Intro GA

18/3/2021

Prelim algebraicos

Contents

Preface **i**

1 Affine Algebraic Sets **1**
1.1 ~~Algebraic Preliminaries~~ 1
1.2 Affine Space and Algebraic Sets 4
1.3 The Ideal of a Set of Points 5
1.4 The Hilbert Basis Theorem 6
1.5 Irreducible Components of an Algebraic Set 7
1.6 Algebraic Subsets of the Plane 9
1.7 Hilbert's Nullstellensatz 10
1.8 Modules; Finiteness Conditions 12
1.9 Integral Elements 14
1.10 Field Extensions 15

2 Affine Varieties **17**
2.1 Coordinate Rings 17
2.2 Polynomial Maps 18
2.3 Coordinate Changes 19
2.4 Rational Functions and Local Rings 20
2.5 Discrete Valuation Rings 22
2.6 Forms 24
2.7 Direct Products of Rings 25
2.8 Operations with Ideals 25
2.9 Ideals with a Finite Number of Zeros 26
2.10 Quotient Modules and Exact Sequences 27
2.11 Free Modules 29

3 Local Properties of Plane Curves **31**
3.1 Multiple Points and Tangent Lines 31
3.2 Multiplicities and Local Rings 34
3.3 Intersection Numbers 36

Hartshorne "Algebraic Geometry"

Moderna

1 2 3 4 5

Clásica

?

4 Projective Varieties **43**
4.1 Projective Space 43
4.2 Projective Algebraic Sets 44
4.3 Affine and Projective Varieties 48
4.4 Multiprojective Space 50

5 Projective Plane Curves **53**
5.1 Definitions 53
5.2 Linear Systems of Curves 55
5.3 Bézout's Theorem 57
5.4 Multiple Points 59
5.5 Max Noether's Fundamental Theorem 60
5.6 Applications of Noether's Theorem 62

6 Varieties, Morphisms, and Rational Maps **67**
6.1 The Zariski Topology 67
6.2 Varieties 69
6.3 Morphisms of Varieties 70
6.4 Products and Graphs 73
6.5 Algebraic Function Fields and Dimension of Varieties 75
6.6 Rational Maps 77

7 Resolution of Singularities **81**
7.1 Rational Maps of Curves 81
7.2 Blowing up a Point in $\mathbb{A}^2$ 82
7.3 Blowing up Points in $\mathbb{P}^2$ 86
7.4 Quadratic Transformations 87
7.5 Nonsingular Models of Curves 92

8 Riemann-Roch Theorem **97**
8.1 Divisors 97
8.2 The Vector Spaces $L(D)$ 99
8.3 Riemann's Theorem 101
8.4 Derivations and Differentials 104
8.5 Canonical Divisors 106
8.6 Riemann-Roch Theorem 108

A Nonzero Characteristic **113**

B Suggestions for Further Reading **115**

C Notation **117**

Chapter 1

Affine Algebraic Sets

Anillo R con $+, \cdot$ y $0 \neq 1$ y conmutativo. $[x \cdot y = y \cdot x]$

1.1 Algebraic Preliminaries

This section consists of a summary of some notation and facts from commutative algebra. Anyone familiar with the italicized terms and the statements made here about them should have sufficient background to read the rest of the notes.

When we speak of a *ring*, we shall always mean a commutative ring with a multiplicative identity. A *ring homomorphism* from one ring to another must take the multiplicative identity of the first ring to that of the second. A $\boxed{\textit{domain}}$, or integral domain, is a ring (with at least two elements) in which the cancellation law holds. A *field* is a domain in which every nonzero element is a unit, i.e., has a multiplicative inverse.

dominio

cuerpo

$\mathbb{Z}$ will denote the domain of integers, while $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will denote the fields of rational, real, complex numbers, respectively.

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$R \quad K$

Any domain R has a quotient field K, which is a field containing R as a *subring*, and any elements in K may be written (not necessarily uniquely) as a ratio of two elements of R. Any one-to-one ring homomorphism from R to a field L extends uniquely to a ring homomorphism from K to L. Any ring homomorphism from a field to a nonzero ring is one-to-one.

$K = \left\{ \frac{a}{b} : a, b \in R,\ b \neq 0 \right\}$

$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b$

$$\begin{tikzcd} & K \arrow[d, dashed, "\exists!"] \\ R \arrow[ur] \arrow[r, hook] & L = \text{cuerpo} \end{tikzcd}$$

For any ring R, $R[X]$ denotes the ring of polynomials with coefficients in R. The *degree* of a nonzero polynomial $\sum a_i X^i$ is the largest integer d such that $a_d \neq 0$; the polynomial is *monic* if $a_d = 1$.

