group.
- So the only nontrivial elements are those arising from the factorization of (2).
- For (2) we see the polynomial has roots 0 and 1 so we get $(2) = (2, \frac{1+\sqrt{-31}}{2})(2, \frac{1-\sqrt{-31}}{2})$.

Another Class Group Example, II

Example: Determine the class group of $\mathcal{O}_{\sqrt{-31}}$.

- If $I_2 = (2, \frac{1+\sqrt{-31}}{2})$ or its conjugate $I_2' = (2, \frac{1-\sqrt{-31}}{2})$ were principal then it would be generated by an element of norm 2, but there are no elements of norm 2 in $\mathcal{O}_{\sqrt{-31}}$.
- The ideal I_2^2 cannot be principal either, since it would have to be generated by an element of norm 4, but the only such elements are ± 2 and we already have the ideal factorization $(2) = I_2 I_2'$ and $I_2 \neq I_2'$ since 2 is not ramified.
- However, I_2^3 has norm 8, and there are elements of norm 8: $\frac{1\pm\sqrt{-31}}{2}$. As $I_2^3 = (8, 2+2\sqrt{-31}, -15+\sqrt{-31}, \frac{-23-7\sqrt{-31}}{2})$, this ideal contains $8 + 2(2+2\sqrt{-31}) + \frac{-23-7\sqrt{-31}}{2} = \frac{1+\sqrt{-31}}{2}$. Thus $I_2^3 = (\frac{1+\sqrt{-31}}{2})$ is principal, and so $[I_2]$ is an element of order 3 in the class group with inverse $[I_2'] = [I_2]^2$.
- So the class group is generated by $[I_2]$ and has order 3.

Recall, I

Last time we discussed some properties of binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$ with discriminant $\Delta = b^2 - 4ac$.

- If there exist relatively prime x, y with $f(x, y) = n$, we say f properly represents n.
- We showed that there exists some binary quadratic form of discriminant Δ properly representing n if and only if D is a quadratic residue modulo $4n$.
- For odd primes p, we can sharpen this to say that there exists some binary quadratic form of discriminant Δ representing p if and only if D is a quadratic residue modulo p (and by quadratic reciprocity, this is simply a congruence condition on p modulo $4D$).

Recall, II

We also defined an equivalence of binary quadratic forms:

Definition

We define the relation $\sim$ on binary quadratic forms by writing $f \sim g$ if there exists a matrix $A \in SL_2(\mathbb{Z})$ such that $g(\mathbf{x}) = f(A\mathbf{x})$, which is to say that g is obtained from f by an invertible linear change of variables with integer coefficients. Equivalently, $f \sim g$ if there exists $A \in SL_2(\mathbb{Z})$ such that $M_g = A^T M_f A$.

$\sim$ is an equivalence relation preserving (proper) representations.

Definition

If $f(x, y) = ax^2 + bxy + cy^2$ is a binary quadratic form whose discriminant Δ is not a square, we say f is reduced when $-|a| < b \leq |a| \leq |c|$, and if $b = |a|$ we also insist that $|a| < |c|$, while if $|a| = |c|$ then we also insist that $b \geq 0$.

Recall, III

Using reduced forms we showed that there were finitely many equivalence classes and gave a method for calculating them all:

Theorem (Reduced Forms)

Let Δ be a nonsquare integer congruent to 0 or 1 modulo 4 and suppose $f(x,y) = ax^2 + bxy + cy^2$ is a reduced form of discriminant Δ. Then the following hold:

1. *If $D < 0$ then a, c must have the same sign and $|a| \leq \sqrt{-\Delta/3}$. If $\Delta > 0$ then a, c have opposite signs and $|a| < \sqrt{\Delta}/2$. In either case, there are finitely many reduced forms of discriminant Δ.*
2. *Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.*
3. *There are finitely many equivalence classes of binary quadratic forms of discriminant Δ.*

Endless Forms Most Beautiful, I

Example: Find all reduced forms of discriminant $\Delta = -40$ and determine the number of equivalence classes.

