Notes on algebraic number theory

Daniel Miller

May 2, 2017

1 Symmetric polynomials and resultants

1.1 Symmetric polynomials

For $r \leqslant n$, the rth *elementary symmetric polynomial* in n variables is defined by

$$s_r(X_1, \dots, X_n) = \sum_{i_1 \leqslant \cdots \leqslant i_r} X_{i_1} \cdots X_{i_r}$$

It is easy to see that s_r is invariant under permutation of the X_i. In fact, s_r is (up to a factor of ± 1) the coefficient of X^r in the product

$$(X - X_1) \cdots (X - X_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$$

Now let A be a commutative ring, and let S_n act on $A[X_1, \dots, X_n]$ by $\sigma X_i = X_{\sigma i}$.

Theorem 1.1.1. *The map $A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]^{S_n}$ given by $X_i \mapsto s_i$ is a ring isomorphism.*

1.2 Resultants

Definition 1.2.1. *Let A be a commutative ring, $f, g \in A[X]$. The* resultant *of f and g, written $R(f, g)$, is the determinant of the matrix*

$$\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \cdots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0 \end{pmatrix} \in M_{m+n}(A)$$

where $f = \sum a_i X^i$ and $g = \sum b_i X^i$.

The following theorem is fundamental.

Theorem 1.2.2. *Let k be a field with $f, g \in k[X]$. Let $s_1, \dots, s_n$ be the roots of f, $t_1, \dots, t_m$ be the roots of g, with multiplicities. Then*

$$R(f, g) = a_n^m b_m^n \prod_{i,j} (s_i - t_j)$$

Proof. This is Theorem 1.6 of [2]. □

As a corollary, we see that if f is a polynomial, then f is separable if and only if $R(f, f') \neq 0$, so that separable polynomials of fixed degree are dense (open, in fact) in the Zariski topology.

2 Field extensions

If k is a field, $\bar{k} = k^a$ denotes a fixed algebraic closure of k. We will write $G_k = \mathrm{Gal}(\bar{k}/k)$ for the absolute Galois group of k.

2.1 Separability

If k is a field, k^s denotes the separable closure of k. We will also write G_k for $\mathrm{Gal}(k^s/k)$, since this is canonically isomorphic to $\mathrm{Gal}(\bar{k}/k)$.

Theorem 2.1.1. *Let k be a field, K/k a (not-necessarily algebraic) extension such that $K \cap k^s = k$. If $f \in k[X]$ is irreducible and separable, then f is also irreducible over K.*

Proof. Suppose $f = gh$ over K. Since the roots of f are all separable over k, we have $g, h \in k^s[X]$. But also $g, h \in K[X]$, so $g, h \in k[X]$, which forces one of f, g to be a unit. □

3 Valuations

3.1 Definitions and notation

Definition 3.1.1. *Let k be a field. A* valuation *on k is a homomorphism $v : k^\times \to \Gamma$, where Γ is a totally-ordered abelian group, such that $v(x + y) \geqslant \inf\{v(x), v(y)\}$ for all $x, y \in k^\times$.*

If $v : k^\times \to \Gamma$ is a valuation, we call $\Gamma_v = v(k^\times)$ the *value group* of v. We say that two valuations v, w are *equivalent* if there is an isomorphism of ordered groups $f : \Gamma_v \to \Gamma_w$ such that $f \circ v = w$. We will often regard equivalent valuations as identical. If $k \subset K$ are fields with valuations v, w, we say that w *divides* v, and write $w \mid v$, if $w|_k = v$. The *rank* of a valuation is defined to be

$$\mathrm{rk}(v) = \mathrm{rk}_{\mathbb{Z}}(\Gamma_v \otimes \mathbb{Q}).$$

We will generally consider valuations of rank one, in which case we will tacitly assume the value group is a subgroup of $\mathbb{Q}$.

Definition 3.1.2. *Let v be a valuation on k. Set*

- $k^\circ = \{x \in k : v(x) \geqslant 0\}$, *the* ring of integers,
- $k^+ = \{x \in k : v(x) > 0\}$, *the* maximal ideal,
- $k^\natural = k^\circ / k^+$, *the* residue field,
- $k^\wedge$, *the* completion.

If two of these operations are applied successively, no parentheses will be used – one should interpret the leftmost as being applied first, the rest in order from left to right. For example, $k^{\wedge+}$ denotes the unique maximal ideal in the ring of integers of $k^\wedge$.

