Lecture 24: Historical view towards algebra

Wednesday, November 29, 2017 10:01 AM

Historically algebra was developed to study zeros of polynomials. Having symbolic algebra in our disposal, it is easy for us to find zeros of deg. 1 and deg. 2 polynomials; but at a time a whole book by Kharazmi was devoted to giving an algorithm for finding zeros of a deg. 2 polynomial. In 11 century Khayyam more or less found zeros of deg. 3 polynomials. In 16 century Ferrari gave an algor. of finding zeros of deg. 4 polynomials. In 1824, Abel proved that there is no solution in radicals to the general poly. eq. of deg. ≥ 5. In 1832, Galois gave an elegent treatment of understanding zeros of a single variable poly.; and he essentially said the group of symmetries of zeros is the key tool to study them.

Then algebra grew in two (related) directions: understanding zeros of multi-variable polynomials (using geometric intuitions); And trying to prove Fermat's last conjecture (finding zeros of

Lecture 24: Ring theory and other parts of math

Wednesday, November 29, 2017 11:14 AM

$x^n+y^n-z^n=0$ in $\mathbb{Z}$ or equivalently zeros of X^n+Y^n-1 in $\mathbb{Q}$.)

These were motivations to study (mostly) commutative, unital rings.

As we mentioned earlier, even to study the commutative rings one is forced to understand their group of symmetries that are often non-commutative. To study groups, a basic tool is to investigate their linear actions, which is called a representation. In representation theory, certain non-commuta. rings naturally arise: for instance group rings and certain Banach algebras.

Another place that non-commutative rings naturally arise is in Lie theory. Again we'd like to understand the group of symmetr. of certain geometry; e.g. hyperbolic geometry, Euclidean geom., ..., but it is easier to study linear objects. So we pass to the Lie algebra. Then Lie algebra is not associative, so we pass to the so-called <u>universal enveloping algebra</u>. (that is typically non-commutative.)

As it was pointed out earlier, geometric intuitions have been extremely instrumental in asking "the right questions" about commutative rings. The subject of <u>non-commutative geometry</u> is trying to develope certain geometric objects in order to help us to ask "the right questions" for non-commutative rings; and it often has connections with physics. (Professor Rogalski is an expert on this subject).

- Zeros of polynomials → geometric, → arithmetic } mostly commutative rings.

- Representation theory: group ring, Banach algebra, ...
- Lie theory: universal enveloping algebra
- Non-commutative geometry and physics.

} mostly non-commutative.

In the 200-series, we mostly study <u>unital commutative rings</u>.

Some of the definitions should be changed in order to be suitable

Lecture 24: Def'n; Examples of non-commutative rings

Wednesday, November 29, 2017 11:41 AM

for non-commutative rings; eg. prime ideals.

Let's recall some of the definitions:

Def. • $(R,+,\cdot)$ is called a ring if

1. $(R,+)$ is an abelian group.
2. (Associativity) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
3. (Distribution) $a\cdot(b+c)=a\cdot b+a\cdot c$ and
   $(b+c)\cdot a = b\cdot a+c\cdot a$

• A ring $(R,+,\cdot)$ is called unital if $\exists\, 1_R\in R$ s.t.

$1_R\neq 0_R$ and $\forall a\in R$, $a\cdot 1_R=1_R\cdot a=a$.

1_R is called the unity of R.

$\left(\to\ 1'_R = 1'_R\cdot 1_R = 1_R\ .\right)$

• A ring $(R,+,\cdot)$ is called commutative if $\forall a,b\in R$, $a\cdot b=b\cdot a$.

Matrix Ring. Suppose R is a ring. Then the set $M_n(R)$ of $n\times n$ matrices with entries in R forms a ring with the following operations: $[a_{ij}]+[b_{ij}]:=[a_{ij}+b_{ij}]$,

$$[a_{ij}][b_{ij}]:=\Big[\sum_{k=1}^{n} a_{ik}b_{kj}\Big].$$

Lecture 24: Matrix ring; Monoid ring

Wednesday, November 29, 2017 12:05 PM

Notice that $\begin{bmatrix}0&1\\0&0\end{bmatrix}\begin{bmatrix}0&0\\1&0\end{bmatrix}=\begin{bmatrix}1&0\\0&0\end{bmatrix}$ and $\begin{bmatrix}0&0\\1&0\end{bmatrix}\begin{bmatrix}0&1\\0&0\end{bmatrix}=\begin{bmatrix}0&0\\0&1\end{bmatrix}$; so for any unital ring R, $M_2(R)$ is non-commutative.

<u>Group ring</u>. Suppose $(M,\cdot)$ is a monoid and R is a ring. Then $RM := \{\underbrace{\sum_{m\in M} r_m m}_{\text{formal sums}} \mid r_m = 0 \text{ except for finitely many } m\}$.

Alternatively $RM := \{f: M \to R \mid f(m)=0 \text{ except for finitely many } m\}$.

$$\Big(\sum_{m\in M} r_m m\Big) + \Big(\sum_{m\in M} r'_m m\Big) := \sum_{m\in M} (r_m + r'_m)\, m \;;\quad (f_1+f_2)(m) := f_1(m)+f_2(m)$$

$$\Big(\sum_{m\in M} r_m m\Big)\cdot\Big(\sum_{m\in M} r'_m m\Big) := \sum_{m\in M} \Big(\sum_{m_1 m_2 = m} r_{m_1} r'_{m_2}\Big)\, m$$

we get this def. using distrib. and regrouping the terms.

since $\{m\in M \mid r_m \neq 0 \text{ or } r'_m \neq 0\}$ is finite, this is a finite sum; and only for $m \in \{m_1\in M \mid r_{m_1}\neq 0\}\{m_2 \in M \mid r_{m_2}\neq 0\}$ it can be non-zero.