The ring of polynomials in n variables over R is written $R[X_1, \ldots, X_n]$. We often write $R[X,Y]$ or $R[X,Y,Z]$ when $n = 2$ or 3. The monomials in $R[X_1, \ldots, X_n]$ are the polynomials $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, i_j nonnegative integers; the degree of the monomial is $i_1 + \cdots + i_n$. Every $F \in R[X_1, \ldots, X_n]$ has a unique expression $F = \sum a_{(i)} X^{(i)}$, where the $X^{(i)}$ are the monomials, $a_{(i)} \in R$. We call F *homogeneous*, or a *form*, of degree d, if all coefficients $a_{(i)}$ are zero except for monomials of degree d. Any polynomial F has a unique expression $F = F_0 + F_1 + \cdots + F_d$, where F_i is a form of degree i; if $F_d \neq 0$, d is the *degree* of F, written $\deg(F)$. The terms $F_0, F_1, F_2, \ldots$ are called the *constant, linear, quadratic, …* terms of F; F is *constant* if $F = F_0$. ~~The zero polynomial is allowed~~

homogeneo:

$F = x^2 + xy + y^2$

$\lambda^d \cdot F(x_1, \ldots, x_n) = F(\lambda x_1, \ldots, \lambda x_n)$

$\Updownarrow$

homogeneo.

$$F = \underbrace{\overset{a_0}{F_0}}_{\text{const}} + \underbrace{\overset{a_1x_1 + \cdots + a_nx_n}{F_1}}_{\text{lineal}} + F_2 + \cdots + F_d, \quad \deg(F) = d$$

$\tilde{\varphi}: x_i \mapsto s_i \ \forall i$

$R = k[x]$
$f(x,y), g(x,y) \in k[x,y]$ sin factores comunes
$\Rightarrow f(x,y), g(x,y) \in k(x)[y]$ sin fact. comunes.
$K = k(x) = \left\{ \frac{p(x)}{q(x)} \right\}$

$R[x_1,\dots,x_n]$ $\exists!\ \tilde{\varphi}$
$R \xrightarrow{\varphi} S \ni s_1,\dots,s_n$

$-\infty$

~~to have any degree~~. If R is a domain, $\deg(FG) = \deg(F) + \deg(G)$. The ring R is a subring of $R[X_1,\dots,X_n]$, and $R[X_1,\dots,X_n]$ is characterized by the following property: if φ is a ring homomorphism from R to a ring S, and $s_1,\dots,s_n$ are elements in S, then there is a unique extension of φ to a ring homomorphism $\tilde{\varphi}$ from $R[X_1,\dots,X_n]$ to S such that $\tilde{\varphi}(X_i) = s_i$, for $1 \le i \le n$. The image of F under $\tilde{\varphi}$ is written $F(s_1,\dots,s_n)$. The ring $R[X_1,\dots,X_n]$ is canonically *isomorphic* to $R[X_1,\dots,X_{n-1}][X_n]$.

$R[x,y] \simeq R[x][y]$

An element a in a ring R is *irreducible* if it is not a unit or zero, and for any factorization $a = bc$, $b, c \in R$, either b or c is a unit. A domain R is a *unique factorization domain*, written UFD, if every nonzero element in R can be factored uniquely, up to units and the ordering of the factors, into irreducible elements.

$\mathbb{Z} \ni 16 \leftarrow$ no es irred.
$= 4 \cdot 4$

If R is a UFD with quotient field K, then (by Gauss) any irreducible element $F \in R[X]$ remains irreducible when considered in $K[X]$; it follows that if F and G are polynomials in $R[X]$ with no common factors in $R[X]$, they have no common factors in $K[X]$.

If R is a UFD, then $R[X]$ is also a UFD. Consequently $\boxed{k[X_1,\dots,X_n]}$ (cuerpo) is a UFD for any field k. The quotient field of $k[X_1,\dots,X_n]$ is written $k(X_1,\dots,X_n)$, and is called the *field of rational functions* in n variables over k.

2 irred. maximales — ptos
Ideal $\leftrightarrow$ Variedad
R — Alg. Comm. Spec(R) — Geom.