Endless Forms Most Beautiful, I

Example: Find all reduced forms of discriminant $\Delta = -40$ and determine the number of equivalence classes.

- From the analysis in (2) we see that any reduced form $ax^2 + bxy + cy^2$ of discriminant $\Delta = -40$ must have $|a| \leq \sqrt{40/3} < 4$, so since $a \neq 0$ this means $a = \pm 1, \pm 2, \pm 3$. Then since $b \in (-|a|, a]$ and $b^2 - 4ac = -40$ so that b is even, we must have $b = 0, \pm 2$.
- If $a = 1$ then $b = 0$ and then $c = (b^2 + 40)/(4a) = 10$, and if $a = -1$ then $b = 0$ and $c = -10$.
- If $a = \pm 2$ then $b = 0, 2$ so that $c = (b^2 + 40)/(4a) = \pm 5$ or $\pm 44/8$, but the second case yields non-integral c.
- If $a = \pm 3$ then $b = 0, \pm 2$ so that $c = (b^2 + 40)/(4a) = \pm 40/12$ or $\pm 44/12$ but these are not integral either.

Endless Forms Most Beautiful, II

Example: Find all reduced forms of discriminant $\Delta = -40$ and determine the number of equivalence classes.

- So in summary, we obtain two positive-definite forms $x^2 + 10y^2$ and $2x^2 + 5y^2$ along with their negatives (which are negative-definite) $-x^2 - 10y^2$ and $-2x^2 - 5y^2$.
- The positive-definite and negative-definite forms are not equivalent to one another, and so we only have to consider equivalence of the two positive-definite forms. But they are not equivalent because they do not represent the same numbers: for example, $2x^2 + 5y^2$ represents both 2 and 5, while $x^2 + 10y^2$ does not.
- Therefore, all these reduced forms are inequivalent, and so there are four inequivalent forms in total.

Endless Forms Most Beautiful, III

Example: Find all reduced forms of discriminant $\Delta = -31$ and determine the number of equivalence classes.

Endless Forms Most Beautiful, III

Example: Find all reduced forms of discriminant $\Delta = -31$ and determine the number of equivalence classes.

- From the analysis in (2) we see that any reduced form $ax^2 + bxy + cy^2$ of discriminant $\Delta = -31$ must have $|a| \leq \sqrt{31/3} < 4$, so since $a \neq 0$ this means $a = \pm 1, \pm 2, \pm 3$. Then since $b \in (-|a|, a]$ and $b^2 - 4ac = -31$ so that b is odd, we must have $b = \pm 1, \pm 3$.
- If $a = 1$ then $b = 1$ and then $c = (b^2 + 31)/(4a) = 8$, and if $a = -1$ then $b = 1$ and $c = -8$.
- If $a = 2$ then $b = \pm 1$ and then $c = (b^2 + 31)/(4a) = 4$, and if $a = -2$ then $b = \pm 1$ and $c = -4$.
- Finally, if $a = \pm 3$ then $b = \pm 1$ or 3 and then $c = (b^2 + 31)/(4a)$ is either $32/\pm 6$ or $40/\pm 6$, but none of these are integers.

Endless Forms Most Beautiful, IV

Example: Find all reduced forms of discriminant $\Delta = -31$ and determine the number of equivalence classes.

- So in summary, we obtain three positive-definite forms $x^2 + xy + 8y^2$, $2x^2 + xy + 4y^2$, $2x^2 - xy + 4y^2$ along with their negatives (which are negative-definite): $-x^2 - xy - 8y^2$, $-2x^2 - xy - 4y^2$, and $-2x^2 + xy - 4y^2$. As before, we only need to consider equivalence of the positive-definite forms.
- It is not hard to see that $x^2 + xy + 8y^2$ is not equivalent to either of the others, since it does not represent 2 whereas the other two do. The other two forms $2x^2 + xy + 4y^2$, $2x^2 - xy + 4y^2$ are also inequivalent, although this is harder.
- In particular, we cannot use the approach from the last example: these two forms represent the same integers because they are obtained via a change of variables $(x, y) \mapsto (x, -y)$ of determinant -1.

