2/4/14

HW 1 due NOW

I will hand out HW 2 on Thurs

HW 1 Discussion.

Problem 1.4(b) (Localization of $\mathbb{Z}$):
Classify the intermediate rings

$$\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$$

Solution: Given any subsemigroup $S \subseteq (\mathbb{Z}, \times, 1)$ we can define the localization

$$\mathbb{Z}[S^{-1}] := \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, \ b \in S \right\}.$$

If $0 \notin S$ then we obtain an intermediate ring

$$\mathbb{Z} \subseteq \mathbb{Z}[S^{-1}] \subseteq \mathbb{Q}$$

Conversely, given $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$, I claim that $R = \mathbb{Z}[S^{-1}]$ for some subsemigroup $S \subseteq (\mathbb{Z}, \times, 1)$.

Indeed, let

$$S := \{ b : \tfrac{a}{b} \in R \text{ and } \gcd(a,b) = 1 \}$$

Note that $1 \in S$ because $\frac{a}{1} \in R$ $\forall a \in \mathbb{Z}$.
Also note that if $b \in S$ then $\exists a \in \mathbb{Z}$ such that $\frac{a}{b} \in R$ and $\gcd(a,b) = 1$.
Then Bézout's Lemma says $\exists x, y \in \mathbb{Z}$ such that

$$1 = ax + by.$$

Divide by b to get

$$\frac{1}{b} = \frac{a}{b} \cdot x + y.$$

Since $x, y, \frac{a}{b} \in R$ we conclude that $\frac{1}{b} \in R$.

In summary, $b \in S \Rightarrow \frac{1}{b} \in R$

Thus if $b_1, b_2 \in S$ then

$$\frac{1}{b_1}, \frac{1}{b_2} \in R \Rightarrow \frac{1}{b_1 b_2} \in R \Rightarrow b_1 b_2 \in S$$

We conclude that $S \subseteq (\mathbb{Z}, \times, 1)$ is a subsemigroup and $\mathbb{Z}[S^{-1}]$ is defined.

Note that $R \subseteq \mathbb{Z}[S^{-1}]$ because $\alpha \in R$
$\Longrightarrow \alpha = a/b$ for some $\gcd(a,b) = 1$
$\Longrightarrow b \in S \Longrightarrow a/b \in \mathbb{Z}[S^{-1}]$

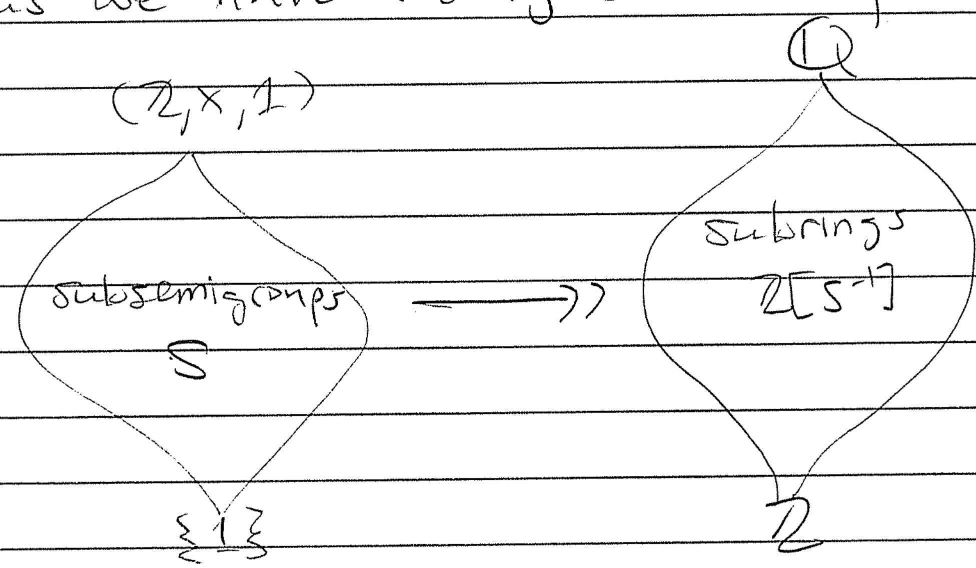
Conversely, consider any $a/b \in \mathbb{Z}[S^{-1}]$, i.e., with $b \in S$. By above remarks we have

$$b \in S \Longrightarrow \frac{1}{b} \in R.$$

and hence $\frac{a}{b} = a\frac{1}{b} \in R$.

We conclude that $R = \mathbb{Z}[S^{-1}]$. ///

Thus we have a surjective map..



However, it is <u>not</u> injective, for example:

$$S = \{2^k : k \in \mathbb{N}\}$$
$$T = \{4^k : k \in \mathbb{N}\}.$$

Then we have $\mathbb{Z}[S^{-1}] = \mathbb{Z}[T^{-1}]$.

<u>Proof</u>: Since $T \subseteq S$ we have $\mathbb{Z}[T^{-1}] \subseteq \mathbb{Z}[S^{-1}]$.

Conversely, consider any $\frac{a}{2^k} \in \mathbb{Z}[S^{-1}]$. Then since 2^k and $a/4^k$ are in $\mathbb{Z}[T^{-1}]$ we have

$$\frac{a}{2^k} = 2^k \cdot \frac{a}{4^k} \in \mathbb{Z}[T^{-1}] \qquad //$$

Given a subsemigroup $S \subseteq (\mathbb{Z}, \times, 1)$, the <u>maximum</u> $T \subseteq (\mathbb{Z}, \times, 1)$ such that $\mathbb{Z}[S^{-1}] = \mathbb{Z}[T^{-1}]$ is defined by

$$T = \{a \in \mathbb{Z} : ab \in S \text{ for some } b \in \mathbb{Z}\}$$

T satisfies the property that

$$ab \in T \implies a \in T \text{ \underline{and} } b \in T.$$

Thus T is generated by a set of primes, i.e., we have

$$T = \{ p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots : e_1, e_2, e_3, \ldots \in \mathbb{N} \}$$

for some set of primes $\{p_1, p_2, p_3, \ldots\}$.

We obtain a bijection between intermediate rings

$$\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$$

and sets of primes $\subseteq \mathbb{Z}$. //

More generally, the same will hold for $D \subseteq R \subseteq \mathrm{Frac}(D)$ whenever D is a PID.

(principal ideal domain)

New Topic: PIDs.

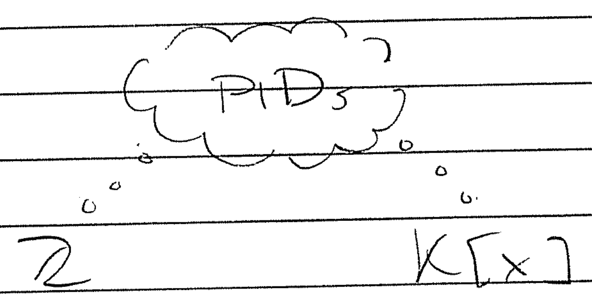
Let R be a ring. Given an element $a \in R$ we define the <u>principal ideal</u> <u>generated</u> by a:

$$(a) := \{ar : r \in R\}$$

<u>Definition</u>: we say R is a <u>principal ideal domain</u> (PID) if

- R is a domain
- Every ideal of R is principal (i.e. generated by one element).

[The purpose of PIDs is to abstract the properties of $\mathbb{Z}$ and $K[x]$.



]

How do we know that $\mathbb{Z}$ and $K[x]$ are PIDs ?

For this we have another definition.

Def : We say that R is a Euclidean domain if.

- R is a domain
- $\exists$ a function $N : R - \{0\} \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$ $\exists\, q, r \in R$ such that
  - $a = qb + r$
  - $N(r) < N(b)$ or $r = 0$.

As you know, $\mathbb{Z}$ and $K[x]$ are Euclidean with.

$$N : \mathbb{Z} - \{0\} \to \mathbb{N} \quad \& \quad N : K[x] - \{0\} \to \mathbb{N}$$
$$a \longmapsto |a| \qquad\qquad f \longmapsto \deg(f).$$

This implies that $\mathbb{Z}$ & $K[x]$ are PIDs because

Theorem: Every Euclidean domain is a PID.