If $\varphi: R \to S$ is a ring homomorphism, the set $\varphi^{-1}(0)$ of elements mapped (finito) to zero is the *kernel* of φ, written $\mathrm{Ker}(\varphi)$. It is an *ideal* in R. And ideal I in a ring R is *proper* if $I \ne R$. A proper ideal is *maximal* if it is not contained in any larger proper ideal. A *prime* ideal is an ideal I such that whenever $ab \in I$, either $a \in I$ or $b \in I$.

R, $m \subset I$: $m = I$ o $I = R$

A set S of elements of a ring R *generates* an ideal $I = \{\sum a_i s_i \mid s_i \in S, a_i \in R\}$. An ideal is *finitely generated* if it is generated by a finite set $S = \{f_1,\dots,f_n\}$; we then write $\boxed{I = (f_1,\dots,f_n)}$. An ideal is *principal* if it is generated by one element. A domain in which every ideal is principal is called a *principal ideal domain*, written $\boxed{\text{PID}}$. The ring of integers $\mathbb{Z}$ and the ring of polynomials $k[X]$ in one variable over a field k are examples of PID's. Every PID is a UFD. A principal ideal $I = (a)$ in a UFD is prime if and only if a is irreducible (or zero).

Típico
ED $\subsetneq$ PID $\subsetneq$ UFD $\subsetneq$ Dom.
E.D.

Let I be an ideal in a ring R. The *residue class ring* of R modulo I is written $\boxed{R/I}$; it is the set of equivalence classes of elements in R under the equivalence relation: $a \sim b$ if $a - b \in I$. The equivalence class containing a may be called the I-residue of a; it is often denoted by $\boxed{\overline{a}}$. The classes R/I form a ring in such a way that the mapping $\pi: R \to R/I$ taking each element to its I-residue is a ring homomorphism. The ring R/I is characterized by the following property: if $\varphi: R \to S$ is a ring homomorphism to a ring S, and $\varphi(I) = 0$, then there is a unique ring homomorphism $\overline{\varphi}: R/I \to S$ such that $\boxed{\varphi = \overline{\varphi} \circ \pi}$. A proper ideal I in R is prime if and only if R/I is a domain, and maximal if and only if R/I is a field. Every maximal ideal is prime.

$0 = [i]$ cociente
$\mathbb{Z} \supset n\mathbb{Z}$
$\mathbb{Z}/n\mathbb{Z}$ = enteros mod. n.

max $(x - \alpha) \leftrightarrow \alpha$
$\mathbb{C}[x] \qquad \mathbb{C}$

Let k be a field, I a proper ideal in $k[X_1,\dots,X_n]$. The canonical homomorphism π from $k[X_1,\dots,X_n]$ to $k[X_1,\dots,X_n]/I$ restricts to a ring homomorphism from k to $k[X_1,\dots,X_n]/I$. We thus regard k as a subring of $k[X_1,\dots,X_n]/I$; in particular, $k[X_1,\dots,X_n]/I$ is a vector space over k.

$I \subset k[x_1,\dots,x_n]$
$R = k[x_1,\dots,x_n]/I$

Let R be a domain. The *characteristic* of R, $\mathrm{char}(R)$, is the smallest integer p such that $1 + \cdots + 1$ (p times) $= 0$, if such a p exists; otherwise $\mathrm{char}(R) = 0$. If $\varphi: \mathbb{Z} \to R$ is the unique ring homomorphism from $\mathbb{Z}$ to R, then $\mathrm{Ker}(\varphi) = (p)$, so $\mathrm{char}(R)$ is a prime number or zero.

If R is a ring, $a \in R$, $F \in R[X]$, and a is a $\boxed{root}$ of F, then $F = (X-a)G$ for a unique

$F(a) = 0$

I primo $\Leftrightarrow R/I$ dominio $\qquad I$ max $\Leftrightarrow R/I$ cuerpo

$k \subset k[x_1,\dots,x_n]$
$\forall\ I$ ideal
$\Rightarrow k \subset k[x_1,\dots,x_n]/I$
Torre
k-álgebra

$\Rightarrow)$ I max, R/I cuerpo?
$\ni x \ne 0 \Rightarrow \exists\ x^{-1} = r$
$J = \langle I, x \rangle \supsetneq I = \max$
$\Rightarrow J = R \ni 1 = i + r \cdot x \ \therefore R/I\ \ 1 = \bar{r} \cdot \bar{x}$

Geom. algebraica

Car = 0

«Real»

Car = p > 0

«el otro mundo»

• Patologías

p = 2

R no lo es
$f(x) = x^2+1$
no tiene raíces.

