AG NOTES

MARK BLUNK

Abstract. Some rough notes to get you all started.

1. Introduction

Here is a list of the main topics that are discussed and used in my research talk. The information is rough and brief, but I have listed references if people want to learn more, or if they want to see precise definitions.

2. Galois Theory

Let F be a field. a field extension K of F is a field which contains F. K is said to be an *algebraic extension* if every element $a \in K$ satisfies a polynomial f with coefficients in F. An algebraic extension is *finite* if K is a finite dimensional F vector space, i.e. of finite degree. A algebraic extension is *separable* if every element satisfied a polynomial with no repeated roots. It turns out that every finite separable extension K of F can be embedded in a finite *Galois* extension of F, which is a separable field extension such that the group of K-automorphisms fixing F has the same size as the degree of K over F. By wild abuse of the Axiom of Choice, one can prove the existence of a separable closure $\overline{F}$ of F, a field containing all the finite separable field extensions of F. It has an automorphism group $\Gamma = \mathrm{Gal}(\overline{F}/F)$, which is the inverse limit of finite groups.

3. Varieties

3.1. algebraically closed case.

3.1.1. *Affine.* Let F be an algebraically closed field (e.g. $\mathbb{C}$). We will denote by $\mathbb{A}^n_F$ the set of n-tuples with entries in the field F. This is called Affine space. For any collection $\{f_\alpha\}$ of polynomials $f_\alpha \in F[x_1, \dots, x_n]$ (i.e. in n-variables with coefficients in F), we denote by $Z(f_\alpha)$ the subset of $\mathbb{A}^n_F$ consisting of all the points a which f_α satisfy, i.e. $f_\alpha(a) = 0$, for all α. The first thing to note is that for any collection f_α, the points that vanish on all the f_α agree with the points that vanish on the all the polynomials in the ideal $I(f_\alpha)$ generated by the f_α. Then, by some magical properties of $F[x_1, \dots, x_n]$ (it is a Noetherian Ring by the Hilbert Basis Theorem), you may always consider the case where the collection is finite.

From the following properties $Z(1) = \emptyset$, $Z(0) = \mathbb{A}^n_F$, $Z(f_1) \cup Z(f_2) = Z(f_1 f_2)$, and $\cap_\alpha Z(f_\alpha) = Z(I(f_\alpha))$, we see that the zero sets form the closed sets of a topology on $\mathbb{A}^n_F$, called the *Zariski topology.* We will call the closed sets of $\mathbb{A}^n_F$ *affine F-varieties*, and the open subsets *quasi-affine F-varieties.*

Note that this definition depends on the embedding. The set $\mathbb{G}_m = \{a \in \mathbb{A}^1, a \neq 0\}$ is a quasi-affine variety since it is an open subset of $\mathbb{A}^1$, but on the other hand the projection $\mathbb{A}^2$ onto $\mathbb{A}^1$ defined by $(x_1, x_2) \mapsto x_1$ maps the closed variety $Z(x_1x_2 - 1)$ bijectively onto $\mathbb{G}_m$, and so $\mathbb{G}_m$ should also be an affine variety. (This variety is labelled $\mathbb{G}_m$ for *groupe multipicatif*, or multiplicative group)

References: [3], [7].

3.1.2. *Projective.* We would like to enlarge our class of objects to include spaces which are not necessarily affine or quasi-affine, but are locally so. This is similar to the world of Topological or Smooth manifolds, where toplogical spaces that can be covered by subspaces which are isomorphic to Euclidean space. The first example one usually sees is projective space, $\mathbb{P}^n$. The points of $\mathbb{P}^n$ are formed by taking the points in $F^{n+1} \setminus \{0\}$, and identifying two points if they are scalar multiples of each other, i.e. if there is a line through the origin connecting both points. We will denote a point of P^n by $[a_0 : \ldots : a_n]$, so that some $a_i \neq 0$, and $[a_0 : \ldots : a_n] = [b_0 : \ldots : b_n]$ if there is a $\lambda \neq 0$ such that $b_i = \lambda a_i$, for all i.