In the language of functions, it is denoted by $*$ and is called the <u>convolution</u> of the given functions:

$$(f_1 * f_2)(m) := \sum_{m_1 m_2 = m} f_1(m_1) f_2(m_2).$$

Lecture 24: Banach algebra

Wednesday, November 29, 2017 12:52 PM

When M is a group, $\mathbb{R}M$ is called a <u>group ring</u>.

Here we did not involve analysis; we can consider

$$L^1(G) := \{ f: G \to \mathbb{C} \mid \sum_{g\in G} |f(g)| < \infty \}.$$

If $f_1, f_2 \in L^1(G)$, we again define

$$(f_1 * f_2)(g) := \sum_{g_1 g_2 = g} f_1(g_1) f_2(g_2).$$

This part was skipped during the lecture

Then $\displaystyle\sum_{g\in G} |(f_1 * f_2)(g)| \le \sum_{g\in G} \Big(\sum_{g_1 g_2 = g} |f_1(g_1)| |f_2(g_2)| \Big).$

By Fubini's theorem, we have

$$\sum_{(g_1', g_2') \in G\times G} |f_1(g_1)| |f_2(g_2)| = \underbrace{\Big(\sum_{g\in G} |f_1(g)|\Big)}_{\|f_1\|_1} \underbrace{\Big(\sum_{g\in G} |f_2(g)|\Big)}_{\|f\|_2} < \infty$$

$$\|$$

$$\sum_{(g, g_1)\in G\times G} |f_1(g_1)| |f_2(g_1^{-1} g)| = \sum_{g\in G} \Big(\sum_{g_1 g_2 = g} |f_1(g_1)| |f_2(g_2)| \Big).$$

So $\|f_1 * f_2\|_1 \le \|f_1\|_1 \cdot \|f_2\|_1 < \infty$. Hence $(L^1(G), +, *)$ is a ring and $\mathbb{C}G$ is a subring of $L^1(G)$.

$L^1(G)$ is an example of Banach algebras.

(If you want to work with Professor Ioana, you would start with the embedding $\mathbb{C}G \hookrightarrow L^1(G)$!)

Lecture 24: Polynomial ring

Wednesday, November 29, 2017 1:09 PM

From this point on we will assume our rings are <u>unital commutative</u>.

<u>Polynomial ring</u>. Suppose R is a ring. Then the ring of polynomials over R with indeterminant x is denoted by $R[x]$. And it is the monoid ring of $M=\{1,x,x^2,\ldots\}$ (notice that $\mathbb{Z}^{\geq 0}\to\{1,x,x^2,\ldots\}$, $i\mapsto x^i$ is an isomorphism of monoids.)

So $R[x]=\{\sum_{i=0}^{\infty} r_i x^i \mid r_i=0$ except for finitely many i's$\}$.

- $\left(\sum_{i=0}^{\infty} r_i x^i\right)+\left(\sum_{i=0}^{\infty} r_i' x^i\right)=\sum_{i=0}^{\infty}(r_i+r_i')x^i$.
- $\left(\sum_{i=0}^{\infty} r_i x^i\right)\left(\sum_{i=0}^{\infty} r_i' x^i\right)=\sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} r_k r_{i-k}'\right)x^i$.

Inductively we can define $R[x_1,\ldots,x_n]$; and this is the same as the monoid ring RM where $M\simeq \underbrace{\mathbb{Z}^{\geq 0}\times\cdots\times\mathbb{Z}^{\geq 0}}_{n \text{ times}}$,

$M=\{x_1^{i_1}\cdot x_2^{i_2}\cdot\ldots\cdot x_n^{i_n} \mid i_1,\ldots,i_n\in\mathbb{Z}^{\geq 0}\}$.

<u>Remark</u>. Any polynomial $p(x)=\sum_{i=0}^{\infty} c_i x^i\in R[x]$ can be viewed as a function (that is denoted by p again) $p:R\to R$,

$p(r):=\sum_{i=0}^{\infty} c_i r^i$ (this is a finite sum.) But distinct polynomials might give rise to the same function.

Lecture 24: Polynomial ring

Wednesday, November 29, 2017 1:36 PM

Ex. $x, x^2, \dots \in (\mathbb{Z}/2\mathbb{Z})[x]$ are distinct polynomials, but they all give us the following function $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $0 \mapsto 0$, $1 \mapsto 1$.

Despite this subtlety our best tool of understanding ring of polynomials is by viewing them as functions; in algebraic geometry we often try to say that we do not lose information by thinking about poly. as functions.

Def. Suppose R_1 and R_2 are two unital rings. $\phi: R_1 \to R_2$ is called a ring homomorphism if

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \phi(1_{R_1}) = 1_{R_2}.$$

Lemma (Evaluation map) Suppose R is a unital commutative ring. Then, for any $r \in R$, $\phi_r : R[x] \to R$, $\phi_r(p(x)) = p(r)$ is a ring homomorphism. (Pf is easy)

Remark. The above lemma is not true for non-commutative rings. If R is non-commutative, ϕ_r is a ring hom. if and only if $r \in Z(R)$ where $Z(R) := \{a \in R \mid \forall b \in R, ab = ba\}$.