LECTURE 19: CHAPTER 10 : RINGS

from Stillwell's Elements of Number Theory.

Begin with the definition of a set "like" $\mathbb{Z}$, the ring

Def/ Let R be a set together with a function $+ : R \times R \to R$ and $\times : R \times R \to R$ known as addition and multiplication such that

1.) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$.
2.) $\exists 0 \in R$ s.t. $a + 0 = 0 + a = a \quad \forall a \in R$
3.) for each $a \in R$ there exists $-a \in R$ s.t. $a + (-a) = 0 = (-a) + a$
4.) $a + b = b + a \quad \forall a, b \in R$

Where we also have,

5.) $a \times (b \times c) = (a \times b) \times c \quad \forall a, b, c \in R$
6.) $a \times b = b \times a \quad \forall a, b \in R$
7.) $a \times 1 = a \quad \forall a \in R$
8.) $a \times 0 = 0 \quad \forall a \in R$
9.) $a \times (b + c) = a \times b + a \times c \quad \forall a, b, c \in R$

- Axiom 4 makes $+$ an abelian group $(R, +)$. Well, technically Axioms 1, 2, 3, 4 and $+ : R \times R \to R$ a function makes R an abelian group under $+$.
- Ok, so this is a lot of structure, but, notice nothing for sure about $\%$. Just $1 \in R$

Continuing discussion from 1. A ring by default is a commutative ring (w.r.t. $\times$)
But, $\mathbb{H}$ has structure of noncommutative ring. And, often we have more structure, but more on that as we continue.

Remark: some books use Rng to denote a "Ring without identity". Or, from that viewpoint a Ring is a Rng with identity.

Collecting the Comments: a ring is just the set together with the basic op. of $+$ and $\times$ paired in the usual way. We don't get $\%$, or multiplicative norm, or unique prime factorization just from ring definition. That stuff is extra.

Examples

$$R = \mathbb{Z}$$

$$R = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

$$\left.\begin{array}{l} R = \mathbb{Q} \\ R = \mathbb{R} \\ R = \mathbb{C} \end{array}\right\}$$ these are more than mere rings. These are fields as we soon discuss.

DIVISIBILITY AND PRIMES

Often we simply denote $a \times b = ab$.

Def^n/ $b \mid a$ if $\exists c$ such that $a = bc$ (here $a, b, c \in R$ a ring)

Of course, we've seen this before, and also

Def^n/ $a \in R$ is <u>prime</u> if the only divisors of a are <u>units</u> and <u>associates</u> of a. We say b is an <u>associate</u> of a if there is a unit u s.t. $b = au$. And a <u>unit</u> is a divisor of 1.

Sorry to be lazy. Of course logically define ① unit ② associate ③ prime.

§10.2 RINGS & FIELDS

A FIELD IS A SPECIAL KIND OF RING,

Def^n/ $\mathbb{F}$ is a <u>field</u> if $\mathbb{F}$ is a ring where $x \neq 0$ is a unit for each such $x \in \mathbb{F}$

Notice a field has no primes since we may factor $a = \frac{1}{b}(ba)$. Every $x \in \mathbb{F}$ is a multiply of $y \in \mathbb{F}$ for $x, y \neq 0$ as $x = \left(\frac{x}{y}\right) y$.

<u>CONCEPT</u>: often a set of numbers is constructed to <u>close</u> some operation. $\mathbb{N} \longrightarrow \mathbb{Z}$ to allow subtraction. $\mathbb{Z} \longrightarrow \mathbb{Q}$ to allow division. $\mathbb{Q} \longrightarrow \mathbb{R}$ to make Cauchy sequences converge. $\mathbb{R} \longrightarrow \mathbb{C}$ to make $f(x) = 0$ have n-sol^{c}s for $\deg(f(x)) = n$. But, in addition to these standard additions we have:

$$\mathbb{Z}[a] = \underbrace{\mathbb{Z} \cup \{a\}}_{\text{with all possible sums, differences and products}}$$

$\mathbb{Z}[a,b]$ = smallest ring with $\mathbb{Z} \cup \{a,b\}$ contained.

