Summary, March 24 and 26

Ideals in $R = \mathbb{Z}[\delta]$, $\delta = \sqrt{-5}$

A subset A of the ring R is an ideal if

- it is an additive subgroup of R, and
- it is closed under multiplication by δ, i.e., if $ra \in A$ and $r \in R$,then $ra \in A$.

A subgroup is closed under multiplication by integers, so if A is closed under multiplication by δ, then it is closed under multiplication by any element of R.

The zero ideal isn't interesting, so we will be discussing nonzero ideals.

An nonzero ideal A will be a sublattice of the lattice R (see 6.5.6). It is discrete because R is a lattice, and if α is a nonzero element of A, then α and $\alpha\delta$ will be independent real vectors.

Every lattice L in $\mathbb{R}^2$ has a *lattice basis*, a pair a, b of elements such that $L = \mathbb{Z}a + \mathbb{Z}b$. Therefore a nonzero ideal A will have a lattice basis. We must distinguish between a lattice basis and a set of generators for an ideal. A set $\{a_1, ..., a_k\}$ *generates* an ideal A if every element of A can be writtten as a combination $r_1a_1 + \cdots + r_ka_k$, with r_i in R. So a lattice basis is a set of generators for the ideal, but not conversely.

Theorem. The nonzero ideals of $R = \mathbb{Z}[\delta]$, $\delta^2 = -5$, are

- the principal ideals, and
- the ideals with lattice basis of the form α, β, where $\alpha \in R$ and $\beta = \frac{1}{2}(\alpha + \alpha\delta)$.

When α is in R, the element β may be in R or not. If β isn't in R, then the second case isn't a possiblility.

proof The first possibility is that A is a principal ideal. If so, how can we find its generator? If A is a principal ideal, it will be generated by a nonzero element of minimal absolute value — a shortest nonzero vector in A. Because the units of R are ± 1, there will be two such vectors.

Whether or not A is a principal ideal, we can start by choosing a nonzero element α of minimal absolute value. Let's denote the principal ideal $R\alpha$ by I. This ideal will be the plane lattice with lattice basis the orthogonal vectors α and $\alpha\delta$. The lattices R and I are similar geometric figures. If we write $\alpha = re^{i\theta}$, where $r = |\alpha|$, then I is obtained from R by stretching by the factor r and rotating by the angle θ.

Since it contains α, A contains the principal ideal I. What other elements could A contain?

Let $\gamma = \alpha\delta$. Let β be an element of A not in I. The elements α and γ form a real basis of the plane $\mathbb{C}$. So we can write the real vector β as $r\alpha + s\gamma$, with $r, s \in \mathbb{R}$. We take out the integer parts of r, 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 $m\alpha + n\gamma$ is in I, and $\beta_0 = r_0\alpha + s_0\gamma$ is in A. Here β is in I and $m\alpha + n\gamma$ is in A. So β_0 is also in I, but it isn't in A. If A contains an element not in I, then it contains an element β in the rectangle Γ whose vertices are $0, \alpha, \gamma, \alpha + \gamma$, and not on the 'far edges' $[\alpha, alpha + \gamma]$ or $[\gamma, \alpha + \gamma]$.

The rectangle Γ is a similar geometric figure to the rectangle whose vertices are $0, 1, \delta, 1 + \delta$. It is situated in the plane in some way that isn't important.

Where in Γ could an element β in A but not in I be? First, since α is an element of minimal absolute value r in A, β can't be in the interior of the circle of radius r about the origin. Also, β can't be in the interior of the circle of radius r about α, because if it were, then $\alpha - \beta$, which is in A, would have absolute value $< r$. Similarly, it can't be in the circles of radius r about γ and about $\alpha + \gamma$.

Next, if β were in the disk D of radius $\frac{1}{2}r$ about the point $\frac{1}{2}\gamma$, then 2β, which is in A, would be too close to γ. This rules out points in the disk D, except for the point $\frac{1}{2}\gamma$ itself. We don't yet know whether or not that point is in A. In the same way, one rules out the disks of radius $\frac{1}{2}r$ about the points $\frac{1}{2}\alpha + \frac{1}{2}\gamma$ and $\alpha + \frac{1}{2}\gamma$, except for those points themselves. (See the figure on page 389.)

Summing up, if A contains a point β not in the principal ideal I, then β is one of the three points $\frac{1}{2}\gamma$, $\frac{1}{2}(\alpha + \gamma)$ or $\alpha + \frac{1}{2}\gamma$.

If A contains $\alpha + \frac{1}{2}\gamma$, it also contains $\frac{1}{2}\gamma$. And, if it contains $\frac{1}{2}\gamma$, then it also contains $\frac{1}{2}\delta\gamma = \frac{1}{2}\alpha\delta^2 = -\frac{5}{2}\alpha$, and therefore it contains $\frac{1}{2}\alpha$. This isn't possible because α has minimal absolute value. This leaves just one possibility: If A is not the principal ideal $I = (\alpha)$, then it has lattice basis $\alpha, \frac{1}{2}\alpha\delta$. Its points re those in the rectangular lattice I, together with the midpoints of the rectangles.

