Lecture 21: (Chapter 11: Ideals, Stillwell Elements of Number Theory)

In Chapter 10 we studied examples of ideals. Let us recall a few definitions for easy reference:

Def^n/ Given a commutative ring with identity R a subset $I \subseteq R$ is an <u>ideal</u> if $\forall x, y \in I$ and $r \in R$ we have $x + y \in I$ and $rx \in I$.

Def^n/ $(a) = \{ar \mid r \in R\} = aR$ is <u>principal ideal generated</u> by a. If I is an ideal for which $\nexists\, a \in I$ s.t. $I = (a)$ then we say I is a <u>non-principal ideal</u>

For the integers we'll prove a few specific claims about ideals in $\mathbb{Z}$. To look ahead:

1.) every ideal $I \subseteq \mathbb{Z}$ has $I = (n) = n\mathbb{Z}$; that is, all ideals in $\mathbb{Z}$ are principal.
2.) $a \mid b$ iff $(a) \supseteq (b)$; divisible by $\Rightarrow$ contains in.
3.) $(\gcd(a,b)) = \{am + bn \mid m, n \in \mathbb{Z}\} = (a) + (b)$.
4.) p is prime $\Longleftrightarrow$ (p) is <u>maximal</u>

In rings which are not unique factorization domains we found non-principal ideals; $\mathbb{Z}[\sqrt{-5}]$ has the gcd ideal of $(2) + (1 + \sqrt{-5})$ ... this leads to product of ideals... we seek to study prime & maximal ideals further here.

Def^n/ I an ideal of R is <u>maximal</u> if no larger ideal $J \supseteq I$ and yet $J \neq R$.

* see ~~previous~~ future Lectures for details here...

§11.1 Ideals and the gcd

① We saw $4 = 2\times 2 = (1+\sqrt{-3})(1-\sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$

was "fixed" by $\underbrace{2\times 2 = 2\left(\frac{1+\sqrt{-3}}{2}\right) 2\left(\frac{1-\sqrt{-3}}{2}\right) = (1+\sqrt{-3})(1-\sqrt{-3})}_{\text{in } \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]}$

where $\frac{1\pm\sqrt{-3}}{2}$ are <u>units</u> in the Eisenstein integers $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ hence 2 & $1\pm\sqrt{-3}$ are <u>associates</u> and what was a non-unique factorization of 4 in $\mathbb{Z}[\sqrt{-3}]$ is now just a reording of a prime factorization by associates of the initial factorization.

② In $\mathbb{Z}[\sqrt{-5}]$, $6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

all prime in $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Q}(\sqrt{-5})$ has no additional units in its algebraic integers to rescue us as in ①.

... will "fix" with <u>ideals</u> the <u>ideal numbers</u> are formed by <u>sets</u> of <u>multiples</u> of numbers

MULTIPLES VS. #'S

$$(4) = 4\mathbb{Z} = \{0, \pm 4, \pm 8, \pm 12, \ldots\}$$
$$(6) = 6\mathbb{Z} = \{0, \pm 6, \pm 12, \pm 18, \ldots\}$$

Add (4) & (6) by adding $x \in (2)$ & $y \in (6)$ to obtain

$$(4)+(6) = \{0, \pm 2, \pm 4, \ldots\} = (2) = (\gcd(4,6)).$$

(this illustrates the def$^{\underline{n}}$ of $I+J$ which follows)

Def^{n}/ If R is a ring with identity and $I \subseteq R$ then I is an <u>ideal</u> if for each $x, y \in I$ and $r \in R$ we have $x + y \in I$ and $rx \in I$.

This definition is modelled on patterns we've seen for $n\mathbb{Z}$, we'll soon argue multiples of $n \in \mathbb{Z}$ forms an ideal. But, sticking with Stillwell, let me first define $I+J$ and then prove it forms a new ideal from given ideals I & J.