$\mathbb{Z}[i,j,k]$ = smallest ring with $\mathbb{Z}, i, j$ & k

$\mathbb{Z}\left[\frac{1+i+j+k}{2}, i, j, k\right]$ = Hurwitz Integers.

In contrast, to close under $+, \times$ and division,

$\mathbb{F}(a)$ = smallest field containing $\mathbb{F}$ and a.

<u>Example</u>: $\mathbb{Q}(\sqrt{2})$ = field with $\mathbb{Q}$ & $\sqrt{2}$.
We proved that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

<u>Comment</u>: in Math 422, much more is said about $\mathbb{F}(a)$, here no abstraction really needed as we do most everything <u>inside</u> $\mathbb{C}$ where complex math works.

FINITE RINGS & FIELDS

$\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ as it's sometimes called is a ring. When $n = p$ is prime then $\mathbb{Z}_p$ forms a <u>field</u>. Moreover, we can always consider the <u>group of units</u> inside $\mathbb{Z}_n$. For $\mathbb{Z}_p$ the group of units is $G = \mathbb{Z}_p - \{\bar{0}\}$ whereas for general composite n it is a bit complicated, but we do know $\exists\ \underbrace{\varphi(n)}_{\text{Euler Phi Fnct.}}$ elements. For example,

$$\mathbb{Z}_{15} \text{ has } \varphi(15) = \varphi(3\cdot 5) = \varphi(3)\varphi(5) = 2\cdot 4 = 8.$$

§ 10.3 ALGEBRAIC INTEGERS

We begin by setting the stage which is <u>very</u> big

Def/ A number $\alpha \in \mathbb{C}$ is algebraic if there exists $P(x) = a_m x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$ where $a_m, \dots, a_1, a_0 \in \mathbb{Z}$ and $P(\alpha) = 0$ where m is <u>smallest</u> such $m \in \mathbb{N} \cup \{0\}$ for which $P(\alpha) = 0$. (m is degree of α)

<u>Example</u>: $\frac{a}{b} \in \mathbb{Q}$ is algebraic where $a, b \in \mathbb{Z}$ since $P(x) = bx - a$ has $P(\frac{a}{b}) = b\frac{a}{b} - a = 0$. Likewise if α is degree 1 $\Rightarrow \exists\, P(x) = a_1 x + a_0$ s.t. $P(\alpha) = \underbrace{a_1\alpha + a_0}_{\deg 1 \Rightarrow a_1 \neq 0} = 0 \therefore \alpha = \frac{-a_0}{a_1} \in \mathbb{Q}$.

We've seen $\mathbb{Q}$ forms the subset of the algebraic #'s of degree 1. Of course there is much more to find

$\sqrt{2}$ is algebraic # as $P(x) = x^2 - 2$ has $P(\sqrt{2}) = 0$

$\frac{1}{\sqrt{2}}$ is algebraic # as $P(x) = 2x^2 - 1$ has $P\left(\frac{1}{\sqrt{2}}\right) = 0$

There is more... Stillwell remarks that the algebraic #'s form a field (this we don't prove this semester)

Def^n/ A number $\alpha \in \mathbb{C}$ is an algebraic integer if it has $P(\alpha) = 0$ for monic polynomial P with $\mathbb{Z}$-coeff.

Examples

$\alpha \in \mathbb{Z}$ has $P(x) = x - \alpha$ with $P(\alpha) = \alpha - \alpha = 0$.

$\alpha \in \mathbb{Q}$ is NOT also algebraic integer as $\alpha = \frac{a}{b}$ has $b\left(\frac{a}{b}\right) - a = 0$ ($P(x) = b(x) - a$

UNLESS $b = 1$ in which case $\alpha \in \mathbb{Z}$.

- the only algebraic integers inside $\mathbb{Q}$ are just the ordinary integers $\mathbb{Z}$.

Examples

$\sqrt[3]{2} : x^3 - 2 = 0$ $\qquad$ $\frac{-1+\sqrt{-3}}{2} : x^2 + x + 1 = 0$.