Let $F[t_0, \ldots, t_n]$ be the (graded) polynomial ring, and let f be a homogeneous polynomial (i.e. all the terms are of the same degree). For a given nonzero point $a \in \mathbb{P}^n_F$, it doesn't make sense to evaluate f at a, but it does make sense to ask whether or not $f(a) = 0$, since f is homogeneous. So for a homogeneous ideal I (i.e. one generated by homogeneous polynomials, we will set $Z(I)$ to be the points of $\mathbb{P}^n_F$ vanishing at that ideal. Then, as in the affine case, the sets $Z(I)$ form the closed sets of a topology on $\mathbb{P}^n_F$. Moreover, for $i = 0, 1, \ldots, n$, the map $\phi_i : \mathbb{A}^n_F \to \mathbb{P}^n_F$, where $(a_1, \ldots, a_n) \mapsto [a_1 : \ldots : 1 : \ldots : a_n]$ (the 1 is in the i^{th} spot) is an open embedding of $\mathbb{A}^n_F$ onto the open set $\mathbb{P}^n_F \setminus \{Z(x_i)\}$. So $\mathbb{P}^n$ can be covered by open sets where are all isomorphic to affine space. We call closed subsets of $\mathbb{P}^n_F$ projective varieties, and open subsets of projective F-varieties (NOT just open subsets of $\mathbb{P}^n$) we will call quasi-projective F-varieties).

For any two varieties X and Y, there is a notion of a product variety, which is obvious in the affine case and easy to understand in the projective case (it uses the Segre Embedding). A morphism of varieties is a polynomial map from one variety to another, and an isomorphism is a morphism with an inverse morphism in the other direction. (This is not the same as a bijective morphism) For a suitably nice variety X, the set of automorphisms form a group $\mathrm{Aut}(X)$, which also has the structure of a variety. (It is an algebraic group!)

3.2. **non-algebraically closed case.** Now let F be a field which is not necessarily algebraically closed (e.g. $\mathbb{Q}$.) If R is any F-algebra and f is a polynomial in n variables with coefficients in F, we can think of f as a polynomial in R, and we can ask whether or not points in R^n vanish at f. So instead of a polynomial f defining a subset of F^n (i.e. an algebraic variety in $\mathbb{A}^n_F$), we think of f defining a subvariety of R^n, for all possible F-algebras R. For any F-variety X and F-algebra R, we will denote the solutions of X in R by $X(R)$.

As a concrete example, let $F = \mathbb{Q}$, and let $f_1 = x^2 + 1$, and $f_2 = 1$, as polynomials in one variable x. Both polynomials do not vanish on the variety $\mathbb{A}^1_F$, but the first polynomial does vanish over any F-algebra that contains a square root of -1, so we would think of these polynomials as defining different varieties. This is a very sketchy example of what's called the *functor of points.*

References: Chapter 1 of [5]

3.2.1. *forms.* Let X be an F-variety. If K is a field extension of F, then we can define the K-variety X_K, naively by taking the same polynomials which defined X and considering them as polynomials over K. If X and Y are two F-varieties such that $X_{\overline{F}}$ is isomorphic to $Y_{\overline{F}}$, then we say that X and Y are *forms* of each other. The example that I care about the most are *Severi-Brauer varieties.* A Severi-Brauer variety X is a projective F-variety such that $X_{\overline{F}}$ is isomorphic to $\mathbb{P}^n_{\overline{F}}$, for some n.

Here is an example relevant to the wonderful world of quadratic forms: let $F = \mathbb{R}$, $X = Z(x^2+y^2-1)$, and $Y = Z(xy-1)$, both considered as subvarieties of $\mathbb{A}^2_{\mathbb{R}}$. Then over $\mathbb{C}$, $x^2 + y^2 - 1 = (x + iy)(x - iy) - 1$, so X and Y are forms of each other.

References: [8]

4. Algebraic groups

An algebraic group is an algebraic variety G such that points of G have a group structure. Examples include $\mathbb{A}^n$ (addition), $\mathbb{G}_m$ (multiplication). This last variety is called a torus, because it plays a similar role the torus in geometry. As another example, take the invertible $n \times n$ matrices over F, and identify two such matrices if they differ by multiplication by a scalar matrix. This defines the AFFINE variety $\mathbf{PGL}_n$, called the *projective general linear group.* Pretty much any reasonable (i.e. semisimple) lie group that you can think of is an algebraic variety.

References: Chapter 6 of [6], [1].

4.1. **group actions.** Let G be an algebraic group and X an algebraic variety. A G-action on X is a morphism (polynomial map) from $G \times X \to X$ such that the points of G act on the points of X. An example is $\mathbb{G}_m$ acting on A^1, by $(t, x) \mapsto tx$. Another example is $(\mathbb{G}_m)^n$ acting on $\mathbb{P}^n_F$, by $(t_1, \ldots, t_n) \times [a_0 : a_1 : \ldots : a_n] \mapsto [a_0 : t_1 a_1 \ldots : t_n a_n]$. Finally, there is an obvious action of $\mathbf{PGL}_{n+1}$ on $\mathbb{P}^n_F$ by the obvious linear multiplication.

