Summaries, March 29 and 31

Plane Lattices

Let A be a lattice in $\mathbb{R}^2$ or in $\mathbb{C}$. A pair of elements (α_1, α_2) is a *lattice basis* if every element of A is an integer combination of those two elements.

Given such a lattice basis, let $\Pi(A)$ denote region of the plane that is obtained from the parallelogram with vertices $0, \alpha_1, \alpha_2, \alpha_1+\alpha_2$ by removing the 'far edges' $[\alpha_1, \alpha_1+\alpha_2]$ and $[\alpha_2, \alpha_1+\alpha_2]$. We refer to this region as a *parallelogram* though two of the edges are missing.

The lattice basis (α_1, α_2) will be a basis for the plane as a real vector space. Any real vector β can be written uniquely as a combination $r\alpha_1 + s\alpha_2$ with r, s in $\mathbb{R}$. We take out the integer parts of r and s, writing $r = m + r_0$ and $s = n + s_0$ with m, n in $\mathbb{Z}$ and $0 \leq r_0, s_0 < 1$. Then $\beta = a + \beta_0$, where a is in the lattice A and β_0 is in the parallelogram $\Pi(A)$ described above.

Thus the translates of the parallelogram $\Pi(A)$ by elements of A cover the plane, and because we've eliminated two edges, they cover the plane without overlaps.

We denote the area of $\Pi(A)$ by $\Delta(A)$. Say that α_i is the vector $(\alpha_{i1}, \alpha_{i2})^t$. Then, up to sign, $\Delta(A)$ is equal to the determinant $\pm(\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21})$. It isn't worth taking time to explain the signs.

Inclusions of Lattices

Let $B \subset A$ be two lattices, with lattice bases (β_1, β_2) and $\alpha_1, \alpha_2)$. Then

$$(\beta_1, \beta_2) = (\alpha_1, \alpha_2)Q$$

where A is a 2×2 integer matrix, and

$$\Delta(B) = \pm\Delta(A)\det Q$$

The additive cosets of B in A are the sets of the form $a + B$, with a in A, and, as always, the *index* $[A : B]$ of B in A is the number of distinct cosets. Every coset of B contains just one point in the parallelogram $\Pi(A)$. So the index $[A : B]$ of B in A is equal to the number of points of A in the parallelogram $\Pi(B)$. All of the translates $b + \Pi(B)$ by vectors in B contain the same number of points.

Lemma 1. The index $[A : B]$ is equal to $\Delta(B)/\Delta(A)$.

proof Let (β_1, β_2) be a lattice basis for B, and let $\Pi(nB)$ be the parallelogram whose vertices are $0, n\beta_1, n\beta_2, n(\beta_1+\beta_2)$, with its far edges removed. Its area is $n^2\Delta(B)$. The number of points a of the lattice A that are in $\Pi(nB)$ is $n^2[A : B]$. Moreover, the region $\Pi(nB)$ is approximately covered by the translates of $\Delta(A)$ by the $n^2[A : B]$ points a. The covering isn't perfect along the boundary, but the area of $\Pi(nB)$ is approximately equal to $(n^2[A : B])\Delta(A)$. This is the usual approximation of the integral $\int\int_R d\alpha_1 d\alpha_2$. Thus $\Delta(B) \approx [A : B]\Delta(A)$, and as n tends to infinity, the error tends to zero. □

Corollary 1. Le $A \supset B \supset C$ be ideals of R. Then $[A : C] = [A : B][B : C]$. □

Estimating the Shortest Vector in a Lattice.

Let α_1 be a (nonzero) vector of minimal length in a lattice A. We choose coordinates so that α_1 is horizontal: $\alpha_1 = (a, 0)$ with $a > 0$. Then $|\alpha_1| = a$.