$\sqrt[5]{3} : x^5 - 3 = 0$

Thm (Closure Properties of algebraic integers)

If α and β are algebraic integers then so are $\alpha+\beta$, $\alpha-\beta$ and $\alpha\beta$.

p. 187 Stillwell

Proof: By assumption & defn of alg. integers $\exists a_0, .., a_{m-1}, b_0, .., b_{n-1} \in \mathbb{Z}$ for which

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$$
$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_1\beta + b_0 = 0.$$

Then solve for α^m & β^n

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha - a_0$$
$$\alpha^{m+1} = -a_{m-1}\alpha^m - \cdots - a_1\alpha^2 - a_0\alpha$$
$$\vdots$$

α^j = linear combination of $1, \alpha, .., \alpha^{m-1}$ with integer coefficients

Likewise $\beta^n = -b_{n-1}\beta^{n-1} - \cdots - b_1\beta - b_0$ * $\Rightarrow$ any power $\beta^j \in \text{span}_{\mathbb{Z}}\{1, \beta, .., \beta^{n-1}\}$ as higher-powers can always be brought down by *. Hence

$$P(\alpha,\beta) = \underbrace{\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} c_{ij}\alpha^i\beta^j}_{} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} c_{ij}\alpha^i\beta^j$$

Polynom. $P \Rightarrow$ finitely many $c_{ij} \neq 0$ for $c_{ij} \in \mathbb{Z}$

Continuing ⑦, If we denote $\alpha^i\beta^j = w_1, w_2, \dots, w_{mn}$ then any poly. in $\alpha, \beta \in \text{span}\{w_1, \dots, w_{mn}\}$ hence: ⓐ

If $\alpha+\beta$, $\alpha-\beta$ or $\alpha\beta = w$ we have $\exists\, k_1, \dots, k_{mn}$ s.t.

$$w = k_1 w_1 + k_2 w_2 + \cdots + k_{mn} w_{mn}$$

$$\Rightarrow w w_1 = k_1 w_1^2 + k_2 w_2 w_1 + \cdots + k_{mn} w_{mn} w_1 \quad \text{by ⓐ}$$
$$= k_1' w_1 + k_2' w_2 + \cdots + k_{mn}' w_{mn}$$

Likewise for $ww_2, ww_3, \dots, ww_{mn}$. Notice we can write these eq$^{\underline{n}}$'s in total as:

$$\underbrace{\begin{bmatrix} k_1'-w & k_2' & \cdots & k_{mn}' \\ k_1'' & k_2''-w & \cdots & k_{mn}'' \\ \vdots & & & \\ \vdots & & & \\ k_1^{(mn)} & k_2^{(mn)} & \cdots & k_{mn}^{(mn)}-w \end{bmatrix}}_{M(w)} \underbrace{\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ \vdots \\ w_{mn} \end{bmatrix}} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

$\exists$ nonzero sol$^{\underline{n}}$, $\exists$ zero sol$^{\underline{n}}$ $\therefore M^{-1}$ d.n.e. by linear algebra!

Hence,

$$\det(M(w)) = 0$$

$$\therefore \pm w^{mn} + \cdots + c_{mn} = 0$$

← in more detail this can be written as monic poly. which has $w = \alpha+\beta$, $\alpha-\beta$ or $\alpha\beta$ as sol$^{\underline{n}}$ $\therefore \alpha\pm\beta, \alpha\beta$ are algebraic integers.

~~Of course if we trust still well they're~~ more ~~indeed a~~ Γ duh.
Algebraic Numbers are field

$\boxed{\textbf{Cor:} \text{ Algebraic integers} \subseteq \mathbb{C} \text{ form a RING.}}$

(not same)

§10.4 Quadratic Fields and Their Integers

- The ring of all algebraic integers does not have unique factorization, simply note $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ $\Rightarrow$ no primes for algebraic integers. However, there are primes w.r.t <u>subsets</u> of the alg. integers. The concept of prime depends on context.

  Notice $3 \in \mathbb{Z}$ is prime (in $\mathbb{Z}$)

  But $3 \in \mathbb{R}$ has $3 = 2\left(\frac{3}{2}\right)$ $\therefore$ 3 not prime in $\mathbb{R}$.

  So be careful to consider "primeness" in context.