This is the shape of the ideals $A = (2, 1 + \delta)$ and $B = (3, 2 + \delta)$ that factor (2) and (3) in R.

algebraic integers

We go now to an arbitrary imaginary quadratic number field. Let d be a square-free negative integer. So d can be any one of the integers $-1, -2, -3, -5, -6, ...$ (The case $d > 0$ is harder.)

The elements of the ring $\mathbb{Q}[\delta]$, $\delta = \sqrt(d)$ are $\alpha = a + b\delta$ wihth $a, b \in \mathbb{Q}$.

One of the biggest discoveries of the 19th century wss the concept of an algebraic integer. An element $\alpha = a + b\delta$ of K is an *algebriac integer* if the monic irreducible polynomial in $\mathbb{Q}[x]$ with root α has integer coefficients.

The monic irreducible polynomial with root α is $x - a$ if $b = 0$, and is

$$f(x) = x^2 - (\alpha + \overline{\alpha})x + (\alpha\overline{\alpha}) = x^2 - (2f)ax + (a^2 - b^2 d)$$

Lemma 1. An element $\alpha = a + b\delta$ is an algebraic integer if and only if $\alpha + \overline{\alpha} = 2a$ and $\alpha\overline{\alpha} = a^2 - b^2 d$ are integers. □

Proposition. The algebraic integers in $\mathbb{Q}[\delta]$ are the elements $\alpha = a + b\delta$ such that

- a and b are integers, or
- a and b are half integers and d is congruent 1 modulo 4.

proof When we write $b = p/q$ where p, q are relatively prime integers, $b^2 d = p^2 d/q^2$. Since d is square-free, it can't cancel any square in the denominator q^2. So if $b^2 d$ is an integer, then b must also be an integer.

The condition that $2a$ is an integer implies that a is either an integer or a half integer. If a is an integer, so is a^2. Then $b^2 d$ must be an integer, an therefore b is an integer.

If a is a half integer, say $a = n + \frac{1}{2}$ with $n \in \mathbb{Z}$, then $a^2 = n^2 + n + \frac{1}{4}$, and so a^2 and $b^2 d$ are elements of $\mathbb{Z} + \frac{1}{4}$. Then, writing $b = p/q$ as before, q must be divisible by 2, say $q = 2q_1$. Then $b^2 d = p^2 d/4q_1^2$. Since d can't cancel a square factor of q_1^2, we must have $q_1 = 1$. So both a and b are half integers. In order that $a^2 - b^2 d$ be an integer, we must also have d congruent 1 modulo 4. □

The first example with $d \equiv 1$ modulo 4 is $d = -3$. With ζ_n denoting $e^{2\pi i/n}$, that ring is generated by $\zeta_6 = \frac{1}{2}(1 + \sqrt{-3})$, or by $\zeta_3 = \frac{1}{2}(-1 + \sqrt{-3})$. It is an equilateral triangular lattice in the complex plane.

Corollary. If an algebraic integer α is a rational number, then it is an ordinary integer. □

arch 26

Let $d = -5$. We saw that the ideals $A = (2, 1+\delta)$ and $B = (3, 1+\delta)$ have the property that $\overline{A}A$ and $\overline{B}B$ are the principal ideals (2) and (3), respectively. The Main Lemma below shows that this was not an accident.

Main Lemma. Let R be the ring of algebraic integers in the field $\mathbb{Q}[\sqrt{d}]$, where d is a negative square-free integer, and let A be a nonzero ideal in R. The product ideal $\overline{A}A$ is a principal ideal, generated by an ordinary positive integer.

proof Let (α, β) be a lattice basis for A. The complex conjugate ideal $\overline{A}$ will have the lattice basis $(\overline{\alpha}, \overline{\beta})$. Therefore the set of four products

$$(u = \overline{\alpha}\alpha, w = \overline{\alpha}\beta, \overline{w} = \overline{\beta}\alpha, v = \overline{\beta}\beta)$$

generates the product ideal in R.

The three elements u, v and $w+\overline{w}$ are algebraic integers, and they are rational numbers because they are equal to their complex conjugates. Therefore they are ordinary integers. We claim that their greatest common divisor generates the product ideal $\overline{A}A$.

In the ring of integers $\mathbb{Z}$, the greatest common divisor n is the generator of the ideal $u\mathbb{Z} + v\mathbb{Z} + (+\overline{w})\mathbb{Z}$. Therefore n divides u, v (and $w+\overline{w}$) in the integers. This gives us two of the generators for the product ideal $\overline{A}A$. To show that n generates $\overline{A}A$, We need to show that, in the ring R, n divides the remaining two generators w and $\overline{w}$ of $\overline{A}A$.

