

CONFESSIONS OF AN INT(D) - ALIOLIC

Note Title

7/6/2009

THE FUNDAMENTAL STRUCTURE OF POLYNOMIAL RINGS IS A BASIC TOPIC IN A BEGINNING ABSTRACT ALGEBRA COURSE. USUALLY TWO EXTREMES ARE EMPHASIZED.

$\mathbb{Q}[x] \rightsquigarrow$ A PID AND HENCE
A UFD

$\mathbb{Z}[x] \rightsquigarrow$ A UFD BUT
DEFINITELY NOT
A PID

$I = (2, x)$ IS NOT
PRINCIPAL.

QUESTION: WHAT "LIVES" BETWEEN
 $\mathbb{Q}[x]$ AND $\mathbb{Z}[x]$?

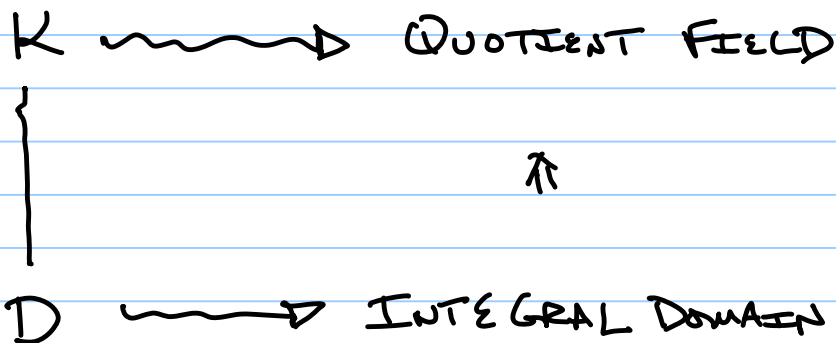
ANSWER: A LOT!

LAST TIME WE CONSIDERED ONE OF THESE RINGS

$$\mathbb{Z} + X \mathbb{Q}[X]$$

WHICH WAS NOT EVEN ATOMIC.

WE CONSIDER HERE THE GENERAL CASE:



WE CONSIDER AN ARITHMETICALLY MOTIVATED EXAMPLE.

DEFINITION: LET $S \subseteq D$, SET

$$\text{INT}(S, D) = \{ f(x) \in K[x] \mid f(s) \in D \forall s \in S \}$$

$\text{INT}(S, D)$ IS KNOWN AS THE RING OF
POLYNOMIALS INTEGER-VALUED ON S .
IF $S=D$, THEN WE WRITE

$$\text{INT}(D, D) = \text{INT}(D).$$

HISTORICAL MOTIVATION FOR ALGEBRAIC
STUDY OF $\text{INT}(S, D)$

POLYA (≈ 1918) STUDIED THIS
RING FOR $D = \mathbb{Z}$ (FOR A
QUADRATIC RING OF INTEGERS).

WHAT WAS POLYA INTERESTED IN?
CONSIDER FOR A MOMENT BINOMIAL
COEFFICIENTS

$$\binom{m}{n} = \frac{m!}{n! (m-n)!} = \frac{m(m-1) \dots (m-n+1)}{n!}$$

WHERE $n, m \in \mathbb{N}$, $0 \leq n \leq m$.

\Rightarrow FACT FROM DISCRETE MATH

$$\binom{m}{n} \in \mathbb{N} \subseteq \mathbb{Z}.$$

THUS, FIX " n " AND LET m

"ROW WIND THROUGH \mathbb{Z} ".

$m \rightarrow \dots \rightarrow X$ A VARIABLE.

$$\binom{X}{n} = \frac{X(X-1)\dots(X-n+1)}{n!}$$

SO $\binom{X}{n} \in \mathbb{Z}$ $X \geq n$, $\binom{X}{n} = 0$

FOR $0 \leq X \leq n-1$. IT IS NOW

EASY TO ARGUE THAT $\binom{X}{n} \in \mathbb{Z}$

FOR $X < 0$. THE SET $\left\{ \binom{X}{n} \right\}_{n \geq 0}$

IS KNOWN AS THE SET OF

BINOMIAL POLYNOMIALS.

$$\binom{X}{0} = 1 \quad \binom{X}{1} = X$$

$$\binom{X}{2} = \frac{X(X-1)}{2!} \quad \binom{X}{3} = \frac{X(X-1)(X-2)}{3!}$$

.....

THIS SET OF POLYNOMIALS ALLOWS
US TO GET A "FEEL" FOR WHAT
THE ELEMENTS OF $\text{INT}(\mathbb{Z})$ LOOK
LIKE.

IMPORTANT THEOREM: EVERY
ELEMENT $f(x) \in \text{INT}(\mathbb{Z})$ CAN
BE EXPRESSED UNIQUELY IN THE
FORM

$$f(x) = c_0 \binom{x}{0} + c_1 \binom{x}{1} \\ + \dots + c_k x^k$$

WHERE EACH $c_i \in \mathbb{Z}$.

So, in the LINEAR ALGEBRA
SENSE $\left\{ \binom{x}{n} \right\}_{n \geq 0}$ FORMS A
"BASIS" OF $\text{INT}(\mathbb{Z})$ OVER
 \mathbb{Z} .