- $\mathbb{Z}[i]$ & $\mathbb{Z}[\sqrt{-2}]$ are formed by the intersection of all algebraic integers and the <u>fields</u> $\mathbb{Q}(i)$ & $\mathbb{Q}(\sqrt{-2})$. Recall,

$\boxed{\text{Def}^{\underline{n}}/\ \mathbb{Q}(\sqrt{d}) \text{ where } d \in \mathbb{Z} \text{ is the smallest field containing } \mathbb{Q} \text{ and } \sqrt{d}}$

- $d \neq 0$ to keep it interesting & $d = n^2$ as 0 and $\sqrt{n^2} = n$ are both in $\mathbb{Q}$ $\therefore$ $\mathbb{Q}(\sqrt{n^2}) = \mathbb{Q}$.

- $n \in \mathbb{N}$, squarefree $\Rightarrow \sqrt{n}$ is irrational and $\mathbb{Q}(\sqrt{n})$ is called a <u>real</u> <u>quadratic</u> <u>field</u>.

- $n \in \mathbb{N}$, squarefree $\Rightarrow \sqrt{-n} = i\sqrt{n}$ where $\sqrt{n}$ irrational and $\mathbb{Q}(\sqrt{-n})$ is called an <u>imaginary</u> <u>quadratic</u> <u>field</u>

There is a big difference between real & imaginary quadratic fields in terms of <u>units</u>. We soon show imaginary case has at most 6 whereas real has infinitely many.

Th^m/ Let d be square free and $d \neq -n^2$ for some $n \in \mathbb{N}$ and $d \neq 0$ to keep it interesting then
$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{d}]$$

Proof: Let $a, b, c, \tilde{d} \in \mathbb{Q}$ and consider, $a \pm b$, $c \pm \tilde{d} \in \mathbb{Q}$ as well etc. thus,
$$(a + b\sqrt{d}) \pm (c + \tilde{d}\sqrt{d}) = a \pm c + (b \pm \tilde{d})\sqrt{d} \in \mathbb{Q}[\sqrt{d}].$$
$$(a + b\sqrt{d})(c + \tilde{d}\sqrt{d}) = ac + b\tilde{d}d + (bc + a\tilde{d})\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$
and if $z \in \mathbb{Q}(\sqrt{d})$ with $z = x + y\sqrt{d} \neq 0$ then,
$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{x - y\sqrt{d}}{x^2 + dy^2}$$
and $\frac{x}{x^2+dy^2}, \frac{-y}{x^2+dy^2} \in \mathbb{Q} \Rightarrow \frac{1}{z} \in \mathbb{Q}[\sqrt{d}]$

thus $\mathbb{Q}[\sqrt{d}]$ is closed under $+$, $\times$ and division hence $\mathbb{Q}[\sqrt{d}]$ is field containing $\mathbb{Q}$ and $\sqrt{d}$. Moreover, any smaller field would not be closed from our calculations above $\therefore$ $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d})$. //

(precise th^m given $\Rightarrow$ next page.

Comment: since $x^2 - d = 0$ has $\alpha = \pm\sqrt{d}$ as sol^n's, we $\pm\sqrt{d}$ are algebraic integers thus $\mathbb{Z}[\sqrt{d}]$ is certainly a subset of algebraic integers contained in $\mathbb{Q}(\sqrt{d})$.

But, this is not all the algebraic integers that can be found in $\mathbb{Q}(\sqrt{d})$ for example $\mathbb{Z}[\zeta_3] \subseteq \mathbb{Q}(\sqrt{-3})$ as
$$\zeta_3^2 + \zeta_3 + 1 = 0 \Rightarrow \zeta_3 \text{ is quad. integer}$$
and $\mathbb{Q}(\sqrt{-3})$ includes $\mathbb{Z}[\sqrt{-3}]$ and rational extensions...

Th$^{\underline{m}}$/ Assume $d \in \mathbb{Z}$ is not divisible by any square except 1. Then,

(1.) when $d \not\equiv 1 \pmod 4$ the integers of $\mathbb{Q}(\sqrt{d})$ are of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$.

(2.) when $d \equiv 1 \pmod 4$ the integers of $\mathbb{Q}(\sqrt{d})$ are $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ or $a + 1/2,\ b + 1/2 \in \mathbb{Z}$.