Proof: Let R be Euclidean with norm $N: R-\{0\} \to \mathbb{N}$. Let $I \leq R$ be any ideal.

If $I=(0)$ then we're done.

So suppose that $I \neq (0)$. Then by well ordering there exists $0 \neq b \in I$ such that $N(b)$ is minimum.

I claim that $I=(b)$. Indeed, since $b \in I$ and I is an ideal we have $(b) \subseteq I$. We want $I \subseteq (b)$. So take any $a \in I$ and divide by b $(\neq 0)$ to get

$$a = qb + r \quad \text{with } r=0 \text{ or } N(r) < N(b).$$

But $r = a - qb \in I \implies N(r) \not< N(b)$
$\implies r=0 \implies a \in (b)$ as desired.

$\blacksquare$

The language of PID is very elegant:

Let R be a PID. Then $\forall u \in R$ we have

$$u \text{ is a unit} \iff (u) = R.$$

Proof: If u^{-1} exists then $1 = uu^{-1} \in (u)$ implies that $a = a1 \in (u)$ for all $a \in R$. Hence $(u) = R$. Conversely, if $(u) = R$ then since $1 \in R = (u)$, $\exists\, v \in R$ such that $uv = 1$. Hence u is a unit. ///

[We say R is the "unit ideal".]

For all $a, b \in R$ we have

$$a \text{ divides } b \iff (b) \subseteq (a)$$

Proof: If $b = ar$ for some $r \in R$ then $b \in (a)$, hence $(b) \subseteq (a)$. Conversely if $(b) \subseteq (a)$ then $b \in (a)$, hence $b = ar$ for some $r \in R$. ///

For all $a, b \in R$ we have

$$a, b \text{ are associate} \iff (a) = (b).$$

Proof: If $a = bu$ for unit $u \in R^\times$ then
$a = bu \implies a \in (b) \implies (a) \subseteq (b)$ and
$b = au^{-1} \implies b \in (a) \implies (b) \subseteq (a)$.
Conversely, suppose that $(a) = (b)$.
Then $\exists\, x, y \in R$ such that

$$a = bx \quad \text{and} \quad b = ay.$$

Hence $a = bx = ayx$
$a(1 - yx) = 0$.

If $a \neq 0$ then since R is a domain
we get $1 - yx = 0 \implies yx = 1$
$\implies a, b$ are associate. //

Recall: We say a is a proper divisor of b if $a | b$ and also

- a is not associate to b
- a is not a unit (i.e. not associate to 1)

We can rephrase this by saying

a is a proper divisor of b $\iff$ $(b) < (a) < (1)$.

<u>Def</u>: We say $a \in R$ is <u>irreducible</u> if it has no proper divisors.

Equivalently, (a) is maximal among principal ideals of R.

Since R is a PID we can just say

$a \in R$ is irreducible $\iff$ $(a) \leq R$ is maximal

Similarly, we define <u>prime</u> elements by saying that

$p \in R$ is prime $\iff$ $(p) \leq R$ is prime.

i.e. if $ab \in (p)$ (i.e. $p \mid ab$) then

$a \in (p)$ (i.e. $p \mid a$) or $b \in (p)$ (i.e. $p \mid b$).

Theorem: Let $p \in R$ in a domain. Then

$$p \text{ is prime} \implies p \text{ is irreducible}$$

Proof: Suppose that $p = ab$ where a & b are nonunits. Since $p \mid ab$ we have $p \mid a$ or $p \mid b$. WLOG assume that $p \mid a$. But then we have $a \mid p$ and $p \mid a$
$\implies$ a and p are associate
$\implies$ b is a unit.
Contradiction. ///

In general, irreducible $\not\Longrightarrow$ prime. But:

Theorem: Let $a \in R$ in a PID. Then

$$a \text{ is irreducible} \iff a \text{ is prime}.$$

Proof: We already saw $\Leftarrow$
To prove $\Rightarrow$ note that

$$\begin{aligned} a \text{ irreducible} &\overset{PID}{\Longrightarrow} (a) \text{ maximal} \\ &\Longrightarrow (a) \text{ prime} \\ &\Longrightarrow a \text{ prime}. \end{aligned}$$

///

2/6/14

HW 2 due Thurs Feb 20.

Recall:

PID

$\mathbb{Z}$ $\qquad$ $K[x]$

Let R be a domain. We say R is Euclidean if it has a "size" function $N : R - 0 \to \mathbb{N}$ such that $\forall\, a, b \in R$ $\exists\, q, r$ such that

- $a = qb + r$
- $r = 0$ or $N(r) < N(b)$

[Remark: The quotient and remainder are not necessarily unique. For example consider $N : \mathbb{Z} - 0 \to \mathbb{N}$ defined by $N(a) = |a|$. Then we have

$$9 = 2 \cdot 4 + 1 \quad \text{with} \quad |1| < |4|$$
$$9 = 3 \cdot 4 - 3 \quad \text{with} \quad |-3| < |4|.$$
]

The language of Euclidean domains is a bit weird so we have a better idea:

We say R is a PID if every ideal $I \leq R$ generated by a single element, i.e, if

$$I = (a) = \{ar : r \in R\}$$

for some $a \in R$.

Theorem: Euclidean $\implies$ PID.

Proof: Use the fact that $\mathbb{N}$ is well-ordered. //

The language of PIDs is very nice:

We have

- $u \in R$ is a unit $\iff (u) = R$
- $a, b \in R$ are associate $\iff (a) = (b)$
- $a \mid b \iff (b) \leq (a)$.
- a is a proper divisor of b $\iff (b) < (a) < 1$.
- a is irreducible $\iff (a)$ is maximal

- a is prime $\iff$ (a) is prime.

Thus in a PID there is no difference between prime and maximal ideals.

Theorem: Consider an ideal $I \leq R$ in a PID. Then we have

$$I \text{ is maximal} \iff I \text{ is prime}$$

Proof: $\Longrightarrow$ is true in any ring.

To prove $\Longleftarrow$ let I be prime. Since R is a PID we have $I = (p)$ for some $p \in R$. Now suppose we have

$$(p) \leq (a) < (1)$$

for some ideal (a). Since $p \in (a)$ we have $p = ab$ for some $b \in R$, i.e., $ab \in (p)$. Then since (p) is prime we have

$$a \in (p) \quad \text{OR} \quad b \in (p).$$

If $a \in (p)$ then we have $(a) = (p)$, hence (p) is maximal, so suppose that $b \in (p)$, i.e., $b = pc$ for some $c \in R$.

But then $p = ab = apc$

$$\Longrightarrow p(1-ac) = 0$$
$$\Longrightarrow 1 - ac = 0$$
$$\Longrightarrow ac = 1.$$
$\Longrightarrow$ a is a unit.

This contradicts the fact that $(a) < (1)$. ///

In other words: Given $a \in R$ in a PID we have

a is irreducible $\Longleftrightarrow$ a is prime ///

Recall: The result for $n \in \mathbb{Z}$ that says

n is irreducible $\Longrightarrow$ n is prime

is called "Euclid's Lemma".
Remember what it's for?

Definition: Let R be a domain. We say that R is a unique factorization domain (UFD) if:

- Every $a \in R$ can be written as a product of irreducibles, times a unit
- The factorization is unique up to reordering irreducibles and multiplying by units.

Now consider $a \in R$ in a PID and suppose we have two factorizations into irreducibles

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

Since $p_1 \mid q_1 q_2 \cdots q_l$ and p_1 is prime we have $p_1 \mid q_i$ for some i. WLOG assume $p_1 \mid q_1$, i.e., $(q_1) \subseteq (p_1)$. Then since (q_1) is maximal we have $(q_1) = (p_1)$, i.e.,

$$q_1 = p_1 u \text{ for some unit } u \in R.$$

Since R is a domain we can cancel p_1 from both sides to get

$$p_2 p_3 \cdots p_k = u\, q_2 q_3 \cdots q_\ell$$

Repeat the argument to get a bijection between $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$. Thus $k = \ell$ and the factorization is unique. ///

But the question remains:

Does $a \in R$ have *any* factorization into irreducibles?

In $\mathbb{Z}$ or $K[x]$ we would use induction on size to prove this

[Example: Consider $n \in \mathbb{Z}$. If n is not irreducible $\exists\ a, b \in \mathbb{Z}$ with

$$n = ab$$

and $1 < |a|, |b| < |n|$. By induction a and b are products of irreducibles. Hence so is n.]

