FIELDS OF DEFINITION OF RATIONAL POINTS ON VARIETIES

JORDAN RIZOV

Abstract. Let X be a scheme over a field K and let M_X be the intersection of all subfields L of $\bar{K}$ such that X has a L-valued point. In this note we prove that for a variety X over a field K finitely generated over its prime field one has that $M_X = K$.

Let K be a field and fix an algebraic closure $K \subset \bar{K}$. For a scheme X over K denote by $\mathscr{C}_X$ the collection of all fields $K \subset L \subset \bar{K}$ such that X has a L-valued point $x\colon \operatorname{Spec}(L) \to X$. Define the field M_X as

$$M_X = \bigcap_{L \in \mathscr{C}_X} L$$

where the intersection takes place in $\bar{K}$. We will be interested in how big M_X can be and in particular in some cases in which it is K itself.

If the set of K-rational points $X(K)$ is non-empty, then obviously M_X is K. In general, if K is a perfect field and X is a scheme of finite type over K then M_X is a finite Galois extension of K. Indeed, let $x\colon \operatorname{Spec}(L) \to X$ be a L-valued point on X corresponding to a point x on the topological space X and an inclusion $\kappa(x) \to L$ where $\kappa(x) = \mathcal{O}_x/\mathfrak{m}_x$ is the residue field of x (see [Har77, Ch. II, §2, Exercise 2.7] and [Mum88, Ch. II, §4, Prop. 3]). For any $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/K)$ one has the conjugate x^σ of x which is a $\sigma(L)$-valued point on X. Hence for any field $L \in \mathscr{C}_X$ and any $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/K)$ the field $\sigma(L)$ is also in $\mathscr{C}_X$ which implies that M_X/K is a Galois extension.

Remark 1. Suppose given two schemes X_1 and X_2 defined over K and a morphism $f\colon X_1 \to X_2$ over K. Then one has that $\mathscr{C}_{X_1} \subset \mathscr{C}_{X_2}$ and therefore $M_{X_2} \subset M_{X_1}$. In particular if $M_{X_1} = K$, then the field M_{X_2} is K, as well.

Before going on let us consider some illuminating examples under different conditions imposed on X and K.

Example 2. If we take X to be $\operatorname{Spec}(K)$, then clearly $M_X = K$.

Example 3. Consider the curve $X\colon x^2+y^2+z^2 = 0$ in $\mathbb{P}^2$ over $\mathbb{Q}$ (i.e. $K = \mathbb{Q}$). One can take $P_1 = [i : 0 : 1]$ which has field of definition $\mathbb{Q}(i)$ and the point $P_2 = [\sqrt{-2} : 1 : 1]$ giving the field $\mathbb{Q}(\sqrt{-2})$. Clearly, the intersection of those two fields is $\mathbb{Q}$, so $M_X = \mathbb{Q}$. This is an example where X is a non-singular, projective curve of genus 0 over $\mathbb{Q}$ with no $\mathbb{Q}$-rational point.

I thank Ben Moonen, Frans Oort, Andrea Giacobbe, Ivan Chipchakov and Grigor Grigorov for stimulating discussions.

Example 4. Let $K = \mathbb{F}_q$ be a finite field and let X be a non-singular, quasi-projective curve over K. We may assume that X is contained in its complete, non-singular model X' over K. Let $X = X' \setminus \{P_1, \dots, P_r\}$ (the complete case is treated in the same way) and denote the genus of X' by g. If $n \in \mathbb{N}$ and N_{q^n} denote the number of $\mathbb{F}_{q^n}$ rational points on X' then by the Weil bound we have that

$$N_{q^n} \geq 1 + q^n - 2g\sqrt{q^n}.$$

Therefore, if n is sufficiently large one has that $N_{q^n} \geq r + 1$ and hence $X(\mathbb{F}_{q^n})$ is not empty. Choose two natural numbers n_1 and n_2 which are sufficiently large so that $X(\mathbb{F}_{q^{n_i}})$ is not empty for $i = 1, 2$ and $\gcd(n_1, n_2) = 1$. Then we have that

$$M_X \subset \mathbb{F}_{q^{n_1}} \cap \mathbb{F}_{q^{n_2}} = \mathbb{F}_q$$

and hence $M_X = K$.

