Summaries, April 2 and 5

Let $\delta = \sqrt{d}$ as before. When d isn't congruent 1 modulo 4, we will have $d \equiv 2$ or 3 modulo 4. In those cases, $R = \mathbb{Z}[\delta]$, and $(1, \delta)$ is a lattice basis for R. Therefore the area $\Delta(R)$ of the parallelogram with vertices $0, 1, \delta, 1+\delta$ is $\sqrt{|d|}$. (Because d is negative, its absolute value $|d|$ is $-d$.) When $d \equiv 1$ modulo 4, the elements $(1, \eta)$ with $\eta = \frac{1}{2}(1 + \delta)$ form a lattice basis, and $\Delta(R) = \frac{1}{2}\sqrt{|d|}$.

We introduce a peculiar number

$$\mu = \frac{2}{\sqrt{3}}\Delta(R)$$

If $d \equiv 2$ or 3 modulo 4, then $\mu = 2\sqrt{\frac{|d|}{3}}$. If $d \equiv 1$ modulo 4, then $\mu = \sqrt{\frac{|d|}{3}}$.

Theorem. Every ideal class contains an ideal A with norm $N(A) \le \mu$.

proof Let A be an ideal and let α be a nonzero vector of minimal length in A. We have seen that $N(\alpha) = |\alpha|^2 \le \frac{2}{\sqrt{3}}\Delta(A)$. Since A contains the principal ideal (α), A divides (α): $(\alpha) = AC$ for some ideal C.

Then $N(\alpha) = N(A)N(C)$. Recall that $N(A) = \Delta(A)/\Delta(R)$. So $N(A)N(C) \le \frac{2}{\sqrt{3}}N(A)\Delta(R)$. Cancelling $N(A)$,

$$N(C) \le \frac{2}{\sqrt{3}}\Delta(R) = \mu$$

Since $AC = (\alpha)$, The class of C is the inverse of the class of A. Therefore $\overline{C}$ is in the class of A, and $N(\overline{C}) = N(C) \le \mu$. □

Corollary. The ideal class group $\mathcal{C}$ of R is a finite group.

There are finitely many ideals with norm $\le \mu$. The proof comes out from the computation of the class group that we explain below.

Proposition. The ideal class group is the trivial group if and only if R is a unique factorization domain, i.e., factoring of elements into irreducible elements is unique.

Proof The class group is trivial if and only if every ideal is in the class of R, i.e., every ideal is a principal ideal.

Any principal ideal domain is a unique factorization domain. Conversely, suppose that R has unique factorization of elements, let P be a prime ideal, an let π be an irreducible nonzero element of P. Because R has unique factorization, π is a prime element. Therefore the principal ideal (π) is a prime ideal, and $(\pi) \subset P$. We've seen that prime ideals of these rings are maximal ideals. Therefore $(\pi) = P$. Evey prime ideal is principal, and since every ideal is a product of prime ideals, every ideal is principal. □

Computing the Ideal Class Group.

We look first for generators of the class group $\mathcal{C}$.

Lemma 1. The ideal class group $\mathcal{C}$ is generated by the classes of prime ideals P whose norms are prime integers p with $p \le \mu$.

proof Let P be a prime ideal with $N(P) \le \mu$. We have seen that $N(P)$ is either a prime p or the square of a prime p, and if $N(P) = p^2$, then $P = (p)$. The integer p generates a prime ideal in R, and one says that p *remains prime in* R. If $N(P) = p$, then $\overline{P}P = (p)$. The integer p doesn't generate a prime ideal in R. One says that p *splits in* R.

Now for the proof of the lemma: If A is an ideal with norm $N(A) \le \mu$, and if we factor into prime ideals, $A = P_1 \cdots P_k$, then $N(P_i) \le \mu$ for every i. So $\mathcal{C}$ is generated by the classes of prime ideals P with norm $N(P) \le \mu$.

If P is a principal ideal (p), its ideal class is the identity element of $\mathcal{C}$. We don't need it in our list of generators. We eliminate those prime ideals. The class group is generated by the classes of prime ideals P, such that $\overline{P}P = (p)$, p is a prime integer that splits in R, and $p \le \mu$. □

Lemma 2. Suppose that $d \equiv 2$ or 3 modulo 4, so that $R = \mathbb{Z}[\delta] \approx \mathbb{Z}[x]/(x^2 - d)$. A prime integer p remains prime in R if and only if $x^2 - d$ is an irreducible element of $\mathbb{F}_p[x]$.

We've seen this before. It results from the diagram

XX

$$\begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{F}_p[x] \\ \big\downarrow & & \big\downarrow \\ \mathbb{Z}[\delta] & \longrightarrow & R/(p) \end{array}$$

The vertical arrows are obtained by killing p, and the horizontal arrows by killing $x^2 - d$. This diagram shows that $R/(p)$ is a domain (a field) if and only if $x^2 - d$ is irreducible in $\mathbb{F}_p[x]$. (See p. 395 of the text.)