Def^{n}/ If I, J are ideals of R then define
$$I + J = \{ x + y \mid x \in I, y \in J$$

Th^{m}/ If I, J are ideals of R then $I+J$ is an ideal of R.

<u>Proof</u>: Suppose I, J ideals of R. Consider $z_1, z_2 \in I+J$ and $r \in R$. Observe $\exists\, x_1, x_2 \in I$ and $y_1, y_2 \in J$ s.t. $z_1 = x_1 + y_1$ and $z_2 = x_2 + y_2$ by def^{n} of $I+J$. Hence,

$$\begin{aligned} z_1 + z_2 &= (x_1 + y_1) + (x_2 + y_2) \\ &= (x_1 + x_2) + (y_1 + y_2) \Leftarrow \left[\begin{array}{l}\text{prop. of } R,\ + \\ \text{is commutative} \\ \text{and associative.}\end{array}\right. \\ &= x_3 + y_3 \in \end{aligned}$$

As $x_1 + x_2 = x_3 \in I$ and $y_1 + y_2 = y_3 \in J$ since I, J ideals. Thus $z_1 + z_2 = x_3 + y_3 \in I + J$. Likewise

$$\begin{aligned} r z_1 &= r(x_1 + y_1) \\ &= \underbrace{r x_1}_{\in I} + \underbrace{r y_1}_{\in J} \overbrace{= x_4 + y_4 \text{ for } x_4 \in I, y_4 \in J}^{\text{if you prefer this style}} \end{aligned}$$

as I & J ideals.

$$\therefore r z_1 \in I + J$$

Hence $I+J$ is an ideal. //

§11.2 Ideals & Divisibility in $\mathbb{Z}$:

Def^n/ $(n) = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ is the principal ideal generated by n.

<u>Example</u>: $(3) = \{0, \pm 3, \pm 6, \dots\}$
$(6) = \{0, \pm 6, \pm 12, \dots\}$ observe $\underbrace{(3) \supseteq (6)}$

this is more commonly denoted $(6) \subseteq (3)$
(6) is subset of (3)

<u>Example</u>: $(3) = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \dots\}$
$(4) = \{0, \pm 4, \pm 8, \pm 12, \dots\}$

Neither $(3) \supseteq (4)$ nor $(4) \supseteq (3)$.
However, $(12) = \{0, \pm 12, \pm 24, \dots\}$
is contained by both; $(3) \supseteq (12)$ and $(4) \supseteq (12)$

All of this leads us to extend divisibility to ideals in terms of <u>containment</u>

$3 \mid 6$ and note $(3) \supseteq (6)$

$3 \nmid 4$ and so $(3) \not\supseteq (4)$

$4 \nmid 3$ and also $(4) \not\supseteq (3)$

$3 \mid 12$ and $4 \mid 12$ and we saw $(3) \supseteq (12)$ & $(4) \supseteq 12$

<u>Looking Forward</u>: a slogan: where divisibility "fails" us in the abstract perhaps containment of ideals will "fix" things...

Next up, show containment models divisibility etc. for $\mathbb{Z}$.

Th$^{\underline{m}}$/ (n) is an ideal of $\mathbb{Z}$ for each $n \in \mathbb{Z}$.

Proof: Let $x, y \in (n)$ and $r \in \mathbb{Z}$. Observe $\exists\, k, l \in \mathbb{Z}$ for which $x = kn$ and $y = ln$ thus $x + y = kn + ln = (k+l)n \in (n)$ as $k + l \in \mathbb{Z}$. Likewise $rx = (rk)n \in (n)$ as $rk \in \mathbb{Z}$ $\therefore$ (n) is an ideal. //

More is true for $\mathbb{Z}$. In fact, the only kind of ideals in $\mathbb{Z}$ are those of the form (n).

Th$^{\underline{m}}$/ If I is an ideal in $\mathbb{Z}$ then $I = (n)$ for some $n \in \mathbb{Z}$.