Endless Forms Most Beautiful, IV

Example: Find all reduced forms of discriminant $\Delta = -31$ and determine the number of equivalence classes.

- We can show the inequivalence using associated matrices: so suppose we had $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ such that
  $$A^T \begin{bmatrix} 2 & 1/2 \\ 1/2 & 4 \end{bmatrix} A = \begin{bmatrix} 2 & -1/2 \\ -1/2 & 4 \end{bmatrix}.$$
- Since A has determinant 1, we have $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ and so we equivalently must solve
  $$A^T \begin{bmatrix} 2 & 1/2 \\ 1/2 & 4 \end{bmatrix} = \begin{bmatrix} 2 & -1/2 \\ -1/2 & 4 \end{bmatrix} A^{-1}, \text{ which means}$$
  $$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 2 & 1/2 \\ 1/2 & 4 \end{bmatrix} = \begin{bmatrix} 2 & -1/2 \\ -1/2 & 4 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Endless Forms Most Beautiful, V

Example: Find all reduced forms of discriminant $\Delta = -31$ and determine the number of equivalence classes.

- This yields an explicit linear system that reduces to $2a - 2d = a + 2b + 4c = 2b + 4c + d = -4a + 4d = 0$, so that $a = d = -2b - 4c$.
- But then $ad - bc = (2b + 4c)^2 - bc = 4b^2 + 15bc + 16c^2$ cannot equal 1, as can be seen by completing the square: $(2b + 15c/4)^2 + (31/16)c^2 = 1$ implies $(8b + 15c)^2 + 31c^2 = 16$ and this has no integer solutions (it requires $c = 0$ and $8b + 15c = 4$).
- Therefore, all three of these reduced forms are inequivalent, and so there are six inequivalent forms in total.

Endless Forms Most Beautiful, VI

Last time, I identified some reduced forms that were equivalent when $\Delta > 0$. But all of our examples of reduced forms with $\Delta < 0$ were inequivalent. This is true in general:

Proposition (Inequivalence of Reduced Forms for $\Delta < 0$)

Suppose $\Delta < 0$ is the discriminant of a quadratic integer ring.

1. *If $f(x, y) = ax^2 + bxy + cy^2$ is a reduced positive-definite form of discriminant Δ, then a, c, and $a - |b| + c$ are the smallest nonzero integers properly represented by f.*
2. *If f and g are reduced positive-definite forms of discriminant Δ and $f \sim g$, then in fact $f = g$.*
3. *Every equivalence class of binary quadratic forms of discriminant Δ is represented by a unique reduced form.*

Endless Forms Most Beautiful, VII

1. If $f(x, y) = ax^2 + bxy + cy^2$ is a reduced positive-definite form of discriminant Δ, then a, c, and $a - |b| + c$ are the smallest nonzero integers properly represented by f.

Proof:

- Since definiteness is preserved by equivalence, without loss of generality we may work only with the positive-definite forms.
- Now suppose $f(x, y) = ax^2 + bxy + cy^2$ is positive-definite and reduced, so that $|b| \leq a \leq c$.
- If $x^2 \geq y^2$ then $f(x, y) \geq ax^2 - |b|\, xy + cy^2 \geq (a - |b| + c)y^2$.
- Similarly if $y^2 \geq x^2$ then $f(x, y) \geq (a - |b| + c)x^2$.
- So we see $f(x, y) \geq (a - |b| + c) \min(x^2, y^2)$.

Endless Forms Most Beautiful, VIII

1. If $f(x,y) = ax^2 + bxy + cy^2$ is a reduced positive-definite form of discriminant Δ, then a, c, and $a - |b| + c$ are the smallest nonzero integers properly represented by f.

