LECTURE 11 : UNIQUE FACTORIZATION DOMAINS

Our overall goal is to understand the following story:

fields ⊂ Euclidean Domains ⊂ PIDs ⊂ UFDs ⊂ integral domains

But, first it would be nice to play a bit in the world of <u>algebraic</u> <u>number</u> <u>theory</u>. These results are taken from LECTURES 8 ⟶ 15 of my # theory course.

$\boxed{E1}$ <u>Pell's Equation</u>: Find solutions to $x^2 - ny^2 = 1$ for some given $n \in \mathbb{N}$.

Brahmagupta ~ 600 AD

Thm/ If (x_1, y_1) and (x_2, y_2) solve $x^2 - ny^2 = 1$ then (x_3, y_3) solves $x^2 - ny^2 = 1$ where $x_3 = x_1x_2 + ny_1y_2$ & $y_3 = x_1y_2 + x_2y_2$

<u>Proof</u>: $N(x+y\sqrt{n}) = x^2 - ny^2 = 1$ is Pell's Eq$^{=}$

$N(zw) = N(z)N(w)$ for $z, w \in \mathbb{Z}[\sqrt{n}]$

Then $N(z_1z_2) = N(z_1)N(z_2) = 1(1) = 1$

$$z_3 = z_1z_2 = (x_1 + y_1\sqrt{n})(x_2 + y_2\sqrt{n})$$
$$= \underbrace{x_1x_2 + ny_1y_2}_{x_3} + (\underbrace{x_1y_2 + y_1x_2}_{y_3})\sqrt{n}$$

$x^2 - 3y^2 = 1$ has smallest solution $(2,1)$

$(2+\sqrt{3})(2+\sqrt{3}) = 4+3+4\sqrt{3} = 7+4\sqrt{3}$

⟶ $(7,4)$ solves $x^2 - 3y^2 = 1$.

$(2+\sqrt{3})^3 = \underbrace{26+15\sqrt{3}}$

$(26, 15)$ solves $x^2 - 3y^2 = 1$.

E2 GAUSSIAN INTEGERS AND GAUSSIAN PRIMES

$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$

$N(a+ib) = a^2+b^2$, $N(zw) = N(z)N(w)$

$N(a+ib) = 1 \iff a+ib = 1, -1, i, -i$ (4 units)

Th^m/ An ordinary prime $p \in \mathbb{N}$ is a Gaussian Prime $\iff p \neq a^2+b^2$

Partial Proof:

If $p = a^2+b^2$ where $a, b \neq 0$ in $\mathbb{Z}$

then $p = (a+ib)(a-ib) \Rightarrow p$ not irreducible since $a \pm ib$ not unit in $\mathbb{Z}[i]$.

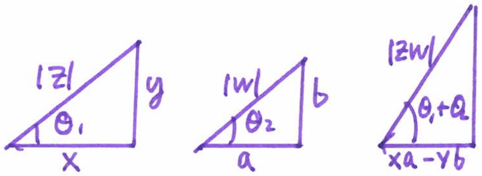
$\Rightarrow p$ not prime in $\mathbb{Z}[i]$.

FERMAT'S TWO SQUARE Th^m

If $n \in \mathbb{N}$ and if $p = 4n+1$ is prime then $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$.

Proof: given in my LECTURE 11 of Math 307, it uses arguments based on $\mathbb{Z}[i]$ and its norm, I have proof that $\mathbb{Z}(i]$ is a UFD and Bezout's Th^m holds for the Euclidean Algorithm for Gaussian Integers etc.

Two Square Identity



LECTURE 15, pg. 11

$z = x+iy$ $\quad z\bar{z} = (x+iy)(x-iy) = x^2+y^2$

$w = a+ib$ $\quad zw = (x+iy)(a+ib) = xa - yb + i(xa+yb)$

$|zw|^2 = |z|^2|w|^2$

$$\boxed{(xa-yb)^2+(xa+yb)^2 = (x^2+y^2)(a^2+b^2)}$$

(this formula is ancient, but its connection to complex #'s is why $\mathbb{Z}[i]$ naturally implements this into $N(zw) = N(z)N(w)$.)