Proof: Let $I \subseteq \mathbb{Z}$ be an ideal. Let a be the smallest element in I which is positive. We claim $I = (a)$. Suppose, to the contrary, that $b \in I$ but $b \notin (a)$. Here's a picture,

There exists $q = na$ such that $b - q = r$ where $r < a$. However, $b, q \in I \Rightarrow b - q = r \in I$ and this contracts our construction of $a \in I$ as the smallest positive element. Thus no such $b \notin (a)$ exists and we conclude $I = (a)$. //

Def$^{\underline{n}}$/ If every ideal in a ring is generated by some element; $I \subseteq R$ an ideal $\Rightarrow$ $I = (r)$ for some $r \in R$ then R is a principal ideal domain or PID.

Remark: we just proved $\mathbb{Z}$ is a P.I.D.

Lemma ① $a, b \in \mathbb{Z}$. If a/b then $(a) \supseteq (b)$.

Proof: Suppose a/b then $b = ma$ for some $m \in \mathbb{Z}$ $\therefore$ $b \in (a)$.
Let $x \in (b)$ then $x = bk$ for some $k \in \mathbb{Z}$ $\Rightarrow$ $x = (ma)k = (mk)a$
but $mk \in \mathbb{Z}$ thus $x \in (a)$ and this shows $(b) \subseteq (a) \Rightarrow (a) \supseteq (b)$. //

Lemma ② $a, b \in \mathbb{Z}$. If $(a) \supseteq (b)$ then a/b.

Proof: Suppose $(a) \supseteq (b)$. Observe $a = a \cdot 1 \in (a)$ and $b = b \cdot 1 \in (b)$.
In particular, $b \in (b) \subseteq (a)$ $\Rightarrow$ $b \in (a)$ $\therefore$ $\exists m \in \mathbb{Z}$ s.t.
$b = ma$ thus a/b. //

Proposition: $a, b \in \mathbb{Z}$, $a/b \iff (a) \supseteq (b)$.

Proof: apply lemmas ① and ②. //

Th^{m}/ $(a) + (b) = (\gcd(a,b))$

remark: the proof I gave in class was a bit different than Stillwell.

Proof: Let $x \in (a)+(b)$ $\Rightarrow$ $x = ma + nb$ for some $m, n \in \mathbb{Z}$.
But, as $\mathbb{Z}$ is PID we know $\exists c \in \mathbb{Z}$ s.t. $(a)+(b) = (c)$
since we proved $(a), (b)$ are ideals and $(a)+(b)$ is also an ideal.
Thus $\exists k \in \mathbb{Z}$ s.t. $kc = ma + nb = x$ for each
$x \in (a)+(b)$. In particular, $a \in (a)+(b)$ and $b \in (a)+(b)$
as $x = 1 \cdot a + 0 \cdot b$ and $x = 0 \cdot a + 1 \cdot b$ produce a & b respective.
Thus $\exists k_1, k_2 \in \mathbb{Z}$ for which $a = k_1 c$ and $b = k_2 c$
hence $c|a$ and $c|b$ thus c is a common divisor of a & b.

(this is not quite clear. Stillwell has argument, see pg. 201, I'll give an argument which does use Euclidean algorithm next ↷

$\boxed{\text{Th}^{m}/ \quad (a)+(b) = (\gcd(a,b))}$

<u>Proof</u>: (following Stillwell closely)

Note $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b \Rightarrow \gcd(a,b) \mid ma+nb \quad \forall m,n \in \mathbb{Z}$. thus, for each $m,n \in \mathbb{Z}$, $\exists k \in \mathbb{Z}$ such that $ma+nb = k\gcd(a,b) \;\therefore\; (a)+(b) \subseteq (\gcd(a,b))$.