A NICE "TRICK"

HOW DO YOU WRITE $f(x) = 2x^3 + x - 1$
IN TERMS OF THE $\left\{ \binom{x}{n} \right\}_{n \geq 0}$?

$f(0)$ $f(1)$ $f(2)$ $f(3)$

-1 2 17 56

3 15 39

12 24

12

$$2x^3 + x - 1 = -1 \binom{x}{0} + 3 \binom{x}{1}$$

$$+ 12 \binom{x}{2} + 12 \binom{x}{3}.$$

MOREOVER $\left\{ \binom{x}{n} \right\}_{n \geq 0}$ CONTAINS
EXACTLY ONE POLYNOMIAL OF EACH
POSITIVE DEGREE.

\implies HENCE WE CALL THIS A
REGULAR BASIS.

POLYA (\approx 1918 CRELLÉ'S JOURNAL)
IF $\bar{\mathbb{Z}}$ IS A QUADRATIC RING
OF INTEGERS, THEN DOES
 $\text{INT}(\bar{\mathbb{Z}})$ HAVE A REGULAR BASIS?

ANSWER \implies NOT ALWAYS

BUT IF $\bar{\mathbb{Z}}$ IS A PID THEN

THE ANSWER IS YES.

IF $S \subseteq \mathbb{Z}$ AND $|S| = \infty$,

THEN $\text{INT}(S, \mathbb{Z})$ HAS A SIMILAR

BASIS. WHAT SUBSETS OF S GIVE

A REALLY NICE BASIS?

HOW ABOUT $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$?

THE SET OF PRIME NUMBERS?

$$\binom{x}{0}_{\mathbb{P}} = 1 \quad \binom{x}{1}_{\mathbb{P}} = x-1$$

$$\binom{x}{2}_{\mathbb{P}} = \frac{(x-1)(x-2)}{2}$$

$$\binom{x}{3}_{\mathbb{P}} = \frac{(x-1)(x-2)(x-3)}{2^3 \cdot 3}$$

$$\binom{x}{4}_{\mathbb{P}} = \frac{(x-1)(x-2)(x-3)(x-5)}{2^4 \cdot 3}$$

$$\binom{x}{5}_P = \frac{(x-1)(x-2)(x-3)(x-5)(x+4)}{2^7 \cdot 3^2 \cdot 5^2}$$

$$\binom{x}{6}_P = \frac{(x-1)(x-2)(x-3)(x-5)(x+4)(x-7)}{2^8 \cdot 3^2 \cdot 5}$$

THE DENOMINATORS OF THESE

POLYNOMIALS ARE CALLED BY

BHARGAVA (MATH. MONTHLY 107 (2008))

"GENERALIZED FACTORIALS"

AND DENOTED $n!_S$

$$\text{So } 0!_P = 1 \quad 1!_P = 1$$

$$2!_P = 2 \quad 3!_P = 2^3 \cdot 3$$

$$4!_P = 2^4 \cdot 3 \quad 5!_P = 2^7 \cdot 3^2 \cdot 5$$

.....

ANOTHER NICE FACT ABOUT $\text{INT}(\mathbb{Z})$:

IT CONTAINS IDEALS THAT ARE NOT FINITELY GENERATED.

LET

$$I = \{ f(x) \in \text{INT}(\mathbb{Z}) \mid f(0) = 0 \}$$
$$= (\binom{x}{1}, \binom{x}{2}, \binom{x}{3}, \dots).$$

WHEN $|S| < \infty$, THEN MANY

THINGS CHANGE (SEE M^cQUILLIAN
PROC. ROYAL IRISH ACADEMY 85(1985)).

IN FACT, IN THIS CASE, $\text{INT}(S, \mathbb{Z})$

IS NOT EVEN ATOMIC.

AN EASY WAY TO SEE THIS:

WHAT IS $\text{INT}(\{0\}, \mathbb{Z})$?

$$f(0) \in \mathbb{Z} \Rightarrow f(x) = z + f_1 x + \dots + f_n x^n.$$

$$\Rightarrow \text{INT}(\{0\}, \mathbb{Z}) = \mathbb{Z} + x \mathbb{Q}[x]$$

NOT ATOMIC BY
THE TALK YESTERDAY.

ALSO CONSIDER THE FOLLOWING:

$$\text{INT}(\{1, 2\}, \mathbb{Z}) \Rightarrow$$

$$f(x) = \frac{(x-1)(x-2)}{10} = 3 \cdot \frac{(x-1)(x-2)}{30}$$

$$= 3 \cdot 5 \cdot \frac{(x-1)(x-2)}{150} = \dots$$

LET'S RETURN TO CAHEN-CHABERT

THEIR PROOF THAT $\rho(\text{INT}(\mathbb{Z})) = \infty$

USES INFINITE SEQUENCES.

AN ALTERNATE PROOF: BASED ON THE
FACT THAT $\left\{ \binom{X}{n} \right\}_{n \geq 0}$ ARE ALL
IRREDUCIBLE.