Example 5. Consider again the curve $X\colon x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2$ but take this time K to be $\mathbb{R}$. Then we have that M_X is $\mathbb{C}$ since X has no $\mathbb{R}$-valued points.

Example 6. Take $K = \mathbb{Q}$ and consider the polynomial $f(x) = x^3 - 7x + 7$. It is irreducible over $\mathbb{Q}$ since it has no rational zeros. Let $\alpha = \alpha_1, \alpha_2$ and α_3 be its roots. Since the discriminant of $f(x)$ is 7^2 its Galois group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and the field $M = \mathbb{Q}(\alpha)$ is a Galois extension of $\mathbb{Q}$ of degree 3. Let $P_i = (\alpha_i, \alpha_i^2)$ for $i = 1, 2, 3$ be three points in $\mathbb{A}^2_{\bar{\mathbb{Q}}}$ and consider the three lines passing through them:

$$\begin{aligned} l_1 &= y - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 = 0 \quad \text{passing through } P_1 \text{ and } P_2;\\ l_2 &= y - (\alpha_1 + \alpha_3)x + \alpha_1\alpha_3 = 0 \quad \text{passing through } P_1 \text{ and } P_3;\\ l_3 &= y - (\alpha_2 + \alpha_3)x + \alpha_2\alpha_3 = 0 \quad \text{passing through } P_2 \text{ and } P_3. \end{aligned}$$

Define the scheme $X \subset \mathbb{A}^2_{\bar{\mathbb{Q}}}$ to be given by the equation $l_1 l_2 l_3 = 0$. The Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ permutes the three points P_1, P_2 and P_3 and respectively the three lines l_1, l_2 and l_3 in $\mathbb{A}^2_{\bar{\mathbb{Q}}}$. Hence X is defined over $\mathbb{Q}$ and it is irreducible over $\mathbb{Q}$.

Let $P\colon \mathrm{Spec}(L) \to X$ be a L-valued point on X for some field $L \subset \bar{\mathbb{Q}}$. If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/L)$, then it fixes the point P on $X_{\bar{\mathbb{Q}}}$. Since an automorphism in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, acting on $\mathbb{A}^2_{\bar{\mathbb{Q}}}$, permutes the three lines we see that, acting on $X_{\bar{\mathbb{Q}}}$, it has fixed points if and only if it acts as the trivial permutation on $\{l_1, l_2, l_3\}$. Hence σ must leave the points P_i, $i = 1, 2, 3$ fixed and therefore M, as well. Thus we conclude that $M \subset L$. Since X has M-valued points (the points P_i for $i = 1, 2, 3$) we have that $M_X = M = \mathbb{Q}(\alpha)$.

In this example one can take $f(x)$ to be any irreducible polynomial over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

The last two examples suggest that if the field of definition K is 'too big' or the scheme X is somehow 'too bad' then the field M_X is a non-trivial extension of K. On the other hand the argument given in example 3 can be easily generalized to number fields and other curves.

Before stating the main result let us make the following convention: In this note a variety X over a field K will mean a separated, geometrically integral scheme X of finite type over K. In particular, X is geometrically irreducible. Also from now on we will assume that K is a finitely generated field over its prime field. We know that for those fields Faltings' finiteness theorem holds (see [Lan91, Ch. I, §2]). Further, if char(K)= 0 or if char(K)= p and $\mathrm{tr.deg}_{\mathbb{F}_p} K \geq 1$, then Hilbert's irreducibility theorem holds for the field K. We refer to [Lan83, Ch. 9] and more precisely to Theorem 4.2 and the remark following it.

Theorem 7. *Let K be a finitely generated field over its prime field and let X be a variety over K. Then one has that $M_X = K$.*

Proof. **Step 1.** We will first show that it is enough to consider non-singular, quasi-projective varieties. If X is not complete, then by Nagata's compactification theorem one can find a complete variety $\bar{X}$ and an open immersion $i\colon X \hookrightarrow \bar{X}$. By Chow's Lemma there exits a projective variety Y' over K and a birational isomorphism $\pi'\colon Y' \to \bar{X}$. Let Y be an alteration of Y' (see [dJ96, §1 and §4, Thm. 4.1]), let $\pi\colon Y \to \bar{X}$ be the composition morphism and let $X' = \pi^{-1}(i(X))$. Then by Remark 1 we have that $M_X \subset M_{X'}$. Hence it is enough to show the validity of the theorem assuming that X is a non-singular, quasi-projective variety over K.