Proof (continued):

- We have $f(x,y) \geq (a - |b| + c)\min(x^2, y^2)$.
- Since $f(x,0) = ax^2$ and $f(0,y) = cy^2$, the only integers with $xy = 0$ properly represented by f are $f(\pm 1, 0) = a$ and $f(0, \pm 1) = c$. Otherwise, $f(x,y) \geq a - |b| + c$, and since $f(1,1) = f(-1,-1) = a + b + c$ and $f(1,-1) = f(-1,1) = a - b + c$, the value $a - |b| + c$ is also properly represented by f.
- Any other value represented by f necessarily has $\min(x^2, y^2) \geq 4$ and is larger than these three values.
- Therefore, the smallest nonzero integers properly represented by f are a, c, and $a - |b| + c$.

Endless Forms Most Beautiful, IX

2. If f and g are reduced positive-definite forms of discriminant Δ and $f \sim g$, then in fact $f = g$.

Proof:

- Let $f(x, y) = ax^2 + bxy + cy^2$, $g(x, y) = a'x^2 + b'xy + c'y^2$ be reduced positive-definite forms of discriminant Δ.
- Then $a \leq c \leq a - |b| + c$ and also $a' \leq c' \leq a' - |b'| + c'$.
- Since $f \sim g$, as we have shown, the integers properly represented by g are the same as those properly represented by f. Therefore, by (1), we must have $a = a'$, $c = c'$, and $|b| = |b'|$, so $b = \pm b'$.
- We claim in fact that b must equal b'.

Endless Forms Most Beautiful, X

2. If f and g are reduced positive-definite forms of discriminant Δ and $f \sim g$, then in fact $f = g$.

Proof (continued):

- We claim in fact that b must equal b'.
- In the case where $a = c$ or where $|b| = a$, since both forms are reduced we must also have b and $b' \geq 0$, so $b = b'$.
- Otherwise, assume $|b| < a < c$ and that $g(x, y) = f(px + qy, rx + sy)$ where $ps - qr = 1$.
- Then $a = g(1, 0) = f(p, q)$ and $c = g(0, 1) = f(r, s)$ are proper representations of a and c respectively, and it is easy to see that f properly represents a only at $(x, y) = (\pm 1, 0)$ and f properly represents c only at $(x, y) = (0, \pm 1)$.
- This forces $(p, q) = (\pm 1, 0)$ and $(r, s) = (0, \pm 1)$, and then the determinant condition requires $(p, q, r, s) = (1, 0, 0, 1)$ or $(-1, 0, 0, -1)$, and in both cases this yields $g(x, y) = f(x, y)$.

Endless Forms Most Beautiful, XI

3. Every equivalence class of binary quadratic forms of discriminant Δ is represented by a unique reduced form.

Proof:

- For positive-definite forms this follows immediately from (2), since as we showed earlier, every equivalence class contains at least one reduced form.
- For negative-definite forms we can simply scale everything by -1 and note that equivalence preserves the definiteness type of a form and that $f \sim g$ implies $-f \sim -g$.

Composition of Forms, I

We now investigate the composition of binary quadratic forms, which we will motivate first via some examples.

- As we have already seen during our discussion of solutions to Pell's equation, the product $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + Dbd) + (ad + bc)\sqrt{D}$ is also an element of $\mathbb{Z}[\sqrt{D}]$.
- Taking norms on both sides yields $(a^2 + Db^2)(c^2 + Dd^2) = (ac + Dbd)^2 + D(ad + bc)^2$, which shows that the product of two integers represented by the quadratic form $x^2 + Dy^2$ is also represented by this form.
- More generally, if $D \equiv 1 \pmod 4$, because the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ is a ring, the product of two elements $a + b\omega$ and $c + d\omega$ is again an element of this ring, and so the product of two elements represented by the norm form $x^2 + xy + \frac{1-D}{4}y^2$ is also represented by that form.

Composition of Forms, II

For some Δ, we have found several inequivalent forms, only one of which necessarily corresponds to the norm form.