But a general PID doesn't have a size function. Are we stuck?

No. We simply generalize the idea of induction...

Let R be a general ring. For any set $S \subseteq R$ we define the ideal *generated* by S:

$$\langle S \rangle := \bigcap \{ \text{ideals } I \leq R : S \subseteq I \}$$

This is an ideal containing S. In fact, it is the smallest ideal containing S. Indeed, suppose $J \leq R$ is an ideal with $S \subseteq J$. Then we have

$$\langle S \rangle = J \cap \bigcap \{ \text{ideals } I \leq R : S \subseteq I, \; I \neq J \}$$

$$\Longrightarrow \langle S \rangle \leq J$$

///

Definition: We say that an ideal $I \leq R$ is *finitely generated* if we have

$$I = \langle S \rangle$$

for some *finite* $S \subseteq R$.

<u>Theorem</u>: Let R be a ring. TFAE:

① Every ideal of R is finitely generated.

② Every increasing chain of ideals stabilized. That is, given ideals

$$I_1 \leq I_2 \leq I_3 \leq \cdots$$

$\exists\, k$ such that $I_k = I_{k+1} = \cdots$

<u>Proof</u>: ① $\Longrightarrow$ ②
Suppose every ideal is f.g and consider a chain of ideals

$$I_1 \leq I_2 \leq I_3 \leq \cdots$$

Define the set $I := \bigcup_{k=1}^{\infty} I_k \subseteq R$.

Claim: I is an ideal. Indeed, given $a, b \in I$ $\exists\, k$ such that $a, b \in I_k$. Then we have $a+b \in I_k \leq I$ and for all $c \in R$ we have $ac \in I_k \subseteq I$. ///

Since I is f.g. we have $I = \langle \{a_1, \ldots, a_m\} \rangle$ for some $a_1, \ldots, a_m \in R$

But then $\exists\, k_1, \dots, k_m$ such that $a_i \in I_{k_i}$ for all i. If $k = \max\{k_1, \dots, k_m\}$ then we have $\{a_1, \dots, a_m\} \subseteq I_k$ and hence

$$I_k = I_{k+1} = \cdots = I$$

///

(2) $\Rightarrow$ (1)

Suppose every increasing chain stabilizes and let I be an ideal. Choose any $a_1 \in I$. Then

$$(a_1) \neq I$$

so we can choose $a_2 \in I - (a_1)$ such that

$$(a_1) < (a_1, a_2) \neq I.$$

Continuing in this way we obtain an infinite increasing chain of ideals. Contradiction

///

Definition: A ring satisfying either of these equivalent conditions is called

NOETHERIAN.

Named after Emmy Noether, "Idealtheorie in Ringbereichen", 1921.

Noetherian rings are nice because we can use inductive arguments

Theorem: Let R be noetherian. Then every $a \in R$ can be written as a product of irreducibles.

Proof: If a is irreducible we're done. Otherwise we can write

$$a = a_1 b_1$$

with $(a) < (a_1), (b_1) < (1)$. If a_1 & b_1 are irreducible we're done. Otherwise WLOG we can write

$$a_1 = a_2 b_2$$

with $(a_1) < (a_2), (b_2) < (1)$. This process must terminate otherwise we obtain an infinite increasing chain

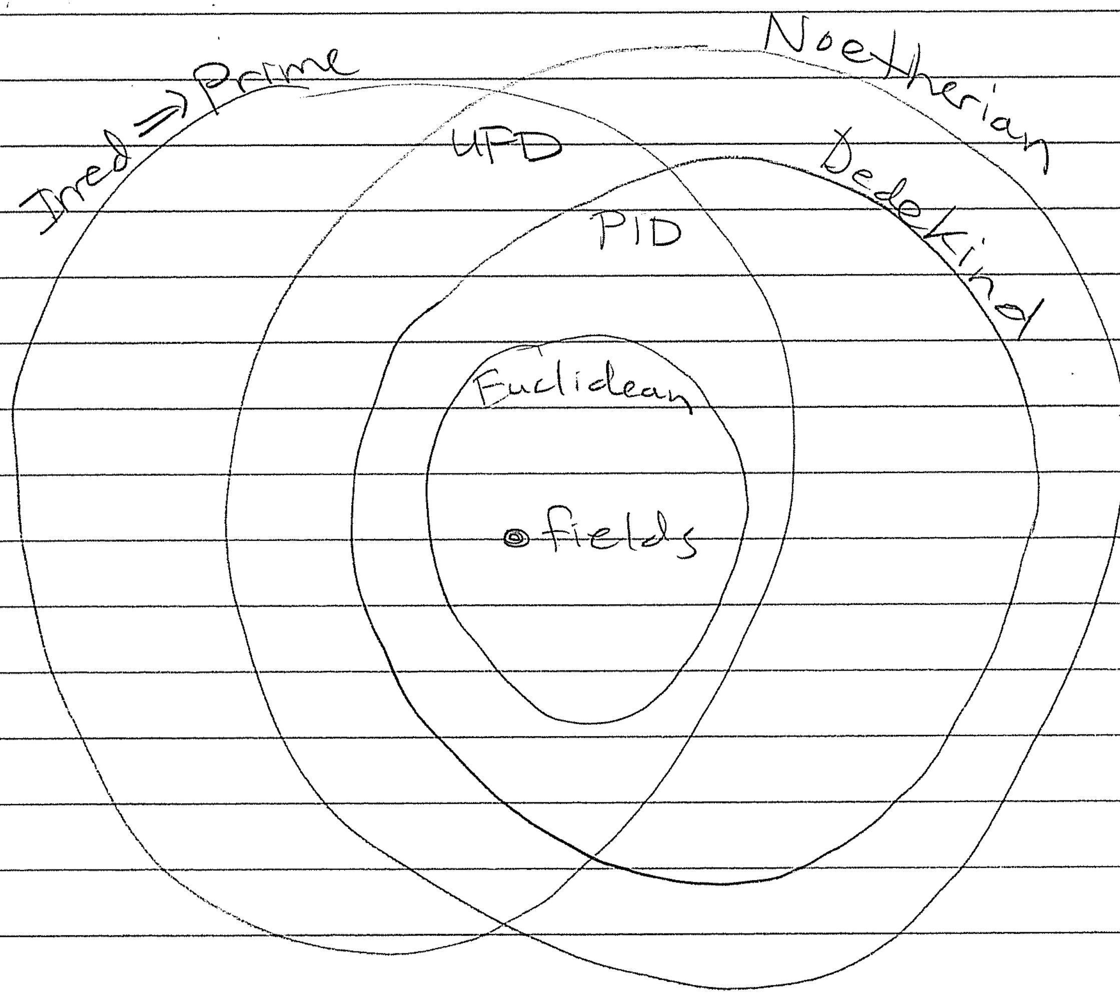
$$(a) < (a_1) < (a_2) < \cdots$$

///

Corollary: PID $\Rightarrow$ UFD.

Proof: Clearly a PID is noetherian (every ideal is very finitely generated). Thus every element has a factorization into irreducibles. Then since irreducible $\Rightarrow$ prime in a PID we get uniqueness. ☒

Picture:



2/11/14

HW 2 due Thurs Feb 20
McKnight - Zame Lecture Wed 5:30pm
in Wesley Gallery (Dusa McDuff).

Last time we proved

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD.

This week we will discuss:

"Who cares about unique factorization?"

This will involve a deep analogy between number theory and complex analysis. We will tread lightly. :)

(1) Complex Analysis

Consider the function $y = \sqrt{x}$ for complex $x \in \mathbb{C}$. It is not really a function because $\sqrt{x}$ has two values for all $x \in \mathbb{C}$.

Specifically, let $x = re^{i\theta}$ with $r \geq 0$
Then since $x = re^{i\theta} e^{2\pi i k}$ for all $k \in \mathbb{Z}$
we have

$$\sqrt{x} = \sqrt{r}\, e^{i\theta/2} e^{i\pi k} \quad \text{for all } k \in \mathbb{Z}$$

$$= \underset{(k \text{ even})}{\sqrt{r}\, e^{i\theta/2}} \quad \text{OR} \quad \underset{(k \text{ odd})}{-\sqrt{r}\, e^{i\theta/2}}$$

where $\sqrt{r} \geq 0$ is uniquely defined

Thus $\sqrt{x}$ does not define a nice function $\mathbb{C} \to \mathbb{C}$. Riemann fixed this by defining $\sqrt{x}$ as a nice function on a <u>new</u> domain $S \to \mathbb{C}$.