We may assume that $X \subset \mathbb{P}^N$ for some N. In the next two steps we will show here that it is enough to prove the theorem assuming that $\dim X = 1$.

Step 2. Suppose that K is an infinite field. If $\dim X = 1$ then the result follows from Proposition 8 below. Suppose that $\dim X = m \geq 2$. Then by Bertini's Theorem ([Har77, Ch. II, §8, Thm. 8.18)]) we know that the set U of points u in the dual projective space $\check{\mathbb{P}}^N$ corresponding to hyperplanes $H \subset \mathbb{P}^N_{\kappa(u)}$ such that $H \cap X$ is smooth of dimension $m-1$ over the residue field $\kappa(u)$ of u contains a dense open subset of $\check{\mathbb{P}}^N$. Since K is infinite the intersection $U \cap \check{\mathbb{P}}^N(K)$ is non-empty. Hence one can find a hyperplane H defined over K satisfying Bertini's Theorem. Further, by [Har77, Ch. III, §11, Exercise 11.3] the intersection $H \cap X$ is geometrically connected and hence it is geometrically irreducible or in other words it is a quasi-projective variety of dimension $m-1$ over K. Repeating this $\dim X - 1$ times one can find a non-singular, quasi-projective curve $Y \subset X$ defined over K. By Remark 1 one has that $M_X \subset M_Y$. Now the claim follows from Proposition 8 below.

Step 3. Let K be a finite field. The case $\dim X = 1$ was considered in example 4. Assume that $\dim X \geq 2$. We will find again a quasi-projective curve defined over K contained in X by intersecting X with hypersurfaces. By Theorem 3.3 and Remarks (1) and (2) in [Poo] there exists a geometrically integral, smooth hypersyrface $H \subset \mathbb{P}^N$ defined over K such that the intersection $X \cap H$ is a smooth variety of dimension $\dim X - 1$. Repeating this $\dim X - 1$ times we can find a non-singular, quasi-projective curve Y in X defined over K. Then just like in Step 2 we conclude the claim from Remark 1 and example 4. □

Proposition 8. *Let K be an infinite field which is finitely generated over its prime field. If X is a quasi-projective curve defined over K, then $M_X = K$.*

Proof. We will split up the proof into three steps.

Step 1. Assume that X is a complete, non-singular curve of genus at least 2 and there is a morphism $f\colon X \to \mathbb{P}^1$ over K of prime degree p. Hilbert's irreducibility theorem assures that there are infinitely many points $P \in \mathbb{P}^1(K)$ such that the fiber $f^{-1}(P) = \{Q_1, \ldots, Q_r\}$ consists of points which are defined over extensions $K(Q_i)$ of K of degree p. If among all those fields (for all points $P \in \mathbb{P}^1(K)$ as above), there are two which are different, then their intersection will be K (as they do not have non-trivial subfields). Hence we would have that $M_X = K$. Assume that all fields $K(Q_i)$ for all $P \in \mathbb{P}^1(K)$ as before are the same. Then we have infinitely many points on X defined over a fixed extension $L = K(Q_i)$ of K. As X is of genus at least 2 we get a contradiction with Faltings' finiteness theorem. Thus we conclude that M_X is K in this case.

Step 2. Now assume that X is complete and non-singular. In general, one should not expect to be able to find a morphism as in Step 1. Instead, we will construct a covering $\pi\colon X' \to X$ over K for some curve X' satisfying the assumptions of Step 1. Then we could conclude the claim of the proposition using Remark 1. Such a curve can be viewed as a divisor on $X \times \mathbb{P}^1$ so we will look at special divisors on this ruled surface.