Algebraic # theory used algebraic techniques in rings of integers such as $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and $\underbrace{\mathbb{Z}[\zeta_3]}_{\text{Eisenstein Integers}}$ where

$$x^2+y^2=(x-yi)(x+yi)$$

$$\underbrace{x^3+y^3=(x+y)(x+\zeta_3 y)(x+\zeta_3^2 y)}\qquad \left(\zeta_3=e^{2\pi i/3}\right)$$

- this algebra is used to prove $\nexists\ x,y,z\in\mathbb{N}$ for which $x^3+y^3=z^3$

  $\mathbb{Z}[\sqrt{-3}]$ is not a UFD since
  $$(1+\sqrt{-3})(1-\sqrt{-3})=4=2\cdot 2$$
  and $1\pm\sqrt{-3}$ not associates for 2.

  The Eisenstein Integers adjoin
  $$\zeta_3=e^{2\pi i/3}=\frac{-1+\sqrt{-3}}{2}$$
  and then $\mathbb{Z}[\zeta_3]$ gives Euclidean Domain hence PID hence UFD.

Comment: $\mathbb{Z}[\sqrt{-5}]$ also not UFD since $N(a+b\sqrt{-5})=a^2+5b^2$ turns out to not support a Euclidean Algorithm. However, unlike $\mathbb{Z}[\sqrt{-3}]$ we can't so easily "fix" $\mathbb{Z}(\sqrt{-5})$ by simply adding more points in $\mathbb{C}$ like with Eisenstein integers.

Lamè published wrong proof of Fermat's Last Th$^{\underline{m}}$ based on assuming unique factorization in $\mathbb{Z}[\zeta_n]$ as in:

$$x^n+y^n=(x+y)(x+y\zeta_n)(x+y\zeta_n^2)\cdots(x+y\zeta_n^{n-1})$$

To modify $\mathbb{Z}[\zeta_n]$ to obtain UFD we cannot continue to work directly inside $\mathbb{C}$, instead we have to group various #'s into ideals and work with "ideal #'s" as pioneered by Dedekind to prove FLT for many cases $\approx$ 1890's.

FOUR SQUARE THEOREM

For each $n \in \mathbb{N}$ there exists $a, b, c, d \in \mathbb{N} \cup \{0\}$ for which $n^2 = a^2 + b^2 + c^2 + d^2$

Proof: uses Hurwitz Integers which are like Eisenstein integers, but within the quaternions, this rests on the 4-square identity which Euler found in 1748 w/o aid of quaternions.

(Lagrange's proof in ≈1770 didn't use Hurwitz integers, he did something more brute force I think.)

$$(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) =$$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)^2$$

$$+ (b_1a_2 + a_1b_2 + c_1d_2 - c_2d_1)^2$$

$$+ (a_1c_2 + a_2c_1 + d_1b_2 - b_1d_2)^2$$

$$+ (a_1d_2 + d_1a_2 + b_1c_2 - c_1b_2)^2$$

(this is the 4-SQUARE IDENTITY, Euler found it 1748)

$$\eta = t + xi + yj + zk \in \mathbb{H} \text{ (quaternions)}$$

$$\bar{\eta} = t - xi - yj - zk$$

$$\eta\bar{\eta} = t^2 + x^2 + y^2 + z^2 = N(\eta)$$

Then $N(\alpha\beta) = N(\alpha)N(\beta)$

$\boxed{\text{E3}}$ Going back to $(xa - yb)^2 + (xa + yb)^2 = (x^2+y^2)(a^2+b^2)$

consider $\underbrace{(3^2+4^2)}_{5^2}\underbrace{(5^2+12^2)}_{13^2} = (z\bar{z})(w\bar{w})$

$$= zw\,\overline{zw}$$

$$= (3+4i)(5+12i)\,\overline{zw}$$

$$= (15 - 48 + i(36+20))\,\overline{zw}$$

$$\boxed{65^2 = 33^2 + 56^2}$$

The calculations and concepts we find in Euclidean Domains were largely pioneered by mathematicians such as Euler, Gauss and their students in the nineteenth century. The necessity of facing the existence of a unique factorization and/or how to deal with the absence of a unique factorization property took a bit longer to be appreciated. As Gallian describes on page 316, the assumption of unique factorization misled Gabriel Lamé to claim he had a proof of Fermat's last theorem (which is that $x^n + y^n = z^n$ has no integer solutions for $n \geq 3$). Unfortunately, Lamé was not familar with the work of Kummer which demonstrated the factorization into irreducibles was not unique in the natural sense which Lamé assumed.