Proof: If $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is also an algebraic integer it follows $\exists\ P(x) = x^2 + Ax + B$ for which $P(a + b\sqrt{d}) = 0$ and we can show $a - b\sqrt{d}$ is the other sol$^{\underline{n}}$ of $P(x) = 0$.

$$(a + b\sqrt{d})^2 + A(a + b\sqrt{d}) + B = 0$$

$$a^2 + ab\sqrt{d} + b^2 d + Aa + Ab\sqrt{d} + B = 0$$

Well, let's complete the square,

$$\begin{aligned}
P(x) &= x^2 + Ax + B \\
&= (x + A/2)^2 + B - A^2/4 \\
&= (x + A/2)^2 - \tfrac{1}{4}(A^2 - 4B) \\
&= (x + A/2)^2 - \left(\frac{\sqrt{A^2 - 4B}}{2}\right)^2 \\
&= \left(x + \frac{A}{2} - \frac{1}{2}\sqrt{A^2 - 4B}\right)\left(x + \frac{A}{2} + \frac{1}{2}\sqrt{A^2 - 4B}\right) \\
&= (x - (a + b\sqrt{d}))(x - r_2)
\end{aligned}$$

wlog, $a + b\sqrt{d} = \frac{-A}{2} + \frac{1}{2}\sqrt{A^2 - 4B}$ & $r_2 = \frac{-A}{2} - \frac{1}{2}\sqrt{A^2 - 4B}$

Since d is squarefree we can equate as follows:

$$a = -\frac{A}{2} \quad \& \quad b\sqrt{d} = \frac{1}{2}\sqrt{A^2 - 4B}$$

Hence $r_2 = \frac{-A}{2} - \frac{1}{2}\sqrt{A^2 - 4B} = a - b\sqrt{d}$. (Stillwell says to use the quadratic f-la, I just decided to work it out.)

continued from 11

From our algebra for $a+b\sqrt{d} = \frac{-A}{2} + \frac{1}{2}\sqrt{A^2-4B}$

$a = \frac{-A}{2}$ & $b\sqrt{d} = \frac{1}{2}\sqrt{A^2-4B}$

$\hookrightarrow$ $\underline{A = -2a}$.

$b^2 d = \frac{1}{4}(A^2-4B) = A^2/4 - B$

$\therefore B = A^2/4 - b^2 d = \underline{a^2 - db^2 = B}$.

Note, $A, B \in \mathbb{Z}$ thus $2a,\ a^2-db^2 \in \mathbb{Z}$. Thus, ① $\underline{a \in \mathbb{Z}}$ or ② $\underline{a+1/2 \in \mathbb{Z}}$. If $a \in \mathbb{Z}$ then

---

① $a^2 \in \mathbb{Z} \Rightarrow db^2 \in \mathbb{Z}$ (since $a^2-db^2 \in \mathbb{Z}$)

$\Rightarrow b^2 \in \mathbb{Z}$ ($n^2 \nmid d \Rightarrow b^2 \neq m^2/n^2$) (when $n>1$)

$\Rightarrow \underline{b \in \mathbb{Z}}$

---

② If $a + 1/2 \in \mathbb{Z}$ $\therefore$ $2a \in 2\mathbb{Z}+1 \Rightarrow (2a)^2 \equiv 1 \pmod 4$

Thus $a^2 - db^2 \in \mathbb{Z} \Rightarrow (2a)^2 - d(2b)^2 \equiv 0 \pmod 4$ (☆)

$\Rightarrow (2a)^2 \equiv d(2b)^2 \equiv 1 \pmod 4$

$\Rightarrow d \equiv 1 \pmod 4$ <u>and</u> $(2b)^2 \equiv 1 \pmod 4$

as $(2b)^2 \equiv 3 \pmod 4$ is not allowed for a square.

$\Rightarrow d \equiv 1 \pmod 4$ and $2b \equiv 1 \pmod 2$

$\Rightarrow d \equiv 1 \pmod 4$ and $\underline{b + 1/2 \in \mathbb{Z}}$.

$-2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$?