We have to show that w/n and $\overline{w}/n$ are in the ring R. Since $R = \overline{R}$, it is enough to show that w/n is in R. How could we possibly do this? There is just one way, and that is to use the definition of R as the ring of algebraic integers in $\mathbb{Q}[\delta]$. We have to show that w/n is an algebraic integer. To show this, Lemma 1 tells us that we must show that $(w + \overline{w})/n$ and $(w/n)(\overline{w}/n)$ are ordinary integers. This is easy: n is the greatest common divisor of u, v and $w + \overline{w}$, so n divides $w + \overline{w}$. Next, $w\overline{w} = (\overline{\alpha}\beta)(\overline{\beta}\alpha) = (\overline{\alpha}\alpha)(\overline{\beta}\beta) = uv$, and n divides u and v. So n^2 divides $w\overline{w}$. □

There are several corollaries to the Main Lemma. Since they all concern nonzero ideals, let's agree that by ideal we mean an ideal that isn't the zero ideal here.

Corollary 1. *(Cancellation Law)* Let A, B, C be ideals. If the product idals AB and AC are equal, $AB = AC$, then $B = C$.

proof Suppose that $AB = AC$. Then $\overline{A}AB = \overline{A}AC$, and since $\overline{A}A$ is a principal ideal (n), $(n)B = (n)C$. Writing $(n) = nR$, $nRB = nRC$. Since B is an ideal, $RB = B$, so $nB = nC$. Dividing by n, $\frac{1}{n}nB = \frac{1}{n}nC$, i.e., $B = C$. □

Corollary 2. If A and B are ideals and if $A \supset B$, then A divides B: There is an ideal C such that $B = AC$.

proof From $A \supset B$, we conclude that $\overline{A}A \supset \overline{A}B$, i.e., $(n) = nR \supset \overline{A}B$. Every element of the product ideal $\overline{A}B$ is divisible by n. Then $R \supset \frac{1}{n}\overline{A}B$. The set $C = \frac{1}{n}\overline{A}B$ is closed under addition and multiplication by elements of R, so it is an ideal of R. Then $AC = \frac{1}{n}A\overline{A}B = \frac{1}{n}nB = B$. □

Corollary 3. The following are equivalent for an ideal P of R:

(1) P is irreducible.

(2) P is a prime ideal.

(3) P is a maximal ideal.

By an irreducible ideal P we mean a proper idal that isn't the product of two proper ideals. Recall that P is a prime ideal if it is a proper ideal, and whenever P containa a product AB of ideals, it contains one of the, factors A or B. And, P is a maximal ideal if it is a proper ideal, $P < R$, and if there is no ideal A such that $P < A < R$.

proof This is very simple.

(3) ⇒ (2): A maximal ideal is a prime ideal in any ring.

(2) ⇒ (1): If $P = AB$, then $P \subset A$ and $P \subset B$. If P is a prime ideal, then $A \subset P$ or $B \subset P$, and therefore P is equal to A or to B, and the factoring $P = AB$ isn't proper.

(1) ⇒ (3): If $P < A$, then by Corollary 1, $P = AC$. The if P is irreducible, one of the ideals A or C is equal to R. If $C = R$, then $A = P$. By hypothesis, this isn't the case. So $A = R$. There is no ideal A such that $P < A < R$, and threfore P is maximal. □

Corollary 4. Every proper ideal of R is a product of prime ideals in a way that is unique, up to ordering of the factors.

proof Let $A = P_1 \cdots P_k$ and $A = Q_1 \cdots Q_\ell$ be two factorings of A into prime ideals. Then P_r divides the product $Q_1 \cdots Q_\ell$, so it divides one of the factors, say Q_ℓ. Then $P_r \supset Q_\ell$, and because a prime ideal is maximal, $P_r = Q_\ell$. By the cancellation law (Corollary 1), $P_1 \cdots P_{r-1} = Q_1 \cdots Q_{ell-1}$. Induction shows tha the two factorings are the same up to order.

The only thing left to do is to show that one can factor an ideal A into prime ideals in at least one way.

Lemma 2. A nonzero ideal A of R has finite index $[R : A]$. If $A \subset B$ are ideals, then $[R : B]$ is a divisor of $[R : A]$, and it is a proper divisor unless $A = B$.

If $A \subset B$ are lattices in the plane, the *index* of A in B is the number of additive cosets $a + B$ of A in B. The lemma will be proved next time.

We go back to our ideal A. If A is irreducible, it is a prime ideal. Otherwise, it is a product $A = BC$ of proper ideals, and $A \subset B$. If $A = B$, then $A = AC$, and since $A = AR, \quad AR = AC$. Cancelling A, $R = C$, contrary to the hypothesis that the factoring is proper. Thus $A < B$. Then the index $[R : B]$ is a proper divisor of the index $[R : A]$.

If B and/or C are not irreducible, we continue by factoring them. Induction on the index $[R : A]$ shows that this factoring process terminates. □