- For example, for $\Delta = -40$, we identified two inequivalent positive-definite forms $x^2 + 10y^2$ (which is the norm form for $D = -10$) and $2x^2 + 5y^2$ (which is not the norm form).
- $x^2 + 10y^2$ values: 0, 1, 4, 9, 10, 11, 14, 16, 19, 25, 26, 35, ...
- $2x^2 + 5y^2$ values: 0, 2, 5, 7, 8, 13, 18, 20, 22, 23, 28, 32, ...
- Aside from 0, these lists are disjoint. The first list is closed under multiplication (as we showed above), but the second visibly is not: indeed, 2, 5, and 7 are all on the second list, but their pairwise products 10, 14, and 35 actually all appear on the first list.

Composition of Forms, III

In fact, the product of any two values represented by $2x^2 + 5y^2$ is represented by $x^2 + 10y^2$: if we multiply out $(2a^2 + 5b^2)(2c^2 + 5d^2) = 4a^2c^2 + 10(a^2d^2 + b^2c^2) + 25b^2d^2$, the result is $x^2 + 10y^2$ for $x = 2ac + 5bd$ and $y = bc - ad$.

- Also, if we multiply an element on the first list by an element on the second list, we seem always to obtain something on the second list: for example, $10 \cdot 2 = 20$, $14 \cdot 2 = 28$, $4 \cdot 5 = 20$, and so forth. This holds in general too: if we multiply out $(2a^2 + 5b^2)(c^2 + 10d^2) = 2a^2c^2 + 5b^2c^2 + 20a^2d^2 + 50b^2d^2$, the result is $2x^2 + 5y^2$ for $x = ac + 5bd$ and $y = bc - 2ad$.
- All of this together shows that the equivalence classes of positive-definite quadratic forms of discriminant $\Delta = -40$ have a group structure isomorphic to $\mathbb{Z}/2\mathbb{Z}$ under multiplication, with the form $x^2 + 10y^2$ as the identity and the form $2x^2 + 5y^2$ as the nontrivial element in the group.

Composition of Forms, IV

All of this together shows that the equivalence classes of positive-definite quadratic forms of discriminant $\Delta = -40$ have a group structure isomorphic to $\mathbb{Z}/2\mathbb{Z}$ under multiplication.

- The form $x^2 + 10y^2$ acts the identity while the form $2x^2 + 5y^2$ acts as the nontrivial element in the group.

We can find similar patterns with the quadratic forms for other discriminants, although in many cases they are harder to identify.

Composition of Forms, V

For example, for discriminant $\Delta = -84$, one may show that there are four positive-definite reduced forms: $x^2 + 21y^2$, $2x^2 + 2xy + 11y^2$, $3x^2 + 7y^2$, and $5x^2 + 4xy + 5y^2$.

Here are the integers less than 100 represented by each form:

	Form	Integers
e	$x^2 + 21y^2$	0, 1, 4, 9, 16, 21, 22, 25, 30, 36, 37, 46, 49, 57, 64, 70, 81, 84, 85, 88, 93
a	$2x^2 + 2xy + 11y^2$	0, 2, 8, 11, 15, 18, 23, 32, 35, 42, 44, 50, 51, 60, 71, 72, 74, 92, 95, 98, 99
b	$3x^2 + 7y^2$	0, 3, 7, 10, 12, 19, 27, 28, 31, 34, 40, 48, 55, 63, 66, 75, 76, 82, 90
c	$5x^2 + 4xy + 5y^2$	0, 5, 6, 14, 17, 20, 24, 33, 38, 41, 45, 54, 56, 62, 68, 69, 77, 80, 89, 96

Composition of Forms, VI

If we hypothesize that the reduced forms up to equivalence form a group under multiplication, we can identify the necessary compositions to make it work out correctly.