Example 1. **(i)** Let $d = -2$. Then $\Delta(R) = \sqrt{2}$, and $\mu = 2\sqrt{\frac{2}{3}}$. So $\mu < 2$. There are no prime integers less than μ, so the class group is trivial, and R is a unique factorization domain.

(ii) Let $d = -5$ Then $\Delta(R) = \sqrt{5}$ an $\mu = 2\sqrt{\frac{5}{3}}$. Here $\mu < 3$. There is just one prime integer < 3, namely 2.

Does 2 remain prime in R? Lemma 2 tells us that 2 remains prime if and only if $x^2 + 5$ is irreducible in $\mathbb{F}_2[x]$. It is not irreducible: In $\mathbb{F}_2[x]$, $\;x^2 + 5 = x^2 + 1 = (x + 1)^2$. So 2 splits in R, say $(2) = \overline{P}P$. The class group is generated by P. Of course, we knew this already.

Lemma 4. For any $d \equiv 3$ modulo 4, the prime 2 splits: $\;(2) = \overline{P}P$, where P is the ideal generated by the pair of elements $(2, 1 + \delta)$. Morover, $P = \overline{P}$, so $(2) = P^2$. The class $\langle P\rangle$ has order 2 in the class group.

proof Let P be the ideal generated by the set $(2, 1 + \delta)$. Then $\overline{P}P$ is generated by the set of four elements $(4, 2 + 2\delta, 2 - 2\delta, 1 - d)$. Since $d \equiv 3$ modulo 4, $1 - d \equiv 2$ modulo 4. Therefore, since $\overline{P}P$ contains 4 and $1 - d$, it also contains 2. And, 2 divides all four generators. So $\overline{P}P = 2$. Moreover, $oP = P$ because $1 - \delta = 2 - (1 + \delta)$. Therefore $\langle P\rangle = \langle P\rangle^{-1}$, and $\langle P\rangle^2 = 1$. So $\langle P\rangle$ has has order 1 or 2. Since neither one of the generators 2 and $1 + \delta$ divides the other, $\langle P\rangle$ has order 2 in the class group. $\square$

Example 2. $d = -29$. Then

$$\mu = 2\sqrt{|d|/3} = 2\sqrt{29/3} \approx 6.1$$

The primes less than μ are $2, 3$ and 5. The polynomial $x^{-}d = x^2 + 29$ factors modulo $2, 3$ and 5, so all of these primes split in R. Say that $(2) = \overline{P}P$, $(3) = \overline{Q}Q$, and $(5) = \overline{S}S$. The class group is generated by the classes $\langle P\rangle$, $\langle Q\rangle$, and $\langle S\rangle$. By Lemma 4, $\langle P\rangle$ has order 2 in $\mathcal{C}$, and $P = \overline{P}$. So we have one relation: $\langle P\rangle^2 = 1$. How can we find other relations? The method is to look at norms of some elements of R.

Suppose that some relation, such as $\langle P\rangle\langle Q\rangle\langle S\rangle = 1$ holds. This means that the class $\langle PQS\rangle$ of the product is equal to 1, i.e., that PQS is a principal ideal, say $PQS = (\alpha)$. Taking norms of both sides, $N(\alpha) = N(P)N(Q)N(S)$, and therefore

$$(\overline{\alpha})(\alpha) = \overline{P}P\overline{Q}Q\overline{S}S$$

When we factor the principal ideals $(\overline{\alpha})$ and (α) into prime ideals in R, the prime factors that occur must be on the right of this equation, and the factors of $(\overline{\alpha})$ will be their complex conjugates. Then (α) will be the product of three of the factors on the right, and $\overline{\alpha})$ will be the product of their conjugates. So we will have $(\alpha) = P^{\pm 1}Q^{\pm 1}S^{\pm 1}$.

Since $\langle P\rangle^2 = 1$, $\;\overline{P} = P$. We haven't decided which prime factor of (3) to label as Q and which to label as $\overline{Q}$. Similarly, we haven't decided between S and $\overline{S}$. So if we label appropriately, the exponents in the equation above will all be equal to $+1$, and $(\alpha) = PQS$. Then in the class group,

$$\langle P\rangle\langle Q\rangle\langle S\rangle = 1$$

This is a second relation. However, at this point we have decided the signs. So, going forward, we aren't allowed to adjust signs again.

We compute some more norms of elements:

$N(2 + \alpha) = 33$: $\;$ not useful, though it tells us something about the prime 11.

$N(3 + \alpha) = 38$: not useful.