Observe $(a)+(b)$ is an ideal as $(a),(b)$ are ideals. Moreover, as $\mathbb{Z}$ is PID there is smallest positive element c in $(a)+(b)$ for which $(c) = (a)+(b)$. Notice $(c) \supseteq (a)$ and $(c) \supseteq (b)$ by def^{n} of $(a)+(b) = \{ma+nb \mid m,n \in \mathbb{Z}\}$ thus $c \mid a$ and $c \mid b \Rightarrow c \mid \gcd(a,b)$. But, we already know c is multiple of $\gcd(a,b) \therefore \gcd(a,b) \mid c$ Hence $\gcd(a,b) = c \;\therefore\; (a)+(b) = (\gcd(a,b))$.

Remark: when we did this in Lecture it seemed easier.

$\boxed{\text{Th}^{m}/ \text{ If } p \text{ is prime and the ideal } (p) \text{ contains } (ab) \text{ then } (p) \supseteq (a) \text{ or } (p) \supseteq (b)}$

<u>Proof</u>: $\S$ $(a) \nsubseteq (p)$ while $(p) \supseteq (ab)$. We seek to show $(p) \supseteq (b)$. Note $(a)+(p)$ contains both (p) and (a) and as $(p) \not\supseteq (a)$ the common divisor of a & p as $p \nmid a$ ~~~~ is $\gcd(a,p) = 1$ Grammar aside, $(a)+(p) = (1)$. Thus, $\exists m,n \in \mathbb{Z}$,

$$1 = am + pn \Rightarrow b = abm + pbn$$

$$\Rightarrow b \in (p) \quad \text{as } p \mid ab \text{ and } p \mid pbn \text{ implies } p \mid (abm + pbn).$$

$$\Rightarrow (b) \subseteq (p). //$$

Remark: the def^{n} of prime ideal waits until §11.7, but it is essentially modelled on the above Th^{m}.

§11.3 Principal Ideal Domains

We've already commented on the fact that $\mathbb{Z}$ is a P.I.D. It's also true that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\zeta_3]$ are PID's, this can be seen as a consequence of the fact $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-2}]$ and the Eisenstein integers are Euclidean Rings.

Def/ A ring R is called a <u>Euclidean Ring</u> if $\exists$ a non-negative $\mathbb{Z}$-valued function $r \longmapsto |r|$ such that $|r| = 0$ iff $r = 0$ and for any $a, b \in R$ with $|b| > 0$, $\exists\, q, r \in R$ s.t. $a = qb + r$ with $0 \leq |r| < |b|$.

Alternatively, we say R is a <u>Euclidean Domain</u>. A Euclidean domain is a ring which has the division property.

Thm/ A Euclidean ring is a PID.

<u>Proof</u>: let R be a Euclidean ring and suppose $I \subseteq R$ is an ideal $I \neq (0)$. Suppose $b \in I$ is an element of minimal norm. It follows $(b) \subseteq I$. Now, if $a \in I$ and $a \notin (b)$ then we'd have $a = qb + r$ for some $q, r \in R$ with $0 < |r| < |b|$ and $r = a - qb \in I$. But, this is impossible as r is an element of I with smaller $|r|$ than $|b|$. Thus $I = (b)$ and as I was arbitrary we conclude that R is a P.I.D. //

- This argument mirrors our proof that $I \subseteq \mathbb{Z}$ must have form $I = (n)$. It also shows us <u>how</u> we should <u>find</u> a generator for an ideal in a Euclidean Domain: search for element of smallest norm.