Let a be a natural number which we will fix later and consider the divisor $D(a) = 2X + a\mathbb{P}^1$ on $X \times \mathbb{P}^1$. Following the notations of [Har77, Ch V, §2] we put $(X, X)_{X\times\mathbb{P}^1} = -e$. Then using Proposition 2.3, Lemma 2.10 and Corollary 2.11 of [Har77, Ch. 5, §2], one sees that

$$(D(a), X) = (2X + a\mathbb{P}^1, X) = a - 2e$$

and the 'adjunction formula' for the divisor $D(a)$ has the form

$$(D(a), D(a) + K_{X\times\mathbb{P}^1}) = 2a + 2(2g_X - 2 - e)$$

where $K_{X\times\mathbb{P}^1}$ is the canonical class of $X \times \mathbb{P}^1$. Let us choose a so that

$$\begin{aligned} a &> 2e \\ a &- 2e \qquad\qquad \text{is a prime number} \\ a + (2g_X &- 2 - e) \geq 1. \end{aligned}$$

The first condition ensures that the linear system $|D(a)|$ contains a non-singular, geometrically irreducible curve X' defined over K. Indeed, one uses [Har77, Ch. V, §5, Cor. 2.18]. Hartshorne assumes that K is algebraically closed. Since the proof only deals with very ample line bundles and uses Bertini's Theorem [Har77, Ch. II, §8, Thm. 8.18] and [Har77, Ch. III, §11, Exercise 11.3] it remains valid over K, as K is an infinite field.

The degree of the morphism $f\colon X' \hookrightarrow X \times \mathbb{P}^1 \to \mathbb{P}^1$ is exactly $(X', X) = a - 2e$ which is a prime number and by the adjunction formula the genus of X' is $a + (2g_X - 2 - e) + 1$ which is at least 2 by our choice. Hence X' satisfies the conditions of Step 1. Therefore by Remark 1 we conclude that $M_X = M_{X'} = K$.

Step 3. Let X be as in the proposition. If it is not complete one can find a completion X' of X which is also defined over K. Take the normalization X'' of X' and let $\tilde{X} \subset X''$ be the preimage of X. The curve X'' is non-singular, projective and defined over K. One can now apply Step 1 and 2 above to X''. Clearly those proofs, and more precisely the one of Step 1, can be carried over excluding a finite number of points (which of course should not change the field of definition K). In other words one sees that $M_{\tilde{X}} = K$. Hence by Remark 1 we have that $M_X \subset M_{\tilde{X}} = K$ and therefore $M_X = K$. □

Remark 9. Note that thought we distinguished the two cases K is finite and K is infinite the two proofs go exactly in the same lines. One tries to find finite extensions L_1 and L_2 of K which are 'different' as subfields of $\bar{K}$, such that $X(L_i)$ is not empty for $i = 1, 2$ and so that one can control the intermediate fields $K \subset M \subset L_i$. In the case K is finite this is easily achievable using the Weil bound. If K is infinite one makes use of Hilbert's irreducibility theorem instead. Below we shall present a proof based on a completely different idea. Namely, in the case K is a number field one tries to find sufficiently many prime ideals of K splitting completely in M_X. This proof was suggested to us by Grigor Grigorov.

Let K be a number field and let $\mathcal{O}_K$ be the ring of integers in K. For a prime ideal $\mathfrak{p}$ of K denote by $k_\mathfrak{p}$ the residue field $\mathcal{O}_K/\mathfrak{p}$. Let $q_\mathfrak{p}$ be the number of elements in $k_\mathfrak{p}$. Then by definition one has that the norm $N(\mathfrak{p})$ of $\mathfrak{p}$ is $q_\mathfrak{p}$. Denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$ and let $\mathcal{O}_{K_\mathfrak{p}}$ be ring of integers in $K_\mathfrak{p}$.

Proof of Proposition 8 *assuming that K is a number field.* We already saw that one can assume that X is non-singular and it is contained in its complete non-singular model X' defined over K. We have that $X = X' \setminus \{P_1, \dots, P_m\}$ for some $m \in \mathbb{N}$ (the proof in the complete case is the same). Take a projective embedding of X' over K in to $\mathbb{P}^N_K$ for some N and its flat closure $\mathcal{X}'$ over $\mathcal{O}_K$ in $\mathbb{P}^N_{\mathcal{O}_K}$. Let $\mathcal{X}$ be the complement $\mathcal{X}' \setminus \{\mathcal{P}_1, \dots, \mathcal{P}_m\}$ where $\mathcal{P}_i$, $i = 1, \dots, m$, is the flat closure of P_i over $\mathcal{O}_K$. Then there is a finite set of primes Σ such that $\mathcal{X}'$ is smooth over $U = \mathrm{Spec}(\mathcal{O}_K) \setminus \Sigma$. For a prime ideal $\mathfrak{p} \notin \Sigma$ let $N_\mathfrak{p}$ be the number of points in $\mathcal{X}'(k_\mathfrak{p})$. The Weil bound reads