If β is an element of A not on the line spanned by α_1, we may add an integer multiple of α_1 to obtain a vector $\alpha_2 = \beta + n\alpha_1$ of the form (b, c), with $-a < b \leq a$. We choose such a vector α_2 with $c > 0$ minimal. Then there will be no point of A in the parallelogram with vertices $0, \alpha_1, \alpha_2, \alpha_1 + \alpha_2$, and (α_1, α_2) will be a lattice basis of A. The area of the parallelogram $\Pi(A)$ spanned by this lattice is ac. Now because α_1 has minimal length, α_2 cannot be in the circle of radius a about the points $0, \alpha_1$, or $-\alpha_1$. Then c cannot be less than $(\sqrt{3}/2)a = \sqrt{3}/2)|\alpha_1|$. (See 13.10.8.)

The area $\Delta(A)$ of the parallelogram spanned by the lattice basis is $\Delta(A) = ac \geq |\alpha_1|^2\sqrt{3}/2$. Therefore

$$|\alpha_1|^2 \leq \frac{2}{\sqrt{3}}\Delta(A)$$

Corollary 2. Every lattice A contains a nonzero vector α with $|\alpha|^2 \le \frac{2}{\sqrt{3}}\Delta(A)$. $\square$

multiplication by n

If A is a lattice, nA is the lattice consisting of the elements that are multiples of n of elements of A. Its index in A is $[A : nA] = n^2$. (We used this fact above, in the proof of Lemma 1.) Also, if $A \supset B$ are lattices, then $[A : B] = [nA : nB]$, simply because multiplication by n is an automorphism of the vector space $\mathbb{R}^2$.

March 31

Back to the Ring of Integers in $\mathbb{Q}[\delta]$**.**

Recall that every ideal A (not the zero ideal) of the ring of integers R is product of prime ideals: $A = P_1 \cdots P_k$ in a unique way, up to order.

Proposition 1. **(i)** Let P be a prime ideal of R. There is an integer prime p such that, either $P = (p)$ $(= pR)$, or $\overline{P}P = (p)$.

(ii) Let p be an integer prime. There is a prime ideal P of R such that, either $(p) = P$, or $(p) = \overline{P}P$.

proof (i) The Main Lemma tells us that $\overline{P}P$ is a principal ideal $(n) = nR$, generated by a positive integer n. We factor n into prime integers: $n = p_1 \cdots p_k$. The principal ideal (n) is the product of the principal ideals (p_i): $\overline{P}P = (n) = (p_1)\cdots(p_k)$, and each (p_i) can befactored into prime ideals. Since $\overline{P}P$ has just two prime factors, $k \le 2$. If $k = 1$, then $\overline{P}P = (p_1)$. If $k = 2$, then $P = (p_1)$.

(ii) We factor (p) into prime ideals in R: $(p) = P_1 \cdots P_k$. Since $(p) = \overline{(p)}$, we also have $(p) = \overline{P}_1 \cdots \overline{P}_k$, and $(p)^2 = (\overline{P}_1P_1)\cdots(\overline{P}_kP_k)$. The k products on the right are principal ideals, say $\overline{P}_iP_i = (n_i)$. Then $p^2 = n_1 \cdots n_k$, and therefore $k \le 2$. If $k = 1$, then $(p) = P_1$ $(= \overline{P}_1)$. If $k = 2$, then $(p) = \overline{P}_1P_1$. $\square$

Note that, when p is given and $(p) = P$ or $P(p) = \overline{P}P$, the ideal P or the pair of prime ideals $P, \overline{P}$ are uniquely detemined. This follows from the uniqueness of the factorization of (p).

Proposition 2. Let A, B, C be ideals, with $B \supset C$. Then the index $[B : C]$ is equal to the index $[AB : AC]$.

proof Since A is a product of prime ideals, it is enough to prove this when A is a prime ideal. Then we can use induction. So we must show that $[B : C] = [PB : PC]$ when P is a prime ideal. By Proposition 1, there is a prime integer such that $P = (p)$ or $\overline{P}P = (p)$. The ideal $(p)B$ is equal to pB, and $(p)C = pC$. Therefore $[B : pB] = p^2 = [C : pC]$ and $[B : C] = [pB : pC]$.

So if $P = (p)$, then $[PB : PC] = [pB : pC] = [B : C]$.