<u>Def</u>: Consider the polynomial

$$f(x,y) = y^2 - x \in \mathbb{C}[x,y]$$

and define the zero set

$$S := \{ (\alpha,\beta) \in \mathbb{C}^2 : f(\alpha,\beta) = 0 \} \subseteq \mathbb{C}^2$$

This is a real 2-dim surface in real 4-dim space $\mathbb{C}^2 = \mathbb{R}^4$.

The equation of the tangent plane at $(\ , \ ) \in S$ is

$$f_x(\alpha,\beta)(x-\alpha) + f_y(\alpha,\beta)(y-\beta) = 0$$

where $f_x(x,y) = -1$
$f_y(x,y) = 2y$

If $f_y(\alpha,\beta) = 2\beta \neq 0$ (i.e. if $\beta \neq 0$) then we can express y as a function of x near (a,b):

$$y \approx \frac{f_x(\alpha,\beta)}{f_y(\alpha,\beta)}(x-\alpha) + \beta.$$

In other words, the projection map

$$\begin{aligned} \pi : S &\longrightarrow \mathbb{C} \\ (\alpha,\beta) &\longmapsto \beta \end{aligned}$$

is a nice function except possibly at $\beta = 0$, where

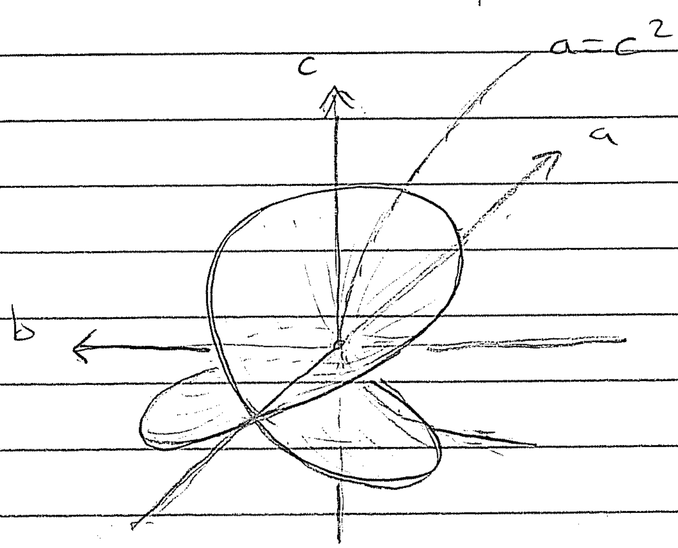
"nice" = isomorphism on small neighborhoods

Q: What does S look like?

Let $x = a + ib$ & $y = c + id$ for $a, b, c, d \in \mathbb{R}$. Then $y^2 = x$ is equivalent to two equations

$$a = c^2 - d^2$$
$$b = 2cd.$$

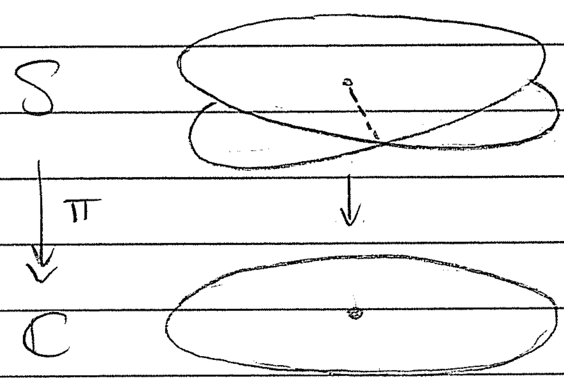
Think of d as "time" and plot this in 3-dim (a,b,c)-space.



(a,b)-plane $=$ x-axis
At time $d = 0$ we get $b = 0$ and $a = c^2$ (parabola).

[The self-intersection on neg. a-axis is not really there in 4D.]

Maybe it's better just to draw this schematically. Let $U \subseteq \mathbb{C}$ be the unit disk and consider the preimage $\pi^{-1}(U)$ above it:



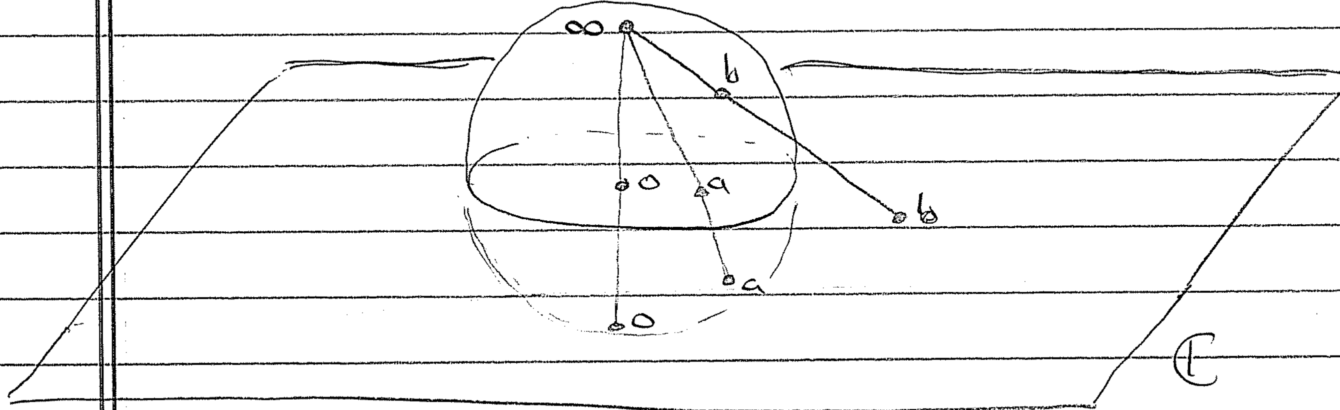
Note: The self intersection in S is not really there.

This is a 2:1 topological covering map except at $0 \in \mathbb{C}$. (we say it is "ramified" or "branched" over 0).

Q: What does S look like globally?

Using stereographic projection we identify the (Riemann) sphere with the extended complex plane

$$\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}.$$



south pole $= 0$
north pole $= \infty$
south hemisphere $= \{ z \in \mathbb{C} : |z| < 1 \}$
north hemisphere $= \{ z \in \mathbb{C} : |z| > 1 \}$.

Note that $z \mapsto 1/z$ is rotation by $180°$ around the real axis.

$$0 \mapsto 1/0 = \infty, \quad \infty \mapsto 1/\infty = 0$$

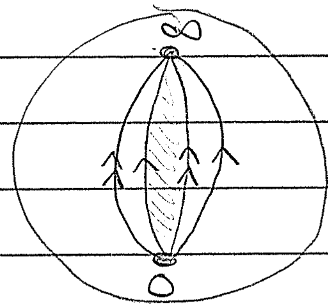
Near ∞ the surface S looks like

$$\left(\frac{1}{y}\right)^2 = \frac{1}{x}$$

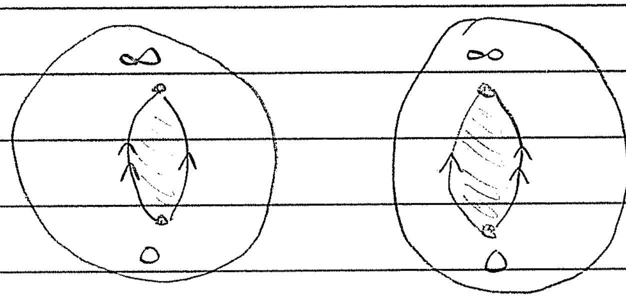
$$\frac{1}{y^2} = \frac{1}{x}$$

$$x = y^2 \quad (\text{same}).$$

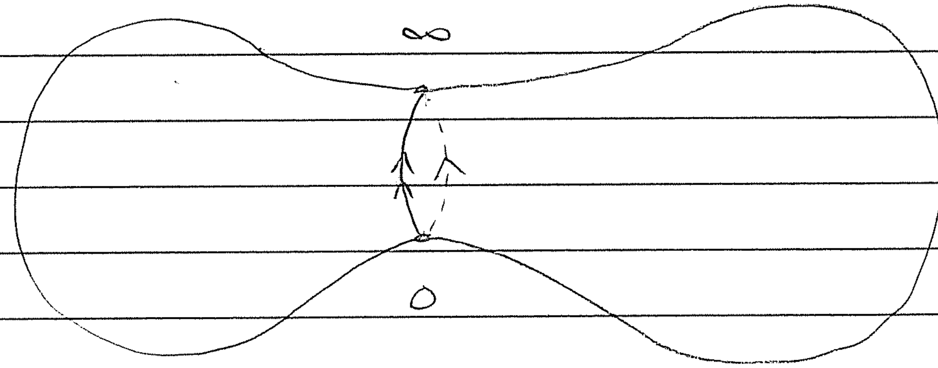
So $S \xrightarrow{\pi} \hat{\mathbb{C}}$ is a two-sheeted cover branched at 0 and ∞. Cut it open:



Take it apart:



Put it back together:



So S is topologically a sphere. The square root function is the projection map.