- Since $x^2 + 21y^2$ is the norm form on $\mathbb{Z}[\sqrt{-21}]$, its set of represented integers is closed under multiplication, so it should be the identity element.
- If we label the other three classes as a, b, and c, then it is not hard to verify that $a \cdot a = e$ for small entries in the table (e.g., $8 \cdot 11 = 88$, $2 \cdot 23 = 46$, etc.), and also $b \cdot b = e$ (e.g., $3 \cdot 7 = 21$, $7 \cdot 12 = 84$) and $c \cdot c = e$ (e.g., $5 \cdot 6 = 30$, $6 \cdot 14 = 84$).
- This suggests the group structure is isomorphic to the Klein 4-group, and so we should also have $a \cdot b = c$ ($2 \cdot 3 = 6$, $11 \cdot 7 = 77$, etc.), $a \cdot c = b$ ($2 \cdot 5 = 10$, $11 \cdot 6 = 66$), and $b \cdot c = a$ ($3 \cdot 14 = 42$, $10 \cdot 5 = 50$), which all do seem to hold.

Composition of Forms, VII

We would expect that these relations should arise from algebraic identities. This is the case, although it is not so easy to find them.

- In general, we are looking for identities of the form $f(x_1, y_1)g(x_2, y_2) = h(B_1, B_2)$ where $B_1 = c_{1,1}x_1x_2 + c_{1,2}x_1y_2 + c_{2,1}y_1x_2 + c_{2,2}y_1y_2 = \mathbf{x}_1^T C\mathbf{x}_2$ and $B_2 = d_{1,1}x_1x_2 + d_{1,2}x_1y_2 + d_{2,1}y_1x_2 + d_{2,2}y_1y_2 = \mathbf{x}_1^T D\mathbf{x}_2$ are appropriate bilinear forms. By multiplying out and comparing coefficients we can find the entries of the matrices C and D.
- So for example to compose $e \cdot a = a$, we can calculate $(a^2 + 21b^2)(2c^2 + 2cd + 11d^2) = 2x^2 + 2xy + 11y^2$ for $x = ac - bc + ad + 10bd$ and $y = 2bc - ad + bd$.
- Similarly, for $a \cdot b = c$ we have $(2a^2 + 2ab + 11b^2)(3c^2 + 7d^2) = 5x^2 + 4xy + 5y^2$ for $x = ac - ad + 2bc + 4bd$ and $y = -ac - ad + bc - 4bd$.

Composition of Forms, VIII

Part of the difficulty is that in some cases, the integers represented by inequivalent forms are the same, so we cannot use tables to identify the group structure, nor can we necessarily identify the composition structure by searching for algebraic identities.

- For example, consider $\Delta = -31$, which has three inequivalent positive-definite forms $x^2 + xy + 8y^2$, $2x^2 + xy + 4y^2$, and $2x^2 - xy + 4y^2$. Here are values represented by each form:

	Form	Integers
e	$x^2 + xy + 8y^2$	0, 1, 4, 8, 9, 10, 14, 16, 20, 25, 28, 31, 32, 35, 36, 38, 40, 47, 49
a	$2x^2 + xy + 4y^2$	0, 2, 4, 5, 7, 8, 10, 14, 16, 18, 19, 20, 25, 28, 32, 35, 36, 38, 40, 41, 45, 49
b	$2x^2 - xy + 4y^2$	0, 2, 4, 5, 7, 8, 10, 14, 16, 18, 19, 20, 25, 28, 32, 35, 36, 38, 40, 41, 45, 49

Composition of Forms, IX

We can see that the forms $2x^2 + xy + 4y^2$ and $2x^2 - xy + 4y^2$ represent the same integers, since they are related via an improper change of variables $(x, y) \mapsto (x, -y)$ of determinant -1.

- As in the examples above, we can write down algebraic identities that yield a group structure on the equivalence classes of these forms.
- However, because of the presence of the improper change of variables relating two of the forms, we can also generate composition relations that do not yield a group structure.
- For example, we have the identity $(a^2 + ab + 8b^2)(2c^2 + cd + 4d^2) = 2x^2 \pm xy + 4y^2$ for $x = \pm(ac - 4bd)$ and $y = ad + 4bc - 2bc + bd$, so depending on our choice of sign, we could either take $e \cdot a = a$ (which is the identity we want if we are to have a group structure) or $e \cdot a = b$ (which would not give a group structure).