It seems Gauss was aware of this issue when he basically avoided using abstract ring arguments. Gauss was aware of Euler's work and Euler and Lagrange used objects like $a + b\sqrt{-d}$ to prove various assertions about primes. Gauss likely realized the danger made explicit by Kummer. Stillwell explains this story in more depth in his text *Elements of Number Theory.* Basically, Gauss just brute-force[11] solved the problems which Euler and Lagrange had been working on in more elegant ways. In some sense, this was bad mathematics, it took some time for us to return to the elegance which Euler and Lagrange had partially understood. The fix to the ambiguity suffered by Lamé was given in part by Kummer with his introduction of **ideal numbers**. This program was fleshed out by Dedekind. Basically, ideals play the role that numbers previously held. The ambiguity is washed away in that there is a unique factorization property for ideals in a ring of algebraic integers[12]

Ultimately, the work of Dedekind brought questions to the mind of Emmy Noether who was one of the first true abstract algebraists. Her work was about structure much more than particular examples. She embraced the concept of abstraction as a means to solve many problems in an elegant fashion. I mention Noether here because the chain condition argument below is certainly due to her influence on our current understanding of abstract algebra.

Definition 4.8.6. *Let D be an integral domain. D is a* **Unique Factorization Domain** *if*

(i.) *every nonzero element of D can be written as a product of irreducible elements in D,*

(ii.) *the factorization of a given element in D into irreducibles is unique up to re-ordering and associates. In particular, if $x \in D$ has irreducible factorizations $x = x_1x_2 \cdots x_n$ and $x = y_1y_2 \cdots y_n$ then there exist units $u_1, u_2, \dots, u_n$ for which*

$$\{y_1, y_2, \dots, y_n\} = \{u_1x_1, u_2x_2, \dots, u_nx_n\}$$

where we do not intend the above equality to imply an ordering.

The uniqueness up to associates is easy enough to see in the context of $\mathbb{Z}$ where the units are ±1 or $F[x]$ where any nonzero scalar is a unit.

Theorem 4.8.7. Ascending Chain Condition in a PID: *In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length.*

Proof: let $I_1 \subset I_2 \subset \cdots$ be a chain of strictly increasing ideals in an principlal ideal domain D. Note $\cup_{j \in \mathbb{N}} I_j$ forms an ideal thus $I = I_1 \cup I_2 \cup \cdots = \langle d \rangle$ for some $d \in D$. Note $d \in I$ implies $d \in I_n$ for some $n \in \mathbb{N}$. But, $I_i \subseteq I = \langle d \rangle \subseteq I_n$ for each $i \in \mathbb{N}$ hence I_n must be the terminal ideal in the chain. □

[11] as in he solved congruence questions via explicit algebra in $\mathbb{Z}$ etc.

[12] see page 767, Corollary 16, of Dummit and Foote, this claim is quite a bit beyond our current course.

I didn't prove unique factorization of $\mathbb{Z}[x]$ (gory detail on page 304-305 of Gallian for the curious), but, if I had this still would not help as $\mathbb{Z}[x]$ is not a PID. That said, if F is a field then this proof gets us that $F[x]$, a PID by Theorem 4.5.17, is a unique factorization domain. The proof of this theorem is perhaps the most interesting proof we will study this semester:

Theorem 4.8.8. *Every principal ideal domain is a unique factorization domain.*

Proof: let D be a PID with set of units U. Let $a_0 \in D$ with $a_0 \neq 0$ and $a_0 \notin U$. Game plan:

(1.) show a factorization of a_0 contains at least one irreducible

(2.) show there is a factorization of a_0 into a product of irreducibles

(3.) show uniqueness up to associates

(1.) If a_0 is irreducible then we have shown a_0 contains an irreducible. Otherwise, $a_0 = a_1b_1$ where a_1 is not a unit and $b_1 \neq 0$. If a_1 is irreducible then a contains an irreducible. Otherwise, suppose $a_1 = a_2b_2$ where $b_2 \neq 0$ and a_2 is not a unit. Continue in this fashion to define a_{n+1} not a unit and $b_{n+1} \neq 0$ for which $a_n = a_{n+1}b_{n+1}$ for $n = 3, 4, \dots$. Observe, $a_n = a_{n+1}b_{n+1}$ implies $\langle a_n \rangle \subset \langle a_{n+1} \rangle$ for $n = 0, 1, 2, \dots$ thus by Theorem 4.8.7 there exists k for which this ascending chain of ideals terminates:

$$\langle a_0 \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_k \rangle.$$

But, the chain terminates when a_k does not permit a factorization into non-units. Hence a_k is irreducible hence $a_0 = ra_k$ shows a_0 contains an irreducible.