The *residue characteristic* of k is the characteristic of $k^\natural$. We say that k is *mixed characteristic* if k has characteristic zero and $k^\natural$ has positive characteristic.

3.2 Extensions of valuations

Theorem 3.2.1. *Let k be a field with valuation v, K/k a field extension. Then there is a valuation w on K with $w \mid v$.*

Proof. This is [1, III.4.3 pr.5]. $\square$

Throughout this section, k will be a field with valuation v, and K/k will be an extension, with a valuation $w \mid v$ on K. If $\sigma \in \mathrm{Gal}(K/k)$, then $w^\sigma(x) = w(\sigma x)$. One readily verifies that this induces a right action of $\mathrm{Gal}(K/k)$ on the valuations of K above v. The stabilizer is the *decomposition subgroup*:

$$D_w = \{\sigma \in \mathrm{Gal}(K/k) : w^\sigma = w\}$$

There is a natural map $D_w \to \mathrm{Gal}(K^\natural/k^\natural)$. For $\sigma \in D_w$, define $\bar{\sigma}$ on $K^\natural$ by $\bar{\sigma}(\bar{x}) = \overline{\sigma x}$; this is well-defined because $\sigma \in D_w$. The kernel of this map is called the *decomposition subgroup*

$$I_w = \ker\left(D_w \to \mathrm{Gal}(K^\natural/k^\natural)\right)$$

If w is a "canonical" extension of v to K, or if the choice of such an extension does not matter, we will sometimes write D_v and I_v instead of D_w and I_w. If K has not been given, D_v and I_v denote the subgroups of G_k induced by some extension of v to k^s. Such an extension exists by 3.2.1.

3.3 Ramification and inertia

Definition 3.3.1. *Let k be a field with valuation v, and K an extension with $w \mid v$. Define the* ramification index *by $f = f_{w/v} = [\Gamma_w : \Gamma_v]$.*

Definition 3.3.2. *Let k be a field with valuation v, and K an extension of k with valuation $w \mid v$. The* inertia degree *of K/k is $e = e_{w/v} = [K^\natural : k^\natural]$.*

3.4 Henselian fields and rings

Theorem 3.4.1. *For a field k with valuation, the following are equivalent:*

1. *Any finite k°-algebra is a direct product of local rings.*
2. *If $f \in k^\circ[X]$ is monic, then for every factorization $f = g_0h_0$ where $g_0, h_0 \in k^\natural[X]$ are relatively prime, there exist monic $g, h \in k^\circ[X]$ with $f = gh$ and $\bar{g} = g_0, \bar{h} = h_0$.*
3. *If K/k is an algebraic extension, then the valuation on k admits a unique extension to K.*

Proof. The equivalence $1 \Leftrightarrow 2$ is [1, III.4 ex.3], while $2 \Leftrightarrow 3$ is [3, II.6.6]. $\square$

Definition 3.4.2. *A valued field k is* henselian *if any of the conditions of the previous theorem hold.*

We will often say "let k be a henselian field" with the valuation assumed. This will note generally cause harm because by [3, II.6 ex.3], a field that is henselian with respect to two inequivalent valuations is already separably closed. If k is a henselian field and K/k is an algebraic extension, we will generally assume that K is equipped with the unique valuation extending that of k.

Theorem 3.4.3. *Let k be a field that is complete with respect to a valuation. Then k is henselian.*

Proof. This is [1, III.4.3 th.1]. $\square$

Theorem 3.4.4. *Let $\{A_\alpha\}$ be a directed system of Henselian rings and local homomorphisms. Then the direct limit $\varinjlim A_\alpha$ is also Henselian.*

Proof. This is [1, III.4 ex.3(a)]. $\square$

Lemma 3.4.5. *Let k be a henselian field, K/k an algebraic extension. Then K° is the integral closure of k° in K.*

Proof. If $x \in K^\circ$, then all the conjugates of x over k are also in K°, hence the minimal polynomial of x is in $k^\circ[X]$, i.e. x is integral over k°. Conversely, if x is integral over k°, let $f = X^n + \cdots + a_0$ be the minimal polynomial of x. From the fact that $v(a_i) \geqslant 0$ for all i, we deduce that $v(x) \geqslant 0$, i.e. $x \in K^\circ$. □

Corollary 3.4.6. *Let k be a henselian field, K/k an algebraic extension. Then K is also henselian.*

Proof. This follows easily from [1, III.3 ex.3(c)], which states that a local integral extension of a henselian ring is henselian. Use 3.4.5 to note that K° is integral over k°. □

3.5 Completion and algebraic closure

Let v be a valuation on a field k, and let σ be an automorphism of k. We define v^σ by $v^\sigma(x) = v(\sigma x)$. It is easy to see that this gives a right action of $\mathrm{Aut}(k)$ on the valuations of k.