Thm/ Prime Divisor Property for PID's
If p is a prime in a PID and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: Let p be a prime in a PID and $p \mid ab$ and $p \nmid a$. We seek to show $p \mid b$. Consider,

R a PID $\Rightarrow$ if $I \subseteq R$ is an ideal then $I = (x)$ for some element $x \in R$

Consider $I = \{ar + ps \mid r, s \in R\} = (x)$ for some $x \in R$.
Hence $(x) \supseteq (a)$ and $(x) \supseteq (p) \Rightarrow x \mid a$ and $x \mid p$
But, p is prime $\Rightarrow x = 1 \therefore 1 = ar + ps$ for some $r, s \in R$. Multiply by b, $b = abr + bps$ and as $p \mid ab$ and $p \mid bps \Rightarrow p \mid (abr + bps)$ or $p \mid b$. //

Next: we see ideals in a ring where unique factorization worked all had same shape. In contrast, a ring which permits non-unique factorizations may have non-principal ideals... you can get ideals with different shapes. Next few sections make this comment explicit

§11.4 a nonprincipal ideal in $\mathbb{Z}[\sqrt{-3}]$

For some $a, b, c, d \in \mathbb{Z}$, (pg. 205) (Stillwell)

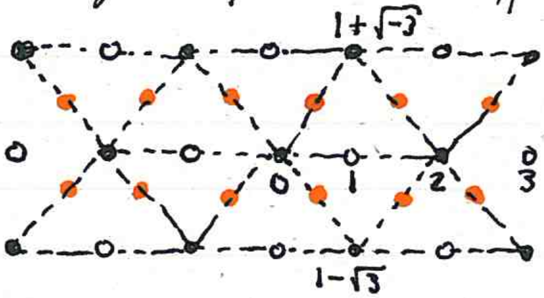
$$
\begin{aligned}
2(a+b\sqrt{-3}) + (1+\sqrt{-3})(c+d\sqrt{-3}) &= \\
&= 2a + 2b\sqrt{-3} + (1+\sqrt{-3})c + d\sqrt{-3} - \underline{3d} \\
&= 2a - \underline{2b} - \underline{4d} + (1+\sqrt{-3})(\underline{2b} + c + \underline{d}) \\
&= 2(a - b - 2d) + (1+\sqrt{-3})(2b + c + d) \\
&= 2m + (1+\sqrt{-3})n \quad \text{for } m, n \in \mathbb{Z}
\end{aligned}
$$

just not super obvious algebra.

Likewise $2m + (1+\sqrt{-3})n \in (2) + (1+\sqrt{-3})$ $\forall m, n \in \mathbb{Z}$. Thus,

$$\boxed{(2) + (1+\sqrt{-3}) = \{2m + (1+\sqrt{-3})n \mid m, n \in \mathbb{Z}\}}$$

This set is an ideal of $\mathbb{Z}[\sqrt{-3}]$. It is geometrically a pattern of equilateral triangles



added ideal #'s

NOT SAME "SHAPE" AS $\mathbb{Z}[\sqrt{-3}]$.

It follows $(2) + (1+\sqrt{-3})$ is a nonprincipal ideal we cannot generate it as (β) for ~~some~~ any $\beta \in \mathbb{Z}[\sqrt{-3}]$ ($\beta \neq 0$ I suppose!)

Remark: $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ has same shape as $(2) + (1+\sqrt{-3})$. We saw $\frac{1+\sqrt{-3}}{2}$ divides both 2 & $1+\sqrt{-3}$ inside $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, moreover $\text{norm}\left(\frac{1+\sqrt{-3}}{2}\right) = 1$ hence $\gcd(2, 1+\sqrt{-3}) = \frac{1+\sqrt{-3}}{2}$.

- THE SHAPE OF $(2) + (1+\sqrt{-3})$ is the same as the principal ideal generated by $\frac{1+\sqrt{-3}}{2}$.

§11.5 A NONPRINCIPAL IDEAL OF $\mathbb{Z}[\sqrt{-5}]$

Consider in $\mathbb{Z}[\sqrt{-5}]$

$$2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

$$\left.\begin{array}{l} \text{norm}(2) = 4 \\ \text{norm}(3) = 9 \\ \text{norm}(1 \pm \sqrt{-5}) = 6 \end{array}\right\} \begin{array}{c} \text{divisors} \\ 2 \text{ \& } 3 \end{array} \Bigg] \begin{array}{c} \text{norm}(a+b\sqrt{-5}) \neq 2,3 \\ \forall\, a,b \in \mathbb{Z}. \\ \therefore\ 2, 3, 1 \pm \sqrt{-5} \text{ are} \\ \text{prime.} \end{array}$$

Do you get the logic here? if $\alpha \mid \beta$ then $\text{norm}(\alpha) \mid \text{norm}(\beta)$ So it suffices to show impossibility by ruling out needed norm patterns.