(2.) if a_0 is irreducible then we have a factoring of a_0 into irreducibles. Otherwise, by (1.) there exists an irreducible p_1 and a non-unit c_1 for which $a_0 = p_1c_1$. If c_1 is an irreducible then we have factored a_0 into irreducibles. Otherwise, apply (1.) to the non-unit c_1 to find $c_1 = p_2c_2$ where p_2 is irreducible and c_2 is not a unit. Notice we have another ascending chain of ideals:

$$\langle a_0 \rangle \subset \langle p_1 \rangle \subset \langle p_2 \rangle \subset \cdots$$

this must terminate, say at $\langle p_t \rangle$. By the construction of the chain, we find p_t is an irreducible and

$$a_0 = p_1c_1 = p_1p_2c_2 = \cdots = p_1p_2 \cdots p_t.$$

Therefore, a_0 is factored into a product of irreducibles.

(3.) Suppose a_0 has two factorizations into irreducibles:

$$a_0 = p_1p_2 \cdots p_t = q_1q_2 \cdots q_s$$

We prove the factorization is unique by induction on t. Suppose $t = 1$ then $a_0 = p_1 = q_1q_2 \cdots q_s$ implies $s = 1$ as to say otherwise contradicts the irreducibilty of p_1. Next, suppose inductively, any factorization into less than t irreducibles is unique up to associates. Again, if

$$a_0 = p_1p_2 \cdots p_t = q_1q_2 \cdots q_s$$

then note $p_1 \mid q_1q_2 \cdots q_s$ hence (by an exercise I might assign) there exists some q_j for which $p_1 \mid q_j$ and thus $p_1 = u_jq_j$ for some unit u_j. Then,

$$q_ju_jp_2 \cdots p_t = q_jq_2 \cdots q_s$$

and by the cancellation property for integral domains ($q_j \neq 0$)

$$u_j p_2 \cdots p_t = q_j q_2 \cdots q_s$$

and by the induction hypothesis we conclude that the remaining $t-1$ irreducibles $u_j p_2, \dots, p_{j-1}, p_{j+1}, \dots, p_t$ must be associated to $s-1 = t-1$ irreducibles $q_2, \dots, q_{j-1}, q_{j+1}, \dots, q_t$. Thus, the factorization of a_0 into irreducibles is unique up to associates and ordering. □

I tried to follow Gallian pretty closely here. Essentially the same proof is given on page 319-320.

Corollary 4.8.9. *Let F be a field. Then $F[x]$ is a unique factorization domain.*

Proof: we proved in Theorem 4.5.17 for F a field the polynomials $F[x]$ form a PID hence by Theorem 4.8.8 we find $F[x]$ is a UFD. □

I abbreviate to illustrate the utility of these abbreviations.

Theorem 4.8.10. *Every euclidean domain is a principal ideal domain.* (did this last Lecture)

Proof: let D be a Euclidean Domain with norm N. If I is a nonzero ideal in D then notice $S = \{N(x) \mid x \in I\}$ is a nonempty subset of non-negative integers. Thus, by the Well-Ordering-Principle, S has a smallest member s_o. Let $x_o \in I$ be a member of I for which $N(x_o) = s_o$. If $z \in I$ then apply the division algorithm in D to obtain q and r for which

$$z = qx_o + r$$

Note $z \in I$ by assumption and $qx_o \in I$ by as $x_o \in I$ thus

$$r = z - qx_o \in I$$

Therefore, $r = 0$ as $r \neq 0$ would provide $r \in I$ for which $N(r) < N(x_o) = s_o$ which contradicts the minimality of s_o in S. In short, every element $z \in I$ is found in $\langle x_o \rangle$. But, I was arbitrary nonzero ideal hence every nonzero ideal is princpal. Moreover, $\langle 0 \rangle = \{0\}$ and the Theorem follows. □

I hope you see this proof is nearly identical in structure to that we gave for Theorem 4.5.17. In retrospect, we could have skipped that proof and simply applied this general result to the context of the norm on $F[x]$ being specified by the degree function.