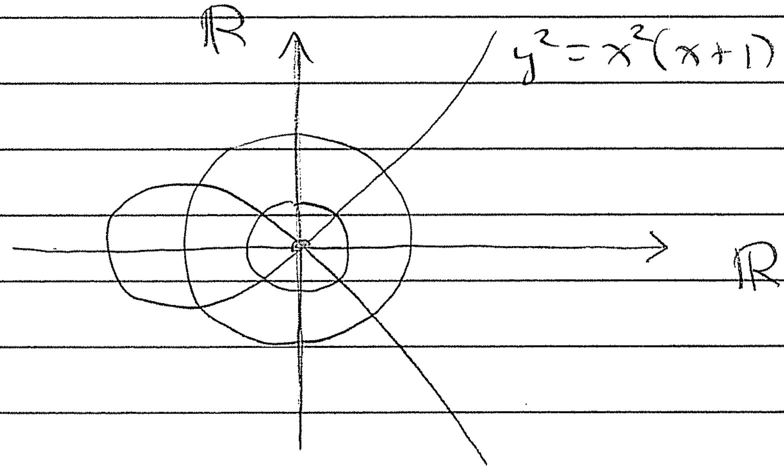
$$\begin{array}{ccc} \text{sphere} & & \text{sphere} \\ \pi : S & \longrightarrow & \hat{\mathbb{C}} \\ (a,b) & \longmapsto & b \end{array} \quad \left(\text{formula valid away from } \infty\right)$$

Another example: Consider the Riemann surface defined by

$$y^2 = x^2(x+1),$$

$$S := \{ (\alpha, \beta) \in \mathbb{C}^2 : \beta^2 = \alpha^2(\alpha+1) \} \subseteq \mathbb{C}^2$$

The real locus looks like:

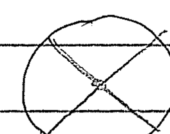


Near $(0,0)$ the curve has a power series expansion:

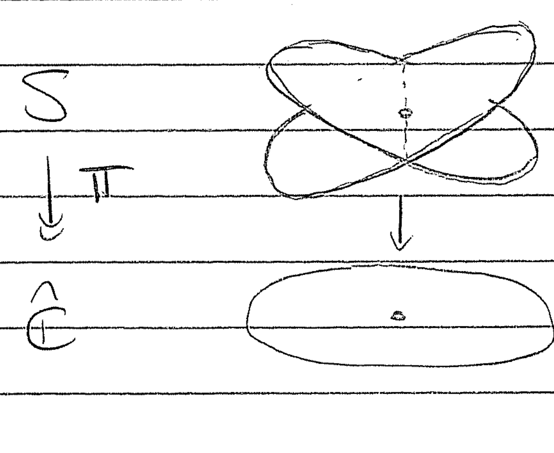
$$y = \pm x\sqrt{x+1}$$

$$y \approx \pm x\left(1 + \binom{1/2}{1}x + \binom{1/2}{2}x^2 + \binom{1/2}{3}x^3 + \cdots\right)$$

$$y \approx \pm x \quad \text{for } |x| \text{ small.}$$

This is a union of two lines. 
(only valid inside the radius of convergence $|x| < 1$.)

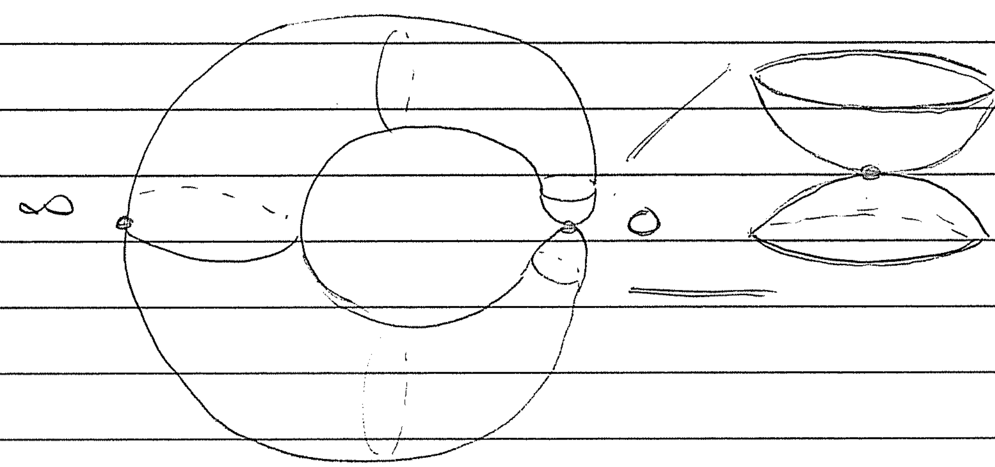
As before, the projection $\pi : S \to \hat{\mathbb{C}}$ defined by $(\alpha, \beta) \mapsto \beta$ expresses y as a function of x with domain S (possibly minus a finite number of bad points). Over the unit disk $U \subseteq \hat{\mathbb{C}}$ we have



Two flat disks meeting only at their center (Can you imagine such a thing?).

[Recall: Two 2-planes in $\mathbb{R}^4$ can meet at a single point. For example, the (a,b)-plane and (c,d) plane in real 4D (a,b,c,d)-space.]

Topologically, the surface $S \subseteq \hat{\mathbb{C}}^2$ looks like



Again, the point $(\alpha, \beta) \in S$ has tangent plane

$$f_x(\alpha,\beta)(x-\alpha) + f_y(\alpha,\beta)(y-\beta) = 0$$

where $f_x = \frac{d}{dx}\left(y^2 - x^2(x+1)\right)$

$$= -3x^2 - 2x$$

$$= -x(3x+2)$$

and $f_y(x,y) = \frac{d}{dy}\left(y^2 - x^2(x+1)\right) = 2y$.

We say that the point $(0,0) \in S$ is <u>singular</u> because

$$f_x(0,0) = 0 = f_y(0,0).$$

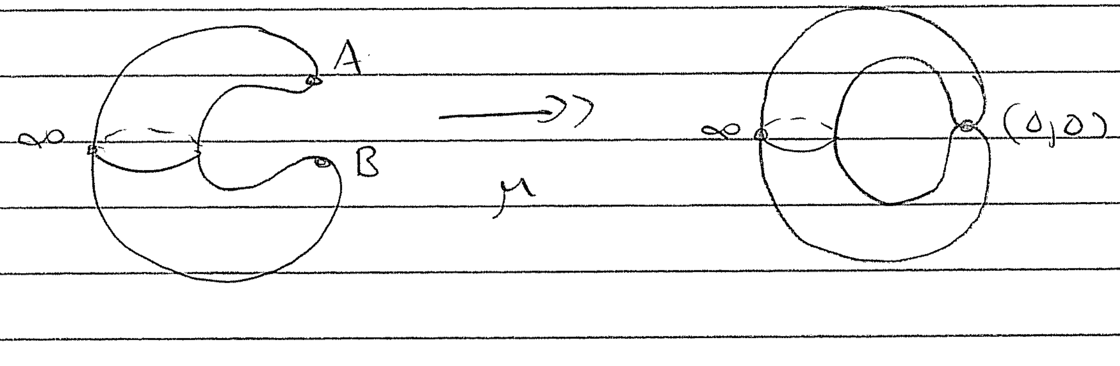
(The tangent plane at $(0,0)$ is "too big".)