4.1.1. *Toric Varieties.* Let T be a form of $\mathbb{G}^n_m$. Such a variety is called an algebraic torus. In the first two examples in the previous section, we have action of tori on a variety X such that X contains an open set Uon which T acts faithfully and transitively. Such a variety is called a Toric Variety. In can be shown that a Toric Variety is determined by two pieces of data: A T-Torsor U, and some combinatorical data called a *fan*.

References: [2], [9].

5. Central simple algebras

A *central simple F-algebra* is a non-commutative algebra A with center F such that the only two sided ideals are 0 and the algebra A. The basic example is the ring of $n \times n$ matrices. If furthermore every non-zero element of A is invertible, we say that A is a division algebra. A classical example is the Quaternions. There are a few main results, worth mentioning. The first is due to Wedderburn. He showed that every simple algebra A is isomorphic to the ring of $m \times m$-matrices over some division algebra D, and that m and D are uniquely determined by A. If A and $B$are two central simple algebras, we say that A and B are *Brauer-equivalent* if they are matrix rings over the same division algebra D. In addition, if A and B are two central simple algebras, so is their tensor product $A \otimes_F B$. Thus we may define a group operation on the Brauer-equivalence classes, by $[A] \cdot [B] = [A \otimes_F B]$. This is called the Brauer group of F, denote $\mathrm{Br}(F)$, and is an important algebraic invariant which arises in number theory and algebraic geometry.

If K is a field extension of F and A a central simple F-algebra, then $A \otimes_F K$ is a central simple K-algebra. Moreover, any central simple algebra over an algebraically closed field is a matrix algebra. Thus, $A \otimes_F \overline{F}$ and $M_n(\overline{F})$ are isomorphic as $\overline{F}$-algebras. In fact the converse is true: If A is an F-algebra such that $A \otimes_F \overline{F}$ is isomorphic to $M_n(\overline{F})$, then A is a central simple F-algebras. Finally, the Skolem-Noether Theorem says that any automorphism of A is given by conjugating by an invertible element. In particular, $\mathrm{Aut}(M_n(F)) = \mathbf{PGL}_n(F)$.

References: [4], [6].

6. Galois Cohomology

Let $\Gamma = \mathrm{Gal}(\overline{F}/F)$ be the Galois group, and let G be an algebraic F-group. A 1-cocycle of Γ with coefficients in G is a map $\Gamma \to G(\overline{F})$, $\gamma \mapsto g_\gamma$, such that $g_{\gamma\gamma'} = g_\gamma \gamma(g_{\gamma'})$, where elements of Γ act on $G(\overline{F})$ by acting on the $\overline{F}$ valued points in $G(\overline{F})$. Two 1-cocycles a, a' are said to be *cohomologous* if there is some $b \in G(\overline{F})$ such that $a'_\gamma = b^{-1} a_\gamma \gamma(b)$ for every $\gamma \in \Gamma$. This defines an equivalence relation on the set of cocycles, and we call the set of equivalence classes the first cohomology group, which we label $H^1(F, G)$. There is an obvious trivial 1-cocycle, which maps Γ to the identity element of $G(\overline{F})$. If G is not abelian, than $H^1(F, G)$ is not a group, but merely a pointed set, i.e. a set with a distinguished element, the equivalence class of the trivial 1-cocycle.

The handy thing about Galois cohomology is the long exact sequence induced a short exact sequence of algebraic groups. If $1 \to G \to G' \to G'' \to 1$ is a short exact sequence of algebraic groups (i.e. short exact on the level of $\overline{F}$

points), then there is a connecting homomorphism from $\delta : G''(F) \to H^1(F, G)$ such that we get the following long exact sequence:

$$1 \to G(F) \to G'(F) \to G''(F) \to H^1(F, G) \to H^1(F, G') \to H^1(F, G'').$$

Here is the important fact that we will need to know about H^1:

Theorem 6.1. *If X an algebraic F-variety There is a 1 - 1 correspondence between the following two sets:*

- *forms of X*
- *elements of $H^1(F, \mathrm{Aut}(X_{\overline{F}}))$*

I will show how to get a cocycle from a form of X. Let Y be a form of X, so that there is an isomorphism $\phi : X_{\overline{F}} \to Y_{\overline{F}}$. The group Γ acts on both $X_{\overline{F}}$ and $Y_{\overline{F}}$ by acting on the coordinates. Pick $\gamma \in \Gamma$, and consider the following (not necessarily commutative) diagram:

$$\begin{tikzcd} X_{\overline{F}} \arrow[r, "\phi"] \arrow[d, "\gamma"] & Y_{\overline{F}} \arrow[d, "\gamma"] \\ X_{\overline{F}} \arrow[r, "\phi"] & Y_{\overline{F}}. \end{tikzcd}$$