Corollary 4.8.11. *Every euclidean domain is a unique factorization domain.*

Proof: note Theorem 4.8.10 gives that D Euclidean implies D is a PID. Then Theorem 4.8.8 provides that D a PID implies D is a UFD. □

Notice that $\mathbb{Z}[x]$ is a UFD, but, $\mathbb{Z}[x]$ is not a PID. The implications in the proof above are not reversible. An example of a PID which is not a Euclidean Domain is a bit harder to find. Gallian gives a reference. I'll add the following link: Tom Oldfield's Construction of PIDs which are not Euclidean Domains the other answer by Bill Dubuque is also useful. Both answers are a bit beyond this course. I expect you to be aware of these results, but, I don't expect you can actually produce a PID which is not a Euclidean Domain. In contrast, knowing that $\mathbb{Z}[x]$ is a UFD but not a PID is exactly the sort of thing you ought to know.

8

Next, we study an elegant proof of Eisenstein's Criterion: (stated as Theorem 4.6.18 in these notes)

Proof: (Gallian credits Richard Singer for the proof we give here). Suppose $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and the prime p is such that $p \nmid a_n$ but $p \mid a_j$ for $j = n-1, \dots, 0$ and $p^2 \nmid a_0$. Suppose $f(x)$ is reducible over $\mathbb{Q}$. Then $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ by Theorem 4.6.11. Notice modulo p the polynomial reduces to $\overline{f(x)} = a_nx^n$ hence $a_nx^n = \overline{g(x)}\ \overline{h(x)}$. But, x is an irreducible in $\mathbb{Z}_p[x]$ and as $\mathbb{Z}_p[x]$ is a UFD as $\mathbb{Z}_p$ is a field we deduce that $x \mid \overline{g(x)}$ and $x \mid \overline{h(x)}$ from which we deduce $\overline{g(0)} = 0$ and $\overline{h(0)} = 0$ thus $p \mid g(0)$ and $p \mid h(0)$ and $f(x) = h(x)g(x)$ gives $f(0) = a_0 = h(0)g(0)$ and we find $p^2 \mid a_0$ which is a contradiction. Consequently, $f(x)$ is irreducible over $\mathbb{Q}$. □.

discuss

Example 4.8.12. *A nice example where unique factorization fails is provided by* $\mathbb{Z}[\sqrt{-5}]$. *Note* $\mathbb{Z}[\sqrt{-5}]$ *forms a subring of* $\mathbb{C}$ *hence is commutative and has no zero divisors. Moreover,* $1 = 1 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ *hence* $\mathbb{Z}[\sqrt{-5}]$ *is an integral domain. We have multiplicative norm* $N(a+b\sqrt{-5}) = a^2 + 5b^2$. *Solving*

$$a^2 + 5b^2 = 1$$

we find just two solutions, $a = 1, b = 0$ *or* $a = -1, b = 0$. *There are just the units* $-1, 1$ *thus judging if a pair of elements are associates is quite easy. Observe,*

$$46 = (2)(23) \qquad \& \qquad 46 = (1 + 3\sqrt{-5})(1 - 3\sqrt{-5})$$

It is immediately clear these the factors $2,\ 23,\ 1 + 3\sqrt{-5}$ *and* $1 - 3\sqrt{-5}$ *are not associates. Furthermore, their irreducibility may be shown from the usual arguments involving the norm. Suppose* $2 = xy$ *for some* $x, y \in \mathbb{Z}[\sqrt{-5}]$ *then* $N(2) = 4 = N(x)N(y)$ *and if* x, y *are not units then we need* $N(x) = N(y) = 2$. *Yet,* $a^2 + 5b^2 = 2$ *clearly has no solution in* $\mathbb{Z}$. *Therefore, 2 is irreducible. Similarly, if* $23 = xy$ *then we would need to find a solution to* $a^2 + 5b^2 = 23$ *to give solution to* $23 = xy$ *where* x, y *are not units. Explicit trial of reasonable* $\mathbb{Z}$ *rules out hope of a solution to* $a^2 + 5b^2 = 23$. *Continuing, if* $1 + 3\sqrt{-5} = xy$ *then* $N(1 + 3\sqrt{-5}) = 1 + 5(9) = 46$ *we require* $N(x) = 2$ *and* $N(y) = 23$ *without loss of generality. Again, it is not possible to solve* $a^2 + 5b^2 = 2$ *over* $\mathbb{Z}$. *In summary, we have provided two factorizations of 46 into irreducibles and there is no hope these are equivalent up to associates and reordering.* $\mathbb{Z}[\sqrt{-5}]$ *is not a UFD.*