I'll end with a Problem:

Find a nonsingular Riemann surface S' and a map

$$\mu : S' \twoheadrightarrow S$$

that is locally an isomorphism, but separates $(0,0) \in S$ into two nonsingular points A & B.



Theorem:

This can always be done. There is a unique such nonsingular $S' \to S$ and it can be constructed by taking the integral closure of a certain domain in its field of fractions.

Wait, what ?!

2/13/14

HW 2 due Thurs Feb 20.

Right now we are discussing:

"Who cares about unique factorization?"

The concept of UFD is motivated by a deep analogy between

(1) Complex Analysis
(2) Algebraic Number Theory

Last time we discussed (1).

(2) Number Theory

Conjecture (Fermat, 1637):

Consider $n \in \mathbb{Z}$, $n \geq 3$. Then for all $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ we have

$$x^n + y^n \neq z^n$$

[The theorem is false when $n = 2$:

$$3^2 + 4^2 = 5^2, \text{ etc.}$$]

In 1847 Lamé gave a proof, but he incorrectly assumed that the ring of cyclotomic integers

$$\mathbb{Z}[\omega_n] := \{a_0 + a_1\omega_n + a_2\omega_n^2 + \cdots + a_{n-1}\omega_n^{n-1} : a_i \in \mathbb{Z}\},$$

where $\omega_n = e^{2\pi i/n}$, is a UFD. In fact, Kummer had shown in 1844 that

$$\mathbb{Z}[\omega_{23}] \text{ is not a UFD.}$$

To prove this is hard, so here is an easier example of a non-UFD.

Consider the ring

$$\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$$

This is a domain with a multiplicative norm inherited from $\mathbb{C}$.

$$\begin{aligned} N(a+b\sqrt{-3}) &= |a + b\sqrt{-3}| \\ &= (a+b\sqrt{-3})(a-b\sqrt{-3}) \\ &= a^2 + 3b^2. \end{aligned}$$

[Warning: We will see that N is not a Euclidean norm.]

Since $N(\alpha\beta) = N(\alpha)N(\beta)$ we have the following

Proposition: Given $\alpha \in \mathbb{Z}[\sqrt{-3}]$ we have

$$\alpha \text{ is a unit} \iff N(\alpha) = 1.$$

Proof: If α is a unit then

$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}).$$

Then since $N(\alpha), N(\alpha^{-1}) \in \mathbb{N}$ we conclude that $N(\alpha) = 1$.

Conversely, suppose that $N(\alpha) = \alpha\bar{\alpha} = 1$. Then $\alpha^{-1} = \bar{\alpha}$, hence α is a unit. //

We can use this prop. to compute the units of $\mathbb{Z}[\sqrt{-3}]$.

Given $\alpha = a + b\sqrt{-3}$ suppose we have

$$N(\alpha) = a^2 + 3b^2 = 1.$$

This implies $b = 0$ (otherwise $N(\alpha) \geq 3$) and hence $a^2 + 3 \cdot 0 = 1$, or $a = \pm 1$. We conclude that

$$\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}.$$

By similar reasoning we can show that

__Lemma:__ $N(\alpha) \neq 2 \quad \forall \alpha \in \mathbb{Z}[\sqrt{-3}]$

__Proof:__ If $N(\alpha) = a^2 + 3b^2 = 2$ then we must have $b = 0$ (otherwise $N(\alpha) \geq 3$), hence $a^2 + 3 \cdot 0 = 2$.

But $a^2 = 2$ is impossible (Pythagoras).

//

__Corollary:__ Given $\alpha \in \mathbb{Z}[\sqrt{-3}]$.

If $N(\alpha) = 4$ then α is __irreducible__.

Proof: Let $N(\alpha) = 4$ and suppose for contradiction that α is reducible, say

$\alpha = \beta\gamma$ with β, γ nonunits.

Then $N(\beta)N(\gamma) = N(\alpha) = 4$ implies that

$$N(\beta) = N(\gamma) = 2$$

This is impossible. //

Theorem: $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Proof: Note that we have

$$2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{-3})$$

where $2, 1 \pm \sqrt{-3}$ are irreducible because $N(2) = N(1 \pm \sqrt{-3}) = 4$.

However, 2 is not associate to $1 \pm \sqrt{-3}$ because the units of $\mathbb{Z}[\sqrt{-3}]$ are just ± 1.

$\blacksquare$

[In other words, 2 is irreducible but not prime.]

Can we fix this? i.e, Can we recover unique factorization by adding some new elements?

Yes. (We need a definition.)

Def: Given a domain D we say that D is "integrally closed" or "normal" if given monic polynomial $f(x) \in D[x]$ and rational roof $f(a/b) = 0$ (here $a/b \in \text{Frac}(D)$) it follows that $a/b \in D$, i.e, $b \mid a$.

Theorem: UFD $\Rightarrow$ Normal

Proof: Let D be UFD and consider any monic polynomial

$$f(x) = ux^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in D[x]$$

i.e. with $u \in D^\times$. Let $\alpha \in \text{Frac}(D)$ satisfy $f(\alpha) = 0$.

Since D is UFD we can cancel common primes in numerator/denominator to get $\alpha = a/b$ with a, b coprime. Then

$$0 = u\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0.$$

Multiply by $u^{-1}b^n$ to get

$$\begin{aligned} a^n &= -u^{-1}c_{n-1}a^{n-1}b - \cdots - c_1 a b^{n-1} - c_0 b^n \\ &= b(\text{something}). \end{aligned}$$

Thus $b \mid a^n$. Since a, b have no common prime factor this means b is a unit.

$\Longrightarrow a/b \in D$. ∎

This suggests we should define the "normalization" of a domain.

Def: Let D be a domain and define the "integral closure" or "normalization"

$$\bar{D} := \left\{ \frac{a}{b} \in \mathrm{Frac}(D) : f\left(\frac{a}{b}\right) = 0 \text{ for some monic } f(x) \in D[x] \right\}$$

Hope:

If D is not UFD, maybe $\bar{D}$ is UFD?

Compute the normalization of $\mathbb{Z}[\sqrt{-3}]$:

Given $a+b\sqrt{-3}$, $c+d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ we have

$$\frac{a+b\sqrt{-3}}{c+d\sqrt{-3}} = \frac{a+b\sqrt{-3}}{c+d\sqrt{-3}}\left(\frac{c-d\sqrt{-3}}{c-d\sqrt{-3}}\right)$$

$$= \frac{(ac+3bd)+(bc-ad)\sqrt{-3}}{c^2+3d^2}$$

$$= \left(\frac{ac+3bd}{c^2+3d^2}\right) + \left(\frac{bc-ad}{c^2+3d^2}\right)\sqrt{-3}.$$

$\Longrightarrow \mathrm{Frac}(\mathbb{Z}[\sqrt{-3}]) \subseteq \{ r+s\sqrt{-3} : r,s \in \mathbb{Q} \}$

Now given any $\alpha = r+s\sqrt{-3} \in \mathrm{Frac}(\mathbb{Z}[\sqrt{-3}])$ we have

$$(x-\alpha)(x-\bar{\alpha}) = x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$$
$$= x^2-2rx+(r^2+3s^2).$$

Thus if $2r,\ r^2+3s^2 \in \mathbb{Z}[\sqrt{-3}]$ we conclude that α is integral over $\mathbb{Z}[\sqrt{-3}]$

Note: $2r \in \mathbb{Z}[\sqrt{-3}] \Rightarrow 2r \in \mathbb{Z} \Rightarrow r = a/2$.

Then $r^2 + 3s^2 = a^2/4 + 3s^2 \in \mathbb{Z}[\sqrt{-3}]$

$\Longrightarrow a^2/4 + 3s^2 \in \mathbb{Z} \Longrightarrow a^2 + 4\cdot 3s^2 \in \mathbb{Z}$.