Composition of Forms, X

Many of the properties of binary quadratic forms we have discussed were first treated by Legendre.

- For example, he gave the definition of a reduced form, discussed the equivalence of forms, and described a procedure for computing the composition of two forms.
- However, Legendre's treatment also allowed what we now call improper equivalence of forms (i.e., changes of coordinates with determinant -1), which collapses the equivalence classes further and makes it very difficult to identify the right composition structure.

Composition of Forms, XI

Here is an example of Legendre's results: suppose we have forms $f(x,y) = ax^2 + 2bxy + cy^2$ and $g(x,y) = a'x^2 + 2b'xy + c'y^2$ of even discriminant $\Delta < 0$ with a, a' relatively prime.

- Also suppose $B \equiv \pm b \pmod{a}$ and also $B \equiv \pm b' \pmod{a'}$.
- Then $B^2 - \Delta/4 \equiv b^2 + (ac - b^2) \equiv 0 \pmod{a}$ and similarly $B^2 - \Delta/4 \equiv 0 \pmod{a'}$, so $B^2 - \Delta/4 \equiv 0 \pmod{aa'}$.
- One can then write down an appropriate linear change of variables to show that the product $f(x,y)g(x',y')$ is equal to $aa'X^2 + 2BXY + \frac{B^2 - \Delta/4}{aa'}Y^2$ for X and Y appropriate bilinear forms in x, y and x', y'.
- However, because of the choice of $\pm$ signs in Legendre's composition above, there are multiple different possible results of composing two forms, and (as with the example for $\Delta = -31$) these need not actually yield forms lying in the same equivalence class.

Composition of Forms, XII

The resolution of this quite tricky issue was first accomplished by Gauss.

- It was Gauss who first introduced the notion of proper equivalence (which is our relation $\sim$) and identified a consistent procedure for composing quadratic forms that does give them the structure of a group: this is known as Gauss direct composition.
- However, Gauss's treatment is fairly complicated, owing to the necessity of identifying the correct choice of compositions whenever there is more than one option, although it is quite remarkable how much of the general theory he was able to characterize, given that the notion of an abstract group was still decades away from being developed.

Composition of Forms, XIII

We will describe a simplified composition law, due to Dirichlet.

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ be positive-definite binary quadratic forms of discriminant $\Delta < 0$. Suppose that $\gcd(a, a', (b+b')/2) = 1$. Then the Dirichlet composition of $f(x,y)$ and $g(x,y)$ is the binary quadratic form $h(x,y) = Ax^2 + Bxy + Cy^2$ where $A = aa'$, B is the unique integer in $(-A, A]$ satisfying $B \equiv b \pmod{2a}$, $B \equiv b' \pmod{2a'}$, and $B^2 \equiv \Delta \pmod{4aa'}$, and $C = \dfrac{B^2 - \Delta}{4aa'}$.

The new form has discriminant Δ since $C = \dfrac{B^2 - \Delta}{4aa'} = \dfrac{B^2 - \Delta}{4A}$, and the coefficients A, B, C are integers since the assumptions on B indicate that $B^2 - \Delta$ is divisible by $4aa'$.

Composition of Forms, XVI

The Dirichlet composition does yield composition identities like the ones we described earlier.

- By hypothesis, B is congruent to $b \pmod{2a}$ and to $b' \pmod{2a'}$, so by applying the appropriate power of T we see that $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = a'x^2 + b'xy + c'y^2$ are equivalent to the forms $f'(x,y) = ax^2 + Bxy + a'Cy^2$ and $g'(x,y) = a'x^2 + Bxy + aC'y^2$ respectively.
- Then one has $f'(x_1,y_1)g'(x_2,y_2) = AX^2 + BXY + CY^2$ where $X = x_1x_2 - Cy_1y_2$ and $Y = ax_1x_2 + a'y_1y_2 + By_1x_2$.

Composition of Forms, XIV

Example: Compute the Dirichlet composition of $x^2 + 10y^2$ with itself (note $\Delta = -40$).