Suppose that $\overline{P}P = (p)$. We inspect the inclusions $B \supset PB \supset \overline{P}PB = pB$. We can't have $B = PB$, because $B = RB$. If we had $RB \supset PB$, the Cancellation law would show that $R = P$. So $B > PB$. Similarly, $PB > \overline{P}PB = pB$. Since $[B : pB] = p^2$ and since $[B : pB] = [B : PB][PB : pB]$, we must have $[B : PB] = [PB : pB] = p$, and similarly, $[C : PC] = p$.

Now the inclusion $B \supset C \subset PC$ shows that $[B : PC] = [B : C]p$, and the inclusion $B \supset PB \supset PC$ shows that $[B : PC] = p[PB : PC]$. Therefore $[B : C] = [PB : PC]$. $\square$

the Norm

This is just terminology. The *norm* of a complex number is defined to be its square length: $N(\alpha) = \overline{\alpha}\alpha = |\alpha|^2$.

If A is an ideal of R, then $\overline{A}A = (n)$ for sme positive integer n. Tht integer is defined to be the norm of A: $N(A) = n$ if $\overline{A}A = (n)$.

Note that $N(\alpha\beta) = N(\alpha)N(\beta)$ and $N(AB) = N(A)N(B)$.

Proposition 3. Let A be an ideal of R. Then

$$N(A) = [R : A] = \frac{\Delta(A)}{\Delta(R)}$$

proof The second equality has been proved before. We show that $N(A) = [R : A]$:

$$n^2 = [R : nR] = [R : \overline{A}A] = [R : A][A : \overline{A}A][R : A][RA : \overline{A}A] = [R : A][R : \overline{A}] = [R : A]^2.$$

□

Ideal Classes

The ideal classes are equivalence classes of ideals, the relation being that $A \sim A'$ if $A' = cA$, for some complex number c. Writing $c = re^{i\theta}$, the geometric meaning of this is that the lattice A' is obtained from the lattice by stretching A by the factor r and rotating by the angle θ. Thus the ideals are similar geometric figures, the similarity being orientation-preserving. I don't know if there is a term for orientation-preserving similarity, but we'll call such a similarity a *proper similarity*. So two ideals are in the same ideal class if they are properly similar geometric figures. We have seen that when $\delta = \sqrt{-5}$, there are two ideal classes.

If A is an ideal, we denote its class by $\langle A \rangle$.

Lemma 2. The class of the unit ideal R consists of the principal ideals.

proof An ideal A is similar to R if and only if $A = cR$, and then $c = c \cdot 1$ is in A and in R. This means that A is a principal ideal. □

Note that whenever $A' = cA$, the scalar c will be an element of the field $K = \mathbb{Q}[\delta]$, but it needn't be an element of R.

Let $\mathcal{C}$ denote the set of ideal classes.

The *product* of two ideal classes is defined by the rule $\langle A \rangle \langle B \rangle = \langle AB \rangle$, where AB is the product ideal. If $A \sim A'$ and $B \sim B'$, say $A' = cA$ and $B' = dB$, then $A'B'' = cdAB$. So the product is well-defined. It is associative and commutative, and the class $\langle R \rangle$ of the unit ideal is an identity element that we may denote by 1 as usual. Moreover, since $\overline{A}A = (n)$ is a principal ideal, $\langle \overline{A} \rangle \langle A \rangle = \langle (n) \rangle = 1$. So $\langle \overline{A} \rangle$ is an inverse of $\langle A \rangle$.

Corollary 3. With multiplication defined as above, the set $\mathcal{C}$ of ideal classes becomes an abelian group, the *ideal class goup*. □

Proposition 4. The ideal class group is the trivial group if and only if R is a unique factorization domain.

proof The class group of R is trivial if and only if every deal of R is principal. Any principal ideal domain has unique factorization of elements. Conversely, suppose that the ring R of algebraic integers has unique factorization of elements. We show that every ideal A is principal. Since A is a product of prime ideals, it suffices to show that every prime ideal P is principal. Let π be an irreducible element of P. Since R is a UFD, π is a prime element, and it generates a prime ideal. In the ring of algebraic integers, a prime ideal is a maximal ideal. Therfore (π) is a maximal ideal, and since $(\pi) \subset P$, $(\pi) = P$. So P is a principal ideal. □