$\Longrightarrow 4\cdot 3s^2 \in \mathbb{Z} \Longrightarrow 3(2s)^2 \in \mathbb{Z}$

$\Longrightarrow 2s \in \mathbb{Z}$

(if not then $2s = A/B$ and $3A^2/B^2 \in \mathbb{Z}$. Since A, B coprime this implies $B^2 \mid 3$, contradiction.)

$\Longrightarrow s = b/2$.

We conclude that $\frac{a}{2} + \frac{b}{2}\sqrt{-3}$ are integral over $\mathbb{Z}[\sqrt{-3}]$. In fact, one can show that

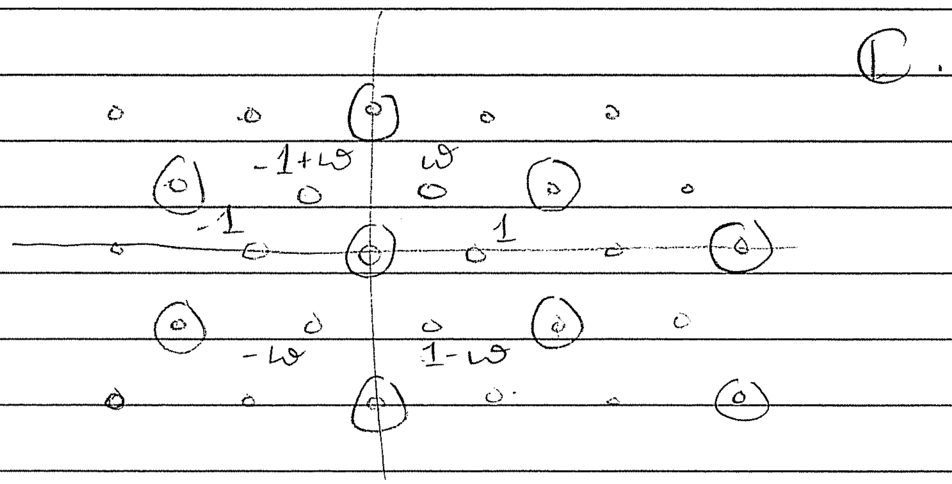
$$\overline{\mathbb{Z}[\sqrt{-3}]} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

<u>Theorem</u>: $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ <u>is</u> UFD.

Proof: Note that

$$\omega := e^{2\pi i/6} = \cos(2\pi/6) + i\sin(2\pi/6)$$
$$= \frac{1}{2} + i\frac{\sqrt{3}}{2}$$
$$= (1+\sqrt{-3})/2.$$

The numbers $\mathbb{Z}[\omega]$, called Eisenstein integers, form a nice triangular lattice

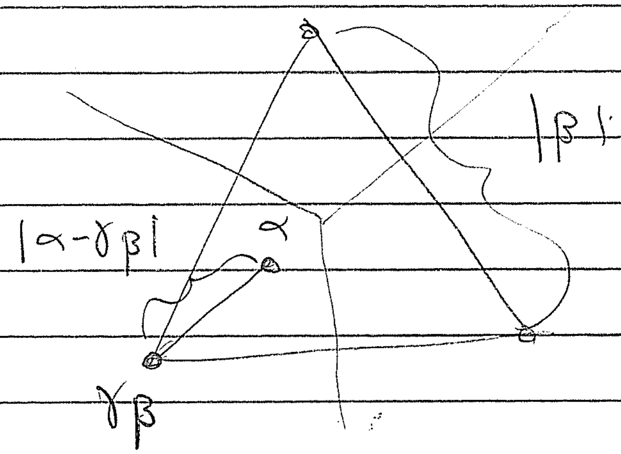


We will do division with remainder: Consider $\alpha, \beta \in \mathbb{Z}[\omega]$ with $\beta \neq 0$ and consider the principal ideal (β).

Note: (β) is a nice triangular sublattice of $\mathbb{Z}[\omega]$. (e.g. $\beta = 1+\omega$, the circled vertices above)

To divide α by β try to find $\mu \in (\beta)$ such that $|\alpha - \mu| < |\beta|$.

Easy: α must fall in some triangle of (β).



Clearly $|\alpha - \gamma\beta| < |\beta|$. Let $\rho := \alpha - \gamma\beta$. Then we have

- $\alpha = \gamma\beta + \rho$
- $\rho = 0$ or $|\rho| < |\beta|$.

Hence $\mathbb{Z}[\omega]$ is

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD.

[Now the two factorizations

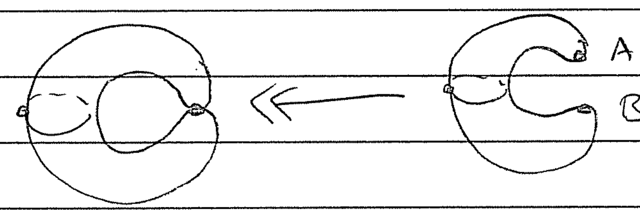
$$2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{-3})$$

are the same because 2 is associate to $1 \pm \sqrt{-3}$ in $\mathbb{Z}[\omega]$.]

Punchline: I claim that the normalization

$$\mathbb{Z}[\sqrt{-3}] \hookrightarrow \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

is directly analogous to the resolution of singularities



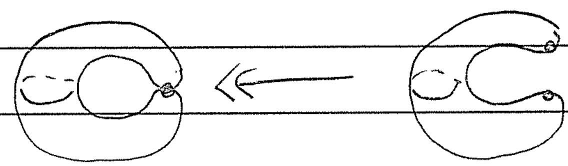
[This week I made a mess. Don't worry; I intend to clean it up.]

2/18/14

HW 2 due this Thurs.

Last week I mentioned an analogy

$$\boxed{\mathbb{Z}[\sqrt{-3}] \hookrightarrow \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]}$$



UFD $\approx$ Nonsingular

Let me try to explain:

Given polynomial $F(x,y) \in \mathbb{C}[x,y]$ we define the "Riemann surface"

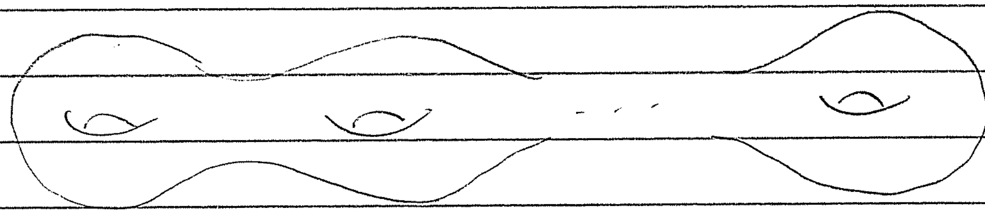
$$S := \{ (\alpha,\beta) \in \mathbb{C}^2 : F(\alpha,\beta) = 0 \} \subseteq \mathbb{C}^2$$

To study S, Klein's Philosophy says we should find a group acting transitively $G \curvearrowright S$ and replace

S by G/stab.

But this won't work.

If $F(x,y)$ is irreducible then S is topologically equivalent to some genus g surface



g holes

possibly with singularities. Then

<u>Theorem</u> (Hurwitz, 1893):

If $g \geq 2$ then the automorphism group is finite. In particular

$$|\mathrm{Aut}(S)| \leq 84(g-1)$$

For example, "Klein's quartic curve" $F(x,y) = x^3y + y^3 + x$ has $g=3$ and achieves the bound:

$$|\mathrm{Aut}(S)| = 84(3-1) = 168$$

This $\mathrm{Aut}(S) \cong PSL(2,7)$ is the second-smallest simple group.

So Klein's Philosophy fails ///

Grothendieck's Philosophy says to look instead at the ring of nice (i.e. polynomial) functions $S \to \mathbb{C}$

$$\mathbb{C}[S] = \{\text{polynomial functions } S \to \mathbb{C}\}.$$

We say a function $\varphi : S \to \mathbb{C}$ is "polynomial" if it comes from some $\Phi(x,y) \in \mathbb{C}[x,y]$, i.e., if:

$$\begin{array}{ccc} \mathbb{C}^2 & \xrightarrow{\Phi} & \mathbb{C} \\ \uparrow & & \| \\ S & \xrightarrow{\varphi} & \mathbb{C} \end{array}$$

Given two $f, g : \mathbb{C}^2 \to \mathbb{C}$ when do they determine the same function $S \to \mathbb{C}$?