$$N_\mathfrak{p} \geq 1 + q_\mathfrak{p} - 2g\sqrt{q_\mathfrak{p}}.$$

where g is the genus of X'. Hence if $q_\mathfrak{p} = N(\mathfrak{p})$ is sufficiently large one has that $N_\mathfrak{p} \geq m + 1$. So enlarging Σ, if needed, we may assume that $\mathcal{X}(k_\mathfrak{p})$ is not empty for all $\mathfrak{p} \notin \Sigma$.

Fix a prime ideal $\mathfrak{p} \notin \Sigma$. Since $\mathcal{X}$ is smooth over U and $\mathcal{X}(k_\mathfrak{p})$ is non-empty one can apply Hensel's lemma (see [BLR90, §2.3, Prop. 5]) to conclude that $X(K_\mathfrak{p})$ is non-empty. Therefore by Theorem 1.3 in [MB89] one can find a finite extension L of K such that $\mathfrak{p}$ splits completely in L and X has a L-valued point. Hence $\mathfrak{p}$ splits completely in M_X. Thus all but finitely many ideals (at most those in Σ) split completely in M_X. By Corollary 6.6 in [Neu86, Ch. V, §6] we have that $M_X = K$. □

Remark 10. Theorem 7 could be viewed as a variant of Theorem 5.1 in [Del71, §5] where Deligne proves that for a Shimura datum (G, X) and any finite extension L of the reflex field $E(G, X)$ of the Shimura variety $Sh(G, X)$ there exists a special point x on X such that its reflex field $E(x)$ is linearly disjoint from L. This result is used in proving the uniqueness of the canonical model of $Sh(G, X)$ over $E(G, X)$. We came across the main result of this note considering a similar descent problem.

How big can M_X be in general? We already saw in examples 5 and 6 that depending on X and K the field M_X can be a non-trivial extension of K. Using the construction in example 6 one can find X over $\mathbb{Q}$ such that $[M_X : \mathbb{Q}]$ is arbitrary large. On the other hand if X is a non-singular, projective curve defined over a field K, then $l(K_X) = g$, where g is the genus of X and K_X is its canonical class. If $g \geq 2$ then there is a non-constant K-rational function f in $L(K_X)$. It gives a morphism $f\colon X \to \mathbb{P}^1$ of degree at most $\deg K_X = 2g - 2$. Hence there is a L-valued point for some extension L/K with $[L : K] \leq 2g - 2$. Therefore we have that $[M_X : K] \leq 2g - 2$.

References

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Springer-Verlag, 1990.
[Del71] P. Deligne, *Travaux de Shimura*, Sém. Bourbaki **LNM 244** (1971), 123–165.
[dJ96] A. J. de Jong, *Smoothness, Semi-stability and Alterations*, Publ. Math de I.H.E.S. **83** (1996), 51–93.
[Har77] R. Hartshorne, *Algebraic Geometry*, GTM, vol. 52, Springer-Verlag, New-York, 1977.
[Lan83] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New-York, 1983.
[Lan91] ———, *Numbert Theory III*, Encyclopedia of Mathematical Sciences, vol. 60, Springer-Verlag, 1991.
[MB89] L. Moret-Bailly, *Groupes de Picard et Problémes de Skolem II*, Ann. Sciet. Éc. Norm. Sup. **22** (1989), 181–194.
[Mum88] D. Mumford, *The Red Book of Varieties and Schemes*, Springer-Verlag, 1988.
[Neu86] J. Neukirch, *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften, no. 280, Springer-Verlag, 1986.
[Poo] B. Poonen, *Bertini Theorems over Finite Fields*, to appear in Annals of Math.

Mathematisch Instituut, P.O. Box 80.010, 3508 TA Utrecht, The Netherlands
E-mail address: rizov@math.uu.nl