Need to calculate the gcd ideal of 2 & $1+\sqrt{-5}$. Consider

$$z \in (2)+(1+\sqrt{-5}) \Rightarrow \exists\, a+b\sqrt{-5},\ c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

such that

$$\begin{aligned} z &= 2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) \\ &= 2a + 2b\sqrt{-5} + c(1+\sqrt{-5}) + d\sqrt{-5} - 5d \\ &= 2a - 5d + c(1+\sqrt{-5}) + \underline{(2b+d)}\sqrt{-5} \\ &= 2a - 5d + c(1+\sqrt{-5}) + (2b+d)(\underline{1}+\sqrt{-5}) - \underline{(2b+d)} \\ &= 2a - 6d - 2b + [c+2b+d](1+\sqrt{-5}) \\ &= 2(\underbrace{a-3d-b}_{m}) + [\underbrace{c+2b+d}_{n}](1+\sqrt{-5}) \end{aligned}$$

Hence $(2)+(1+\sqrt{-5}) \subseteq \{2m + n(1+\sqrt{-5}) \mid m,n \in \mathbb{Z}\}$.

Conversely, $2,\ 1+\sqrt{-5} \in \{2m+n(1+\sqrt{-5}) \mid m,n \in \mathbb{Z}\}$

therefore, $\boxed{(2)+(1+\sqrt{-5}) = \{2m + n(1+\sqrt{-5}) \mid m,n \in \mathbb{Z}\}}$

oops, I solved one of your homeworks ☺.

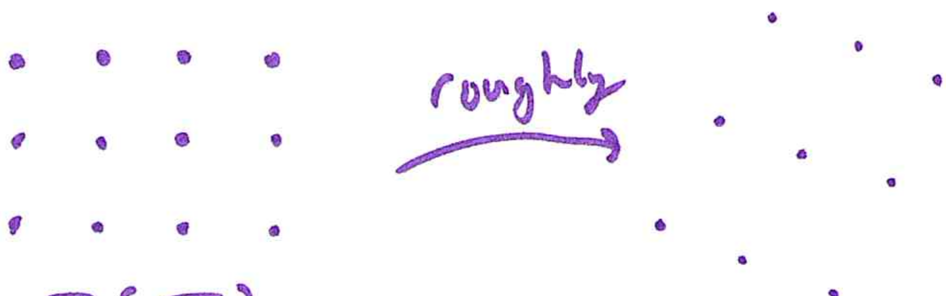
Remark: Stillwell's comment about §8.1 is pointing to wrong section. Probably p. 120 figure 7.1 is ballpark for that comment. I'll attempt to explain ↓

Ex] Let $\beta \in \mathbb{Z}[\sqrt{-5}]$ then $(\beta) = \{\beta\alpha \mid \alpha \in \mathbb{Z}[\sqrt{-5}]\}$

Recall $\beta\alpha$ is multiplication of complex numbers and geometrically we know from Exercise 8.1.2

$$\alpha\beta = |\alpha\beta| e^{ia} e^{ib} = |\alpha\beta| e^{i(a+b)}$$

Geometrically, $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is rotated by angle b of $\beta = |\beta| e^{ib}$ and dilated by $|\beta|$.