In this diagram all arrows are isomorphisms. The composite $\phi^{-1}\gamma^{-1}\phi\gamma \in \mathrm{Aut}(X_{\overline{F}})$ is not necessarily the identity (it is if the diagram is commutative.) The assignment $\gamma \mapsto \phi^{-1}\gamma^{-1}\phi\gamma$ defines a 1-cocycle of Γ with coefficients in $\mathrm{Aut}(X_{\overline{F}})$.

References: Chapter 7 of [6], [8].

7. Blow Up

The Blow Up is a process on a variety X which replaces a point x with the tangent spaces of directions at x, without effecting any other part of the variety. Here is an awesome picture of the blow up of $\mathbb{P}^2$ at three points:

The map $p^1 : \widetilde{S} \to \mathbb{P}^2$ is the blow up at the three points defined by the intersection of any pair of the three lines. The inverse image of each point is a line in $\widetilde{S}$ (the lines m_0, m_1, and m_2), and the lines connecting these three points pull back to the three lines l_0, l_1, and l_2.

References: Chapter 5 of [3], [7]

References

[1] A. Borel, *Linear Algebraic Groups* Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991.

[2] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, 131, Princeton University Press, Princeton, NJ, 1993.

[3] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[4] I. Herstein, *Non-commutative Rings*, The Carus Mathematical Monographs, No. 15 Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York 1968.

[5] J. Jantzen, *Representations of algebraic groups*, Second Edition, Mathematical Surveys and Monographs, 107. American Mathematical Society, Providence, RI, 2003.

[6] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The Book of Involutions*, American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.

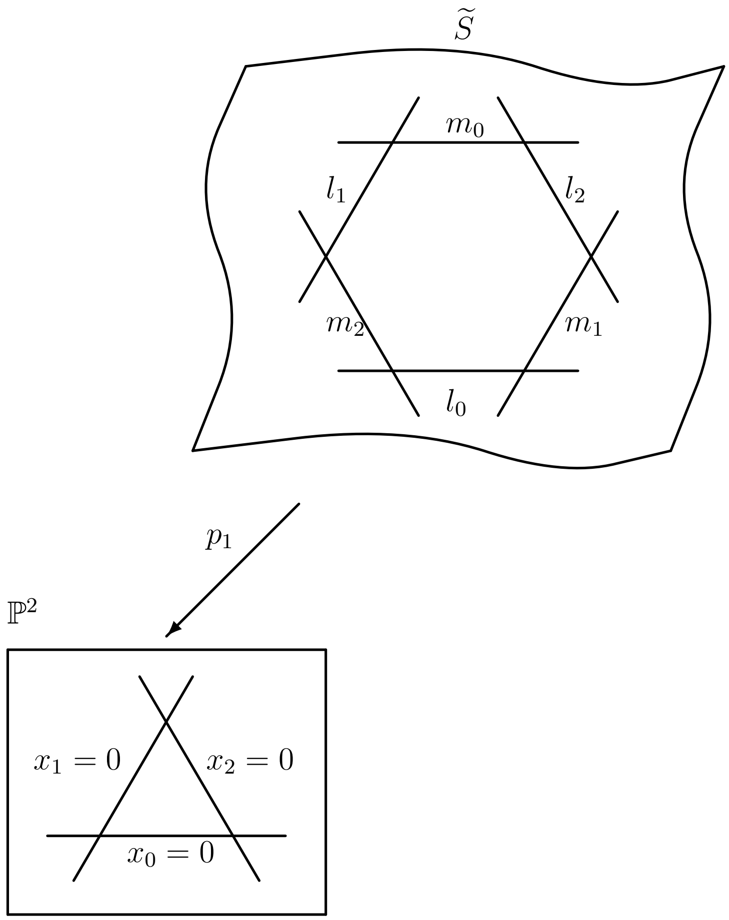

FIGURE 1. The Hexagon of Lines.

[7] I. Shafarevich, *Basic Algebraic Geometry I*, Springer-Verlag (1994).
[8] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion.
[9] V. E. Voskresenskiĭ, *Projective invariant Demazure models*, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), no. 2, 195–210.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CA 90095-1555
E-mail address: mblunk@math.ucla.edu