- We see $A = 1 \cdot 1 = 1$, $B \equiv 0 \pmod 2$, $B \equiv 0 \pmod 2$, and $B^2 \equiv -40 \pmod 4$, so that $B = 0$, and then $C = (B^2 - \Delta)/(4A) = 10$.
- Thus, the Dirichlet composition of $x^2 + 10y^2$ with itself is again $x^2 + 10y^2$.

Example: Compute the Dirichlet composition of $x^2 + 10y^2$ with $2x^2 + 5y^2$ (note $\Delta = -40$).

- We see $A = 1 \cdot 2 = 2$, $B \equiv 0 \pmod 2$, $B \equiv 0 \pmod 4$, and $B^2 \equiv -40 \pmod 8$, so that $B = 0$, and then $C = (B^2 - \Delta)/(4A) = 5$.
- Thus, the Dirichlet composition of $x^2 + 10y^2$ with $2x^2 + 5y^2$ is $2x^2 + 5y^2$.

Composition of Forms, XV

Example: Compute the Dirichlet composition of $2x^2 + 2xy + 11y^2$ with $3x^2 + 7y^2$ (note $\Delta = -84$).

- We see $A = 2 \cdot 3 = 6$, $B \equiv 2 \pmod 4$, $B \equiv 0 \pmod 6$, and $B^2 \equiv -84 \pmod{24}$, so that $B = 6$, and then $C = (B^2 - \Delta)/(4A) = 5$.
- Thus, the Dirichlet composition of $x^2 + 10y^2$ with $2x^2 + 2xy + 11y^2$ with $3x^2 + 7y^2$ is $6x^2 + 6xy + 5y^2$.
- This form is not reduced, but applying S yields $5y^2 - 5xy + 6y^2$ and then applying T yields the reduced form $5x^2 + 4xy + 5y^2$.

Composition of Forms, XVI

It can be shown that Dirichlet composition is well-defined on equivalence classes of forms (boring details omitted).

- So in situations where the condition for evaluating the Dirichlet composition is not met (i.e., when $\gcd(a, a', (b + b')/2) > 1$) we may instead use equivalent non-reduced forms for computing compositions.

Composition of Forms, XVII

Example: Compute the Dirichlet composition of $2x^2 + 5y^2$ with itself ($\Delta = -40$).

- We cannot use the composition formula directly since $\gcd(a, a', (b + b')/2) = 2$.
- Instead, we compute the composition of $2x^2 + 5y^2$ with the equivalent form $5x^2 + 2y^2$ obtained by applying T.
- We get $A = 2 \cdot 5 = 10$, $B \equiv 0 \pmod 4$, $B \equiv 0 \pmod{10}$, and $B^2 \equiv -40 \pmod{40}$, so that $B = 0$, and then $C = (B^2 - \Delta)/(4A) = 1$.
- Thus, the Dirichlet composition of $2x^2 + 5y^2$ with $2x^2 + 5y^2$ is $10x^2 + y^2$.
- This form is not reduced, but applying S yields the reduced form $x^2 + 10y^2$.

Composition of Forms, XVIII

Dirichlet's composition law makes the collection of equivalence classes of forms of discriminant Δ into an abelian group:

Theorem (Composition of Quadratic Forms)

Suppose Δ is the discriminant of a quadratic integer ring and let $\mathcal{F}$ be the set of equivalence classes of quadratic forms of discriminant Δ. Then $\mathcal{F}$ has the structure of an abelian group under Dirichlet composition. The identity of $\mathcal{F}$ is the norm form on the quadratic integer ring Δ and the inverse of the class containing $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

I will prove the non-tedious parts of this result next time. But I will finish today's lecture by telling you the magical result lurking in the background: that the composition law on quadratic forms gives the exact same group structure as the ideal class group of the associated quadratic integer ring.

Summary

We did more examples of computing class groups and enumerating reduced forms.

We motivated and then defined a composition law for binary quadratic forms.

Next lecture: Composition and the ideal class group, complex multiplication.