$\mathbb{Z}[\sqrt{-5}]$

$\beta\,\mathbb{Z}[\sqrt{-5}]$

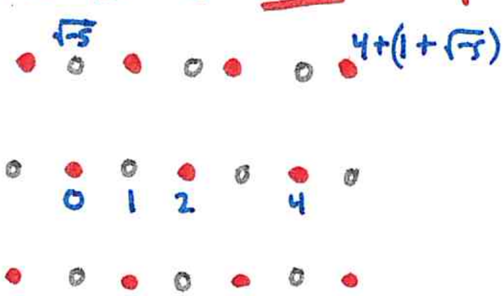
(same shape, just rotated by $\operatorname{Arg}(\beta)$ and stretched by $|\beta|$.

BUT

this is not the shape of $(2)+(1+\sqrt{-5})$ as we found

$$I = (2)+(1+\sqrt{-5}) = \{2m + n(1+\sqrt{-5}) \mid m,n \in \mathbb{Z}\}$$

Hence I is not a principal ideal of $\mathbb{Z}[\sqrt{-5}]$



- the red dots illustrate $I = (2)+(1+\sqrt{-5})$ which clearly is not the rectangular grid shape of $\mathbb{Z}[\sqrt{-5}]$ see pg. 208 for Stillwell's diagram of this.

Additional Comments about $(2)+(1+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$

1.) $(2)+(1+\sqrt{-5})$ is nonprincipal (oh I said this on ②)

2.) since $(a)+(b)=(\gcd(a,b))$ in $\mathbb{Z}$ it is by analogy reasonable to say $(2)+(1+\sqrt{-5})$ is the gcd ideal of (2) and $(1+\sqrt{-5})$. Indeed,

$$(2)+(1+\sqrt{-5}) \supseteq (2) \ \& \ (1+\sqrt{-5})$$

So this is like saying $(2)+(1+\sqrt{-5})$ "divides" both ideals. (Again we wait for § 11.8 to be precise on this point)

3.) $(2)+(1+\sqrt{-5})$ is reasonably called "PRIME". Recall a prime's principal ideal (P) was <u>maximal</u> in the sense only (P) and (1) contain (P). Likewise the only ideal containing $(2)+(1+\sqrt{-5})$ is itself and $\mathbb{Z}[\sqrt{-5}]$ <u>Why?</u>

Notice $(2)+(1+\sqrt{-5}) = \{\underbrace{2m}_{\text{even}} + (1+\sqrt{-5})n \mid m,n \in \mathbb{Z}\}$

Thus points outside of $(2)+(1+\sqrt{-5})$ have form $\underbrace{(2m+1)}_{\text{odd}} + (1+\sqrt{-5})n$ * and any <u>ideal</u> with terms such as * will contain 1 hence all of $\mathbb{Z}[\sqrt{-5}]$ $\therefore$ $(2)+(1+\sqrt{-5})$ is <u>maximal</u>

(later we prove maximal $\Rightarrow$ prime)

[Note: we have not even <u>defined</u> the term "prime ideal" as we have yet to construct the product of ideals.]

We do show eventually $(2)+(1+\sqrt{-5}) \supseteq (2) \Rightarrow (2) = \big((2)+(1+\sqrt{-5})\big) \times I$ ← product of ideals

§11.6: Ideals of imaginary quadratic fields as lattices

We saw ideals of $\mathbb{Z}$ need just one generator. Well, ideals of the integers of $\mathbb{Q}(\sqrt{d})$, for d squarefree, have ideals generated by <u>at</u> <u>most</u> <u>two</u> generators. We almost proved the integers of $\mathbb{Q}(\sqrt{d})$ are of the form $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

in either case these integers form <u>subgroup</u> of $\mathbb{C}$ with two generators:

$\mathbb{Z}[\sqrt{d}]$ generated by 1 & $\sqrt{d}$

$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ generated by 1 & $\frac{1+\sqrt{d}}{2}$

All of this for $d<0$ or $d>0$. If we focus on $d<0$ then the generators are <u>nearest</u> <u>elements</u> to zero, not colinear.