$\mathbb{R} \subset \mathbb{C} = \overline{\mathbb{R}}$
Teo fund del álgebra.

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$\overline{\mathbb{F}_p}$ es infinito
car $= p > 0$

$k = \overline{k}$
$\Rightarrow \#\{k\} = \infty$

Dem/ Sino
$k = \{\alpha_1, \dots, \alpha_n\}$
$\Rightarrow f(x) = (x-\alpha_1)\cdots(x-\alpha_n) + 1$
no tiene raíces en k →←

$G \in R[X]$. A field k is *algebraically closed* if any non-constant $F \in k[X]$ has a root. It follows that $F = \mu \prod (X - \lambda_i)^{e_i}$, $\mu, \lambda_i \in k$, where the λ_i are the distinct roots of F, and e_i is the *multiplicity* of λ_i. A polynomial of degree d has d roots in k, counting multiplicities. The field $\mathbb{C}$ of complex numbers is an algebraically closed field.

Let R be any ring. The *derivative* of a polynomial $F = \sum a_i X^i \in R[X]$ is defined to be $\sum i a_i X^{i-1}$, and is written either $\frac{\partial F}{\partial X}$ or F_X. If $F \in R[X_1, \dots, X_n]$, $\frac{\partial F}{\partial X_i} = F_{X_i}$ is defined by considering F as a polynomial in X_i with coefficients in $R[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n]$. The following rules are easily verified:

derivada formal.

(1) $(aF + bG)_X = aF_X + bG_X$, $a, b \in R$.
(2) $F_X = 0$ if F is a constant.
(3) $(FG)_X = F_X G + F G_X$, and $(F^n)_X = nF^{n-1} F_X$.
(4) If $G_1, \dots, G_n \in R[X]$, and $F \in R[X_1, \dots, X_n]$, then

$$F(G_1, \dots, G_n)_X = \sum_{i=1}^{n} F_{X_i}(G_1, \dots, G_n)(G_i)_X.$$

(5) $F_{X_i X_j} = F_{X_j X_i}$, where we have written $F_{X_i X_j}$ for $(F_{X_i})_{X_j}$.
(6) (*Euler's Theorem*) If F is a form of degree m in $R[X_1, \dots, X_n]$, then

$$\boxed{mF = \sum_{i=1}^{n} X_i F_{X_i}.}$$

Problems

1.1.* Let R be a domain. (a) If F, G are forms of degree r, s respectively in $R[X_1, \dots, X_n]$, show that FG is a form of degree $r+s$. (b) Show that any factor of a form in $R[X_1, \dots, X_n]$ is also a form.

1.2.* Let R be a UFD, K the quotient field of R. Show that every element z of K may be written $z = a/b$, where $a, b \in R$ have no common factors; this representative is unique up to units of R.

1.3.* Let R be a PID, Let P be a nonzero, proper, prime ideal in R. (a) Show that P is generated by an irreducible element. (b) Show that P is maximal.

1.4.* Let k be an infinite field, $F \in k[X_1, \dots, X_n]$. Suppose $F(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in k$. Show that $F = 0$. (*Hint:* Write $F = \sum F_i X_n^i$, $F_i \in k[X_1, \dots, X_{n-1}]$. Use induction on n, and the fact that $F(a_1, \dots, a_{n-1}, X_n)$ has only a finite number of roots if any $F_i(a_1, \dots, a_{n-1}) \neq 0$.)

1.5.* Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[X]$. (*Hint:* Suppose $F_1, \dots, F_n$ were all of them, and factor $F_1 \cdots F_n + 1$ into irreducible factors.) ← ...

1.6.* Show that any algebraically closed field is infinite. (*Hint:* The irreducible monic polynomials are $X - a$, $a \in k$.)

1.7.* Let k be a field, $F \in k[X_1, \dots, X_n]$, $a_1, \dots, a_n \in k$. (a) Show that

$$F = \sum \lambda_{(i)} (X_1 - a_1)^{i_1} \dots (X_n - a_n)^{i_n}, \quad \lambda_{(i)} \in k.$$

(b) If $F(a_1, \dots, a_n) = 0$, show that $F = \sum_{i=1}^{n} (X_i - a_i) G_i$ for some (not unique) G_i in $k[X_1, \dots, X_n]$.