We consider the restriction map from $\mathbb{C}^2$ to S

$$\text{res} : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[S]$$

This map is surjective by definition. The kernel is called the vanishing ideal

$$I(S) := \{ f \in \mathbb{C}[x,y] : f(\alpha,\beta) = 0 \ \forall (\alpha,\beta) \in S \}.$$

Hence we have

$$\mathbb{C}[S] \approx \mathbb{C}[x,y] / I(S).$$

This is called the coordinate ring of S.

Given any point $p \in S$ we have an evalation function

$$\begin{aligned} ev_p : \mathbb{C}[S] &\longrightarrow \mathbb{C} \\ f &\longmapsto f(p) \end{aligned}$$

This function is clearly surjective (let f be any constant function) hence we have

$$\mathbb{C}[S]/m_p \approx \mathbb{C}, \quad \text{where}$$

$$m_p = \{ f \in \mathbb{C}[S] : f(p) = 0 \}$$

is a maximal ideal of $\mathbb{C}[S]$.
We will see later that

Theorem (Weak Nullstellensatz):

Every maximal ideal of $\mathbb{C}[S]$ has this form.
That is, we have a bijection

$$\text{points of } S \longleftrightarrow \text{maximal ideals of } \mathbb{C}[S]$$

$$p \longleftrightarrow m_p$$

[It's a bit tricky to prove and depends on the fact that $\mathbb{C}$ is algebraically closed, i.e., the Fundamental Theorem of Algebra.].

Anyway, this allows us to replace the surface S by its coordinate ring $\mathbb{C}[S]$.

This is Grothendieck's Philosophy. //

Now suppose we have two Riemann surfaces and a nice (i.e. polynomial) map

$$\varphi : S \to S'$$

This induces a ring homomorphism in the other direction

$$\varphi^* : \mathbb{C}[S'] \to \mathbb{C}[S]$$

defined by $(\varphi^* f)(p) := f(\varphi(p))$ for all $f \in \mathbb{C}[S']$ and $p \in S$.

Fact: If $\varphi : S \twoheadrightarrow S'$ is surjective, then $\varphi^* : \mathbb{C}[S'] \hookrightarrow \mathbb{C}[S]$ is injective.

Proof: Suppose that $\varphi : S \twoheadrightarrow S'$ is surjective, and consider two functions $f, g \in \mathbb{C}[S']$ such that

$$\varphi^* f = \varphi^* g \in \mathbb{C}[S].$$

I claim that $f = g \in \mathbb{C}[S']$.

Indeed, given any $q \in S'$, $\exists\, p \in S$ with $q = \varphi(p)$. Then we have

$$\begin{aligned}
& \varphi^* f = \varphi^* g \\
\Longrightarrow\quad & \varphi^* f(p) = \varphi^* g(p) \\
\Longrightarrow\quad & f(\varphi(p)) = g(\varphi(p)) \\
\Longrightarrow\quad & f(q) = g(q).
\end{aligned}$$

Since this holds for all $q \in S'$, we conclude that $f = g \in \mathbb{C}[S']$. ///

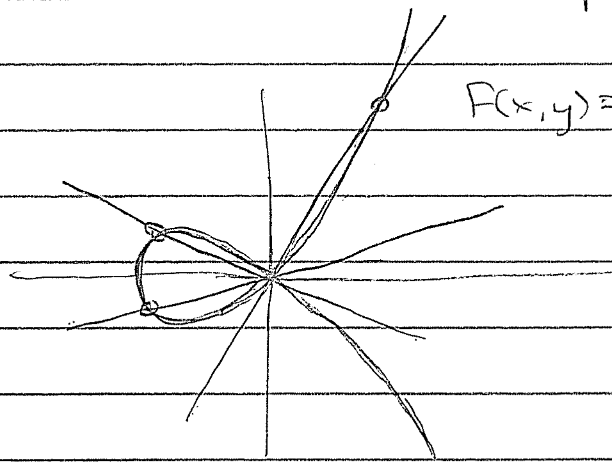
Thus if $\varphi : S \twoheadrightarrow S'$ is a resolution of singularities, we obtain an injection of coordinate rings

$$S \twoheadrightarrow S'$$

$$\mathbb{C}[S] \hookleftarrow \mathbb{C}[S']$$

Moreover the nice properties of $S \twoheadrightarrow S'$ will translate to nice properties of $\mathbb{C}[S'] \hookrightarrow \mathbb{C}[S]$.

Recall our favorite example:



$F(x,y) = y^2 - x^2(x+1).$

There is a singularity at $(0,0) \in S$ and this allows us to do a trick:

Consider the line $y = tx$ of slope t passing through $(0,0)$. It will intersect S in exactly one other point. We have

$$\begin{aligned} y^2 &= x^2(x+1) \\ (tx)^2 &= x^2(x+1) \\ t^2 \cancel{x^2} &= \cancel{x^2}(x+1) \\ t^2 &= x+1 \\ x &= t^2 - 1. \end{aligned}$$

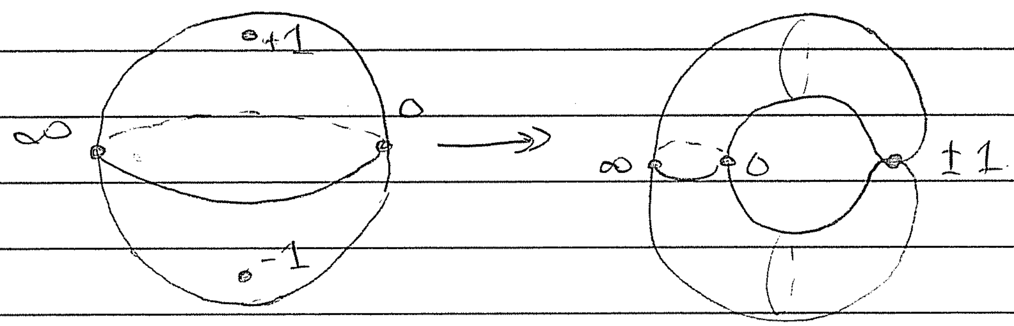
$$\Longrightarrow \quad \begin{aligned} y &= t(t^2-1) \\ &= t^3 - t. \end{aligned}$$

This gives us a parametrization of the curve/surface

$$\hat{\mathbb{C}} \twoheadrightarrow S$$
$$t \longmapsto (t^2 - 1, t^3 - t).$$

This map is a nice (i.e. polynomial) surjection, but it sends both ± 1 to the same point $(0,0)$.

Picture



This is the resolution of singularities we want. This induces an injection of coordinate rings

$$\mathbb{C}[S] \hookrightarrow \mathbb{C}[\hat{\mathbb{C}}]$$

How to describe this <u>algebraically</u>?

We have a ring homomorphism

$$\begin{aligned} \mathbb{C}[x,y] &\longrightarrow \mathbb{C}[t] \\ x &\longmapsto t^2-1 \\ y &\longmapsto t^3-t \end{aligned}$$

The kernel is exactly $I(S)$ so we have

$$\mathbb{C}[S] = \frac{\mathbb{C}[x,y]}{I(S)} \approx \mathbb{C}[t^2-1, t^3-t] \subseteq \mathbb{C}[t].$$

The field of fractions is

$$\mathrm{Frac}(\mathbb{C}[S]) = \mathrm{Frac}(\mathbb{C}[t^2-1, t^3-t]) = \mathbb{C}(t)$$

But $\mathbb{C}[S]$ is not integrally closed in $\mathbb{C}(t)$.

In fact, the integral closure of $\mathbb{C}[S]$ is precisely the resolution of singularities

$$\mathbb{C}[S] \hookrightarrow \overline{\mathbb{C}[S]} = \mathbb{C}[\hat{\mathbb{C}}]$$

$$\mathbb{C}[t^2-1, t^3-t] \hookrightarrow \mathbb{C}[t].$$

Theorem: This always works. Given a Riemann surface S, the integral closure of the coordinate ring

$$\varphi : \mathbb{C}[S] \hookrightarrow \overline{\mathbb{C}[S]}$$

lifts up to the resolution of singularities

$$\varphi^* : S' \twoheadrightarrow S$$

[We probably won't prove this, but I hope at least that it helps you believe in integral closure.]