It follows $d<0$, $\boxed{\text{integers of } \mathbb{Q}(\sqrt{d}) = \{m\alpha+n\beta \mid m,n\in\mathbb{Z}\}}$

Defn/ If the integers of $\mathbb{Q}(\sqrt{d})$ are given by $\{m\alpha+n\beta \mid m,n\in\mathbb{Z}\}$ then α,β forms an <u>integral</u> <u>basis</u> for the integers of $\mathbb{Q}(\sqrt{d})$

Lattice Property of Ideals

When $d<0$, any nonzero ideal in the integers of $\mathbb{Q}(\sqrt{d})$ is a lattice.

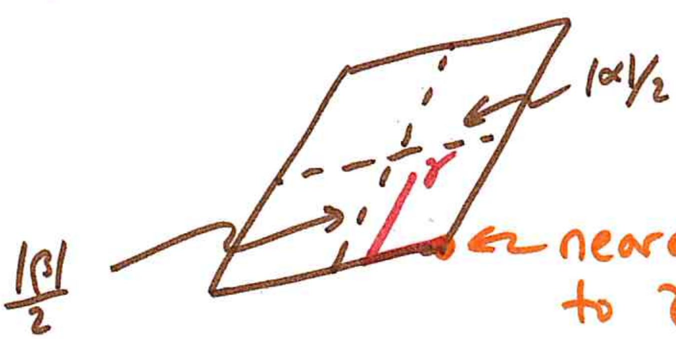
<u>Notation</u>: let the integers of $\mathbb{Q}(\sqrt{d})$ be called L.

<u>Proof</u>: Suppose $I \subseteq L$ is a nonzero ideal. Let $\alpha \in I$ be an element as close as possible to zero ($\alpha \neq 0$). Notice $-\alpha$, $\alpha\sqrt{d}$ are also in I as I is an ideal. Notice

$\measuredangle(\alpha, \alpha\sqrt{d}) = 90°$ as $\sqrt{d} = \sqrt{-d}\, e^{i\pi/2}$

rotates by $\pi/2$ aka $90°$. Thus I includes sums of α & $\alpha\sqrt{d}$ which forms a lattice.

Next, pick $\beta \in I$ as close to zero as possible ($\beta \neq 0$) not in direction of $\mathbb{Z}\alpha$. We claim $I = \{\alpha m + \beta n \mid m, n \in \mathbb{Z}\}$. To see this β to the contrary $\exists \gamma \notin \{\alpha m + \beta n \mid m, n \in \mathbb{Z}\}$ yet $\gamma \in I$ and consider,



$\leftarrow$ nearest point in $\{\alpha m + \beta n \mid m, n \in \mathbb{Z}\}$ to γ say $\alpha m + \beta n$

Notice, then $\gamma - (\alpha m + \beta n) \in I$ and $|\gamma - (\alpha m + \beta n)| < \max(|\alpha|, |\beta|)$ which $\rightarrow\!\leftarrow$ construction of α & β $\therefore$ $I = \{\alpha m + \beta n / m, n \in \mathbb{Z}\}$.

Comments about proof on 15

1.) the proof in Stillwell is careful to only use closure of I under $+$ and $-$. The added closure of I under L-multiplication leads to conclusion $I = (\alpha) + (\beta)$ (which we have seen in practice already) (§11.4 & §11.5)

Thm

Proof:

It is simple to see

$$I = \{\alpha m + \beta n \mid m, n \in \mathbb{Z}\} \subseteq (\alpha) + (\beta)$$

Since $\alpha m \in (\alpha)$ and $\beta n \in (\beta)$ (this is just using $\alpha m = \alpha + \alpha + \dots + \alpha$ m-fold times is again in (α)). Conversely, if I is an ideal then as $\alpha \in I$ it follows $(\alpha) \subseteq I$ and likewise $\beta \in I \Rightarrow (\beta) \subseteq I$ thus $I \supseteq (\alpha) + (\beta)$. In conclusion,

$$I = (\alpha) + (\beta). //$$