PICK $n > 0$

$$(X-n) \binom{X}{n} = \frac{X(X-1) \cdots (X-n+1)(X-n)}{n!}$$

$$= (n+1) \frac{X(X-1) \cdots (X-n+1)(X-n)}{(n+1)n!}$$

$$= (n+1) \binom{X}{n+1}$$

$$\Rightarrow \underbrace{(X-n) \binom{X}{n}}_{\text{ATOMS}} = n+1 \binom{X}{n+1}$$

AS

MANY FACTORS

AS YOU

WANT

$$P(\text{INT}(\mathbb{Z})) \geq \frac{P}{2}$$

$$\rightarrow P \rightarrow \infty$$

$$\rightarrow P(\text{INT}(\mathbb{Z})) = \infty$$

SO HOW DO ELEMENTS OF $\text{INT}(\mathbb{Z})$

REALLY FACTOR?

DEFINITION: LET $f(x) \in \text{INT}(\mathbb{Z})$.

SET

$$d(f(x)) = \text{GCD}\{f(u) \mid u \in \mathbb{Z}\}.$$

$d(f(x))$ IS CALLED THE FIXED DIVISOR
OF $f(x)$.

MOREOVER, IF $d(f(x)) = 1$, THEN

CALL $f(x)$ IMAGE PRIMITIVE.

OBSERVATION: $f(x) \in A(\text{INT}(\mathbb{Z}))$

$\implies f(x)$ IMAGE PRIMITIVE.

PROOF: $d(f(x)) = n > 1$, THEN

$$f(x) = n \cdot \left(\frac{f(x)}{n} \right)$$

LET $f(x) = f_0 + f_1 x + \dots + f_k x^k$
 $\in \mathbb{Z}[x]$. IF $\text{GCD}(f_0, \dots, f_k) = 1$
THEN $f(x)$ IS CALLED PRIMITIVE.

HENCE IF $f(x) \in A(\text{INT}(\mathbb{Z}))$ THEN

$$f(x) = \frac{f'(x)}{d(f'(x))} \quad (*)$$

WHERE $f'(x)$ IS PRIMITIVE IN $\mathbb{Z}[x]$.

OBSERVATION: $d(x) = 1$

$$d((x-1)) = 1$$

$$d(x(x-1)) = 2$$

More: $d(f_1(x)f_2(x)) \neq d(f_1(x))d(f_2(x))$

BUT $d(f_1(x))d(f_2(x)) \mid d(f_1(x)f_2(x))$.

THEOREM: LET $f(x) = \frac{f'(x)}{d(f'(x))}$

BE IMAGE PRIMITIVE IN $\text{INT}(\mathbb{Z})$.

$f(x) \in A(\text{INT}(\mathbb{Z})) \iff$ WHENEVER

$f'(x) = s(x)t(x)$ FOR $s(x), t(x) \in$

$\mathbb{Z}[x]$ AND $\text{DEG } s(x), \text{DEG } t(x) > 0$,

THEN $d(s(x))d(t(x)) < d(s(x)t(x))$.

EXAMPLE: WHY IS $\frac{x(x-1)(x-2)}{3 \cdot 2 \cdot 1}$

IRREDUCIBLE IN $\text{INT}(\mathbb{Z})$?

IS $\frac{x(x-10)(x-8)}{3}$ IRREDUCIBLE?

YES! \implies THIS INSPIRES
 \equiv A GENERAL CONSTRUCTION.

LEMMA: LET p BE A PRIME NUMBER.

\exists INTEGERS i_1, i_2, \dots, i_p

SO THAT

$$f_p(x) = \frac{(x-i_1)(x-i_2)\dots(x-i_p)}{p}$$

IS IRREDUCIBLE IN $\mathbb{Z}[x]$.

PROOF BY THE CHINESE REMAINDER

THEOREM, CHOOSE i_1, \dots, i_p SO THAT

$$\begin{array}{l|l} i_1 \equiv 0 \pmod{p} & i_1 \equiv 1 \pmod{q} \\ i_2 \equiv 1 \pmod{p} & i_2 \equiv 1 \pmod{q} \\ \vdots & \vdots \\ i_p \equiv p-1 \pmod{p} & i_p \equiv 1 \pmod{q} \end{array}$$

FOR ALL PRIMES

$$q < p.$$

FOR THE $f_p(x)$ JUST CONSTRUCTED,

SET $h_p(x) = (x-i_1) \cdots (x-i_p)$.

$$\text{So } f_p(x) = \frac{h_p(x)}{p}.$$

THEOREM (CHAPMAN-McCLAIN)

JOURNAL OF ALGEBRA 293(2005):

LET $R, S \in \mathbb{N}$. THEN

$$p(h_p^R(x) f_p^S(x)) = \frac{p^{R+S}}{2R+S}$$

COROLLARY: LET $\frac{t}{u} \in \mathbb{Q}$ WITH

$\frac{t}{u} > 1$. THEN \exists A PRIME $p \in \mathbb{Z}$

AND $R, S \in \mathbb{N}$ SO THAT

$$\frac{t}{u} = \frac{p^{R+S}}{2R+S}.$$

THUS $\text{INT}(z)$ IS FULLY
ELASTIC!