$a^2 - (4m+1)b^2 =$

$= a^2 - b^2 - 4mb^2$

We assumed $a+b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ and found $a, b \in \mathbb{Z}$ or $a+1/2,\ b+1/2 \in \mathbb{Z}$. Consider $d = 4m+1$ ($d \equiv 1 \bmod 4$) and study sol'n's of $x^2 - 2ax + (a^2-db^2) = 0$

$$x = \frac{2a \pm \sqrt{4a^2 - 4(a^2-db^2)}}{2} = a \pm \sqrt{4b^2 d}$$
$$= a \pm 2b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

(Stillwell claims it suffices to show the coeff. are in $\mathbb{Z}$

§10.5 Norm and Units of Quadratic Fields

The norm on $\mathbb{Q}(\sqrt{d})$ is defined by:

$$\boxed{\text{Def}^{n}/\ \text{norm}(a+b\sqrt{d}) = a^2 - db^2}$$

It's clear from our work in §10.4 that $a^2-db^2 \in \mathbb{Z}$ when $a+b\sqrt{d}$ is a quadratic integer. We already studied this in a few cases:

Example: $d=-1$, $\text{norm}(a+b\sqrt{-1}) = a^2+b^2$; $\mathbb{Z}[i]$
$d=-2$, $\text{norm}(a+b\sqrt{-2}) = a^2+2b^2$; $\mathbb{Z}[\sqrt{-2}]$

We can show (much as before) that

$$\boxed{\text{norm}(z_1 z_2) = \text{norm}(z_1)\,\text{norm}(z_2) \quad \text{for } z_1, z_2 \in \mathbb{Q}(\sqrt{d})}$$

This amounts to, for $z_1 = a_1+b_1\sqrt{d}$ & $z_2 = a_2+b_2\sqrt{d}$,

$$\boxed{(a_1a_2+db_1b_2)^2 - d(a_1b_2+a_2b_1)^2 = (a_1^2-db_1^2)(a_2^2-db_2^2)}$$

$d=-1$ gives Diophantus Identity

$d>0$ have Brahmagupta's identity

We find,

$$\boxed{\begin{array}{l}\text{Th}^{m}/\ \text{If } x_1 \mid x_2 \text{ for integers } x_1, x_2 \text{ of } \mathbb{Q}(\sqrt{d}) \\ \quad \text{then } \text{norm}(x_1) \mid \text{norm}(x_2)\end{array}}$$

Recall u is a unit of the integers of $\mathbb{Q}(\sqrt{d})$ if

$u \mid 1 \Rightarrow \text{norm}(u) \mid \text{norm}(1) \Rightarrow \text{norm}(u) \mid 1$

$\therefore$ $\underline{\text{norm}(u) = \pm 1}$.

Continuing to discuss units in integers of $\mathbb{Q}(\sqrt{d})$

u a unit $\Rightarrow$ norm$(u) = \pm 1$.

Conversely norm $(a+b\sqrt{d}) = a^2 - db^2 = \pm 1$ then

$$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 = \pm 1$$

Hence $a+b\sqrt{d} \mid 1$.

How many units?

- If $d>1$ then $x^2 - dy^2 = 1$ is Pell's Eq^{n} then $\exists\, \infty$ly many sol^{n}s hence units.
  $\mathbb{Q}(\sqrt{2})$ has units as sol^{n} $x^2 - 2y^2 = 1 \leftrightarrow \pm(3+2\sqrt{2})^n$ units -2
- If $d<0$ then $\exists$ finitely many sol^{n} of $x^2 - dy^2 = 1$
  - $\mathbb{Z}[i]$ has $\pm 1, \pm i$
  - $\mathbb{Z}[\sqrt{-2}]$ has ± 1
  - $\mathbb{Z}[\zeta_3]$ has $\pm 1, \pm \zeta_3, \pm \zeta_3^2$ $\leftarrow$ ~~most~~ almost all the possible for integers of imaginary quad. field.

$$\boxed{\text{Th}^{m}/\ \text{The only units among the integers of imaginary quad. field are } \pm 1, \pm i, \pm \zeta_3, \pm \zeta_3^2}$$

Proof: