Elyasheev Leibtag
Weizmann institute of science

Tutorial

WEEK 1

1. Preliminaries on Rings

Definition 1.0.1. A triple $(R,, \cdot)$ is a ring if $(R, +)$ is an abelian group and the multiplication $\cdot$ is distributive on both sides, i.e.

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

and $\cdot$ is associative.

Example 1.0.1.
- $\mathbb{Z}$
- $2\mathbb{Z}$ (but not the "odds")
- $\mathbb{R}[x]$ - the ring of polynomials
- Any field
- $K[x_1, ..., x_n]$
- $K[k_1, ...]$ ring with infinitely many variables, still each element in this ring is a finite collection of symbols
- $Mat_{n\times n}(K)$
- $R[x_1, ...x_n]$ letting R be a ring and not a field is still ok!

Definition 1.0.2. We ay R is a ring with a unit if there is $1 \in R$ s.t. $a \cdot 1 = a = 1 \cdot a$

Exercise 1.0.1. In a ring- the units 0,1 are unique

Definition 1.0.3. A ring R is called commutative if $(R, \cdot)$ is commutative.

Exercise 1.0.2. Which ring above are commutative

From now on we will only deal with commutative rings with unit!

Definition 1.0.4. A ring R is called an integral domain if $a \cdot b = 0 \to a = 0 \; or \; b = 0$

Definition 1.0.5. The set$I$ in a ring R is called an ideal, and denoted $I \lhd R$ if $(I, +)$ is an abelian subgroup of $(R, +)$ and for any $r \in R\, a \in I$, $a \cdot r \in I$.
Note: for non commutative rings we need to separate right and left ideals.

Exercise 1.0.3. Let $S \subset R$, TFAE:

- $I = \bigcap_{S \subset J \lhd R} J$
- $I \lhd R$ (unique) minimal ideal containing S
- $I = \{s_1 r_1 + ... + s_n r_n \ : \ n \in \mathbb{N}, s_i \in S, r_i \in R\}$

Definition 1.0.6. Let S and R as above. We call this ideal "The ideal generated by S and denote it by $< S >$.
If S is a singleton then $< S >$ is called a principle ideal.

Definition 1.0.7. Let R be a (commutative unital..) ring, if any ideal I in R is principle we say that R is a principle ideal domain - PID.

Exercise 1.0.4. Show that $\mathbb{Z}$ is PID.

Exercise 1.0.5. Show that $K[x]$ is PID. (Hint- look at the degree of polynomial)

Exercise 1.0.6. Show that $\mathbb{C}[x, y]$ is NOT PID. ($< x, y >$). Same for $\mathbb{R}, \mathbb{Z}$

2. Some more on ideals

Definition 2.0.1. Let I be an ideal in R, the radical of I denoted by $\sqrt{I}$ is the set $\sqrt{I} := \{r \in R \ : \ r^n \in I \ \ for\ some\ n\}$
An ideal is called radical if $I = \sqrt{I}$.

Exercise 2.0.1. Show that the radical is indeed an ideal.

Exercise 2.0.2. What is $\sqrt{n\mathbb{Z}}$ in the ring $\mathbb{Z}$.

Lemma 2.0.1. Let R be an integral domain, and I an ideal

- R/I is a field iff I is maximal

3. Fields

Definition 3.0.1. We say that $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ if there exist $p \in \mathbb{Q}[x]$ (non trivial) s.t. $p(\alpha) = 0$.
If no such polynomial exist then we call α transcendental.

Recall notation, $\mathbb{Q}[\alpha]$ is polynomials in α i.e. formal sums $\sum_i q_i \alpha^i$, if α is algebraic then this ring is actually a field, this condition is iff.

Definition 3.0.2. For $\alpha \in \mathbb{C}$ the field $\mathbb{Q}(\alpha)$ is the minimal sub-field of $\mathbb{Q}$ containing α.

Let $K \subset L$ be a field extension, define $Gal(L/K)$ (The Galois group of L over K to be all field automorphism of L that fix K).
If the extension if finite (as dim vector space viewpoint) then the field fixed by elements of $Gal(L/K)$ is exactly K.
Let $f \in K[x]$ be a polynomial if $f(\alpha) = 0$ then $K(\alpha)/K$ is a finite extension.
Set $G := Gal(K(\alpha)/K)$ we get that $p_\alpha := \prod_{\sigma \in G}(x - \sigma(\alpha))$ is in $K[x]$ since all coefficients are fixed by G.
Also $f(\sigma(\alpha)) = 0$ for any element in the Galois group. Hence $p_\alpha \mid f$. (This is how we went down a degree for our induction claim in class.)

4. Curves

.

In class we saw a definition of an algebraic curve, it is the "zero set" in $\mathbb{C}^2$ of a polynomial in two variables $f \in \mathbb{C}[x, y]$ we denote the zero set as $\mathcal{Z}(f) := \{(x, y) \ : \ f(x, y) = 0\}$(z for zeros/Zariski).

By corollary of theorem we saw in class ($|\mathcal{Z}(f) \cap \mathcal{Z}(g)| < \infty$) we will often refer to the polynomial itself as the curve, notice any constant times a curve it the same curve.

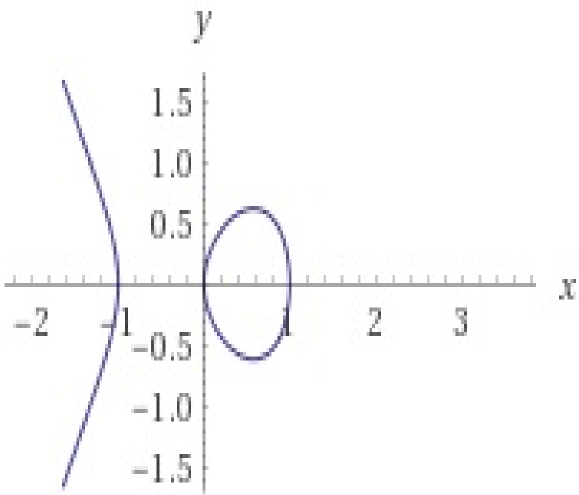
Example 4.0.1. The curve $f(x, y) = x + y$ is the anti diagonal line, the curve $f(x, y) = xy$ is the two axis.

Can we say how these curves are different?
One is irreducible and one is reducible.

Definition 4.0.1. A curve $C = \mathcal{Z}(f)$ is called irreducible if it is reducible as a polynomial, and reducible otherwise i.e. if $f = g \cdot h$ (g, h non units)

We can look at the drawing of the curve and see the difference between the reducible and irreducible ones- but caution!

Exercise 4.0.1 (For home)**.** Describe the curve $f(x, y) = y^2 - x + x^3$ prove that is it irreducible.



$y^2 - x + x^3$

Notice that this is just the "real" picture of the curve, for example the curve $x^2 + y^2 + 1$ is empty in "Real life" but actually is non empty over the complex field.
Some fact are true also over non algebraically closed fields.

5. GENERIC POINTS

A generic point over field is a transcendental number, for example π over $\mathbb{Q}$.
The fact about these point is that given a field k, and π generic over k, then $k(\pi) \cong k(x)$.
For example given a curve $f(x, y)$ with coefficients in$\mathbb{Q}$ we may regard $f(\pi, y) \in \mathbb{Q}(\pi)[y]$ (a polynomial in one variable defined over a sub-field of $\mathbb{C}$) we know by fundamental theorem of algebra that this polynomial has at most deg(f) solutions.
(The idea behind the generic point is the if we look at the field K which is the field generated by coefficients, and look at the topology in $\mathbb{C}^n$ generated by closed subsets defined as zeros of polynomials in $K[X]$ we get that the generic point is a dense set. i.e. any algebraic statement true for a generic point is true in general.)

Exercise 5.0.1 (Saw in lecture)**.** If $f(x, y)$ irreducible then so is $f(\pi, y)$

Example 5.0.1. The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$ so we should be careful when just saying irreducible in general.

6. PROJECTION TO AXIS

Given a curve $f(x, y)$ we may project the curve to the x-axis.

$$Prj_X(f) = \{x \in \mathbb{C} \ : \ \exists y \in \mathbb{C} \ f(x, y) = 0\}$$

Exercise 6.0.1 (In class)**.** Show that besides a finite number of points the fiber over each point is finite.
Write $f(x, y) = a_0(x) + a_1(x)y + a_2(x)y^2 + ... + a_n(x)y^n$. If fiber if x_0 is infinite then $|\{y \in \mathbb{C} \ : \ f(x_0, y) = \sum_i a_i(x_0)y^i = 0\}| = \infty$ thus $a_i(x_0) = 0$ there are only finite many x_0 that satisfy this condition.

Exercise 6.0.2 (In class)**.** Let F_q be a finite field with q elements. Let $f(x, y) \in F_q[x, y]$ of degree d, then $|\mathcal{Z}(f)| \leq q \cdot d$.
Since:
$|\mathcal{Z}(f)| = \sum_{x \in F_q} |\{y \in F_q \ : \ f(x, y) = 0\}|$ if $f(x_0, y) \in F_q[x]$ is the zero polynomial by writing $f(x, y) = a_0(x) + a_1(x)y + a_2(x)y^2 + ... + a_n(x)y^n$. We have that $a_i(x_0) = 0$ for any i. Let $h := gcd(\{a_i\}) \in F_q[x, y]$ then of course $h \mid f$ so there exist $g \in F_q[x, y]$ s.t. $f = h \cdot g$. Notice that $f(x', y') = 0$ if ether $h(x', y') = 0$ or $g(x', y') = 0$.
Assume $f(x', y') = 0$, If $h(x', y') = 0$ then $h(x', y) = 0$ for all y. This happens when x' is a root of h thus the amount of such pair is bounded by $\deg(h) \cdot q$.
If $h(x', y') \neq 0$ then $g(x', y') = 0$ and for any such x' there are at most $deg(g)$ such y that give zero thus the amount of such pair is bounded by $deg(g) \cdot q$ we get that

$$|\mathcal{Z}(f)| \leq deg(g) \cdot q + deg(h) \cdot q = deg(f) \cdot q$$

as needed!

Exercise 6.0.3 (For home or in class if time premits)**.** Let $f(x,y) \in \mathbb{C}[x,y]$ non constant, then $|\mathcal{Z}(f)| = \aleph$.

7. Affine Algebraic Varieties

In the previous part of the course we regarded a single polynomial in 2 variables. In this part we consider any collection of polynomials in many variables.

Definition 7.0.1. Given a sub collection of polynomials $S \subset \mathbb{C}[x_1, ...x_n]$, we define $\mathcal{Z}(S) := \{x \in \mathbb{C}^n \ : \ s(x) = 0 \ \forall s \in S\}$.

Exercise 7.0.1. Notice the following

- If $S_1 \subset S_2$ then $\mathcal{Z}(S_2) \subset \mathcal{Z}(S_1)$
- $\mathcal{Z}(S_1 \cup S_2) = \mathcal{Z}(S_1) \cap \mathcal{Z}(S_2)$, $\mathcal{Z}(S_1 \cdot S_2) = \mathcal{Z}(S_1) \cup \mathcal{Z}(S_2)$
- $\mathcal{Z}(S) = \mathcal{Z}(< S >) = \mathcal{Z}(\sqrt{< S >})$

So an "algebraic set" or a "Zariski closed set" is the zero-locus of a radical ideal.
Q: What is a closure of a set with respect to this topology?

Definition 7.0.2. Given any set $X \subset \mathbb{C}^n$ we define $\mathcal{I}(X) := \{f \in \mathbb{C}[x_1, ..., x_n] \ : \ f(x) = 0 \forall x \in X\}$.
Notice this is radical ideal.

Exercise 7.0.2. We have the following

- If $X_1 \subset X_2$ then $\mathcal{I}(X_2) \subset \mathcal{I}(X_1)$.
- $\mathcal{I}(X_1 \cap X_2) = \sqrt{\mathcal{I}(X_1) + \mathcal{I}(X_2)}$ (Notice that for radical ideal $I_1 + I_2$ does no need to be radical (take $x, x - y^2$))
- $\mathcal{I}(X_1 \cap X_2) = \mathcal{I}(X_1) \cdot \mathcal{I}(X_2)$
- $I \lhd \mathbb{C}[x_1, ..., x_n]$, $I \subset \mathcal{I}(\mathcal{Z}(I))$
- $X \subset \mathcal{Z}(\mathcal{I}(X))$

We may this of the NSS in the following formulation (seen in class)

Theorem 7.0.1 (NSS)**.**

$$\mathcal{I}(\mathcal{Z}(S)) = \sqrt{< S >}$$

And notice that the closure of a set Y is $\overline{Y} = \mathcal{Z}(\mathcal{I}(Y))$

Examples of affine varietys

Example 7.0.1. Examples of algebraic sets:

- matrix SL_n
- the set Gl_n of invertable matrices is open (Later we will fallow Rabinowitz trick to show how it can be thought of as a closed set)

Definition 7.0.3. Let G be a group, a representation of G is an n dimensional a homomorphism $\pi \colon G \to GL_n(\mathbb{C})$. Using HBT we can show the following:

Theorem 7.0.2. Let Γ be a finitely generated group (not necessarily finitely presented) then there exist a finitely represented group Δ with a surjection $\Delta \twoheadrightarrow \Gamma$ such that Δ and Γ have same representations for every dimension n.

Proof. What we will show is that the set of n-dimensional representations of Γ is an algebraic set.
Assume $\Gamma =< \gamma_1, ..., \gamma_k >$ (maybe take $k = 2$ for convenience).
Define the following n^2 tuples in $\mathbb{C}^{(2k)n^2}$.

$$\begin{bmatrix} a_{11} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n.1} & \dots & a_{n,n} \end{bmatrix}, \begin{bmatrix} b_{11} & \dots & b_{1,n} \\ \vdots & \ddots & \vdots \\ b_{n.1} & \dots & b_{n,n} \end{bmatrix}, \begin{bmatrix} A_{11} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{n.1} & \dots & A_{n,n} \end{bmatrix}, \begin{bmatrix} B_{11} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{n.1} & \dots & B_{n,n} \end{bmatrix}$$

One lower case and one upper case (matrix) for each generators.
And define the polynomials that state $A_{i,j}a_{i,j} = Id_{i,j}$ and all relations etcetera... Since Γ is not necessarily finitely presented there can be infinite amount of polynomials defining this set. From HBT there are just finitely many polynomials defining this set. Take all relations that include such a polynomial from the defining set. And define $\Delta =< \gamma_1, ..., \gamma_k >$ to be the group generated by $\{\gamma_i\}$ but only with the selected relations.
What we have show is that if the representation satisfies the relations of Δ then it satisfies the relations for Γ. $\square$

Note that there are unaccountably many finitely generated groups but just countably many finitely presented ones.