$N(4 + \alpha) = 45 = 3^2 5$:

This norm tells us that $(45)^2 = (\overline{Q}Q)^2\overline{S}S$. Therefore in the class group, $\langle Q\rangle^2\langle S\rangle^{\pm 1} = 1$, and $\langle S\rangle = \langle Q\rangle^{\pm 2}$. We can eliminate $\langle S\rangle$ from our list of generators, but then we must eliminate it from the relation

$\langle P\rangle\langle Q\rangle\langle S\rangle = 1$. There are two possibilities: If $\langle S\rangle = \langle Q\rangle^2$, the relation becomes $\langle P\rangle\langle Q\rangle^3 = 1$, while if $\langle S\rangle = \langle Q\rangle^{-1}$, it becomes $\langle P\rangle\langle Q\rangle^{-1} = 1$. However, this second possibility can be ruled out: $\langle P\rangle = \langle Q\rangle$ isn't possible because $\langle P\rangle^2 = 1$. We would have $\langle Q\rangle^2 = 1$ too, so $\overline{Q}^2 Q^2 = (3)^2 = (9)$ would be the norm of some element α. It isn't a norm.

So we have the two relations $\langle P\rangle^2 = 1$ and $\langle P\rangle\langle Q\rangle^2 = 1$, which imply that $\langle P\rangle = \langle Q\rangle^3$ and $\langle Q\rangle^6 = 1$. Since it is equal to $\langle P\rangle$, $\langle Q\rangle^3 \neq 1$. We saw above that $\langle Q\rangle^2 \neq 1$. The class group is generated by the class $\langle Q\rangle$ of order 6. It is a cyclic group of order 6.

If one wants to check directly that $\langle Q\rangle^6 = 1$, one can do this by showing that $3^6 = 729$ is the norm of an element of R. I think that $729 = N(2 + 5\delta)$.

Exercise. $N(11+\delta) = 121 + 29 = 150 = 2 \cdot 3 \cdot 5^2$. Proceeding as above, we find that $\langle P\rangle\langle Q^{\pm 1}\rangle\langle S\rangle^{\pm 2} = 1$. Reconcile this equation with the information obtained above.

Example 3. $d = -43$. Here $d \equiv 1$ modulo 4. So $\mu = \sqrt{43/3} < 4$. We have to examine the primes 2 and 3. Do they split in R? In this case, R is generated, not by δ, but by $\frac{1}{2}(1+\delta)$, which is the midpoint of the rectangle with vertices $0, 1, \delta, 1+\delta$. Proceding as above, in (), a prime p splits if and only if the polynomial

$$x - (\overline{\eta} + \eta)x + \overline{\eta}\eta = x^2 - x + \frac{1-d}{4} = x^2 - x + 11$$

has a root modulo p. It has no root modulo 2 or 3, so neither of these primes splits. The class group is generated by the empty set. It is a trivial group. Therefore R is a Unique Factorization Domain (see Proposition 4 of the Summaries for March 29 and 31).

Example 4. $d = v - 89$. Here $d \equiv 3$ modulo 4, so $\mu = 2\sqrt{89/3} < 2\sqrt{30} < 11$. The class group is generated by the primes $< \mu$ that split in R. The primes $< \mu$ are $2, 3, 5, 7$, and they all split. Say $(2) = \overline{P}P$, $(3) = \overline{Q}Q$, $(5) = \overline{S}S$, and $(7) = \overline{T}T$, and $P = \overline{P}$, so the class $\langle P\rangle$ has order 2. We compute some norms:

$N(1+\delta) = 90 = 2 \cdot 3^2 \cdot 5$
$N(3+\delta) = 98 = 2 \cdot 7^2$
$N(6+\delta) = 125 = 5^3$

The last of these shows that $(6-\delta)(6+\delta) = (5)^3 = (\overline{S}S)^3$. Therefore $(1+\delta)$ is either S^3 or $\overline{S}^3$, and in either case, $\langle S\rangle^3 = 1$.

Next, $N(3+\delta) = 2 \cdot 7^2$ shows that $(3-\delta)((3+\delta) = \overline{P}P(\overline{T}T)^2$, and since $P = \overline{P}$, $(3+\delta) = PT^{\pm 2}$. In either case, $\langle P\rangle = \langle T\rangle^2$. Since $\langle P\rangle$ has order 2, $\langle T\rangle^4 = 1$. It follows that $\langle T\rangle$ has order 4.

The fact that $\langle P\rangle = \langle T\rangle^2$ allows us to eliminate $\langle P\rangle$ from the list of generators, and using $N(1+\delta)$, on can eliminated $\langle Q\rangle$. So the class group is generated by two elements, of orders 3 and 4 , respectivly. It is a product $C_3 \times C_4$ of cyclic groups of orders 3 and 4, and is also isomorphic to a cyclic group of order 12. This is the largest order that occurs with $|d| < 100$.