We begin with a lemma.

Lemma 3.5.1 (Krasner)**.** *Let k be a henselian valued field, $K = k(x)$ a finite separable extension. If $y \in k^s$ satisfies $v(y - x) > v(y - \sigma x)$ for all $\sigma \in G_k$ with $\sigma x \neq x$, then $k(x) \subset k(y)$.*

Proof. It is equivalent to prove that $G_{k(y)} \subset G_{k(x)}$. If not, then there is some $\sigma \in G_k$ such that $\sigma y = y$ but $\sigma x \neq x$. One then computes

$$v(y - \sigma x) = v(\sigma y - \sigma x) = v(y - x) > v(y - \sigma x),$$

a contradiction. We have $v(\sigma t) = v(t)$ for all $t \in k^s$ because v^σ is also a valuation on k^s extending v, and such valuations are unique by 3.4.1. □

Corollary 3.5.2. *Let k be a henselian field, K/k a finite separable extension. If $k_0 \subset k$ is dense, then $K = k(x)$ for some $x \in k_0^s$.*

Proof. Write $K = k(x)$ for some $x \in k^s$. Let $f \in k[X]$ be the minimal polynomial of x, $n = \deg f$. We interpret elements of affine n-space k^n as degree n monic polynomials via

$$(a_0, \ldots, a_{n-1}) \leftrightarrow X^n + \cdots + a_1 X + a_0 = a \in k[X].$$

Let R denote the resultant (1.2.1), and define $\phi : k^n \to k$ by

$$(a_0, \ldots, a_{n-1}) \mapsto R(X^n + a_{n-1}X^{n-1} + \cdots + a_0, f)$$

This is a polynomial mapping, so it is continuous. Let $N = \sup\{v(x - \sigma x) : x \neq \sigma x\}$. Consider the open set

$$U = \{a \in k^n : a \text{ separable and } v(\phi a) > n^2 N\}$$

Since k_0 is dense in k, $U \cap k_0^n$ is nonempty, so there exists some separable $g \in k_0[X]$ with $v(R(f,g)) > n^2 N$. By 1.2.2, $R(f,g) = \prod(x_i - y_j)$, where x_i runs over the conjugates of x and y_i are the roots of g. Note further that

$$n^2 \sup\{v(x_i - y_j)\}_{i,j} \geqslant v(R(f,g)) > n^2 N,$$

so there exists i, j with $v(x_i - y_j) > N$. After applying some $\sigma \in G_k$, we may assume $x_i = x$. An application of Krasner's lemma (3.5.1) shows that $k(x) \subset k(y_j)$. Since $[k(y_j) : k] \leqslant n$, we actually have equality. □

Corollary 3.5.3. *Let k be a henselian field, $k_0 \subset k$ a dense subfield. One has $k^s = k \cdot k_0^s$.*

Corollary 3.5.4. *If k is henselian, $k_0 \subset k$ is dense, then k_0^s is dense in k^s.*

Proof. Let $x \in k^s$. The field $K = k(x)$ has finite degree n over k, so by 3.5.2, $K = k(y)$ for some $y \in k_0^s$. It easily follows that $k_0(y)$ is dense in K. So, if $U \subset k^s$ is an arbitrary open set with $x \in U$, $U \cap K$ is open, so there exists $z \in k_0(y) \cap U$, i.e. $U \cap k_0^s \neq \varnothing$. □

Let k be a field with valuation v. The completion $k^\wedge$ of k is henselian by 3.4.3, so the induced valuation on $k^\wedge$ has a unique extension (also denoted v) to $k^{\wedge s}$. At the same time, the map $k \to k^\wedge$ extends to a non-canonical embedding $\iota : k^s \to k^{\wedge s}$. This yields a map $\iota_* : G_{k^\wedge} \to G_k$ given by $\iota_* \sigma = \iota^{-1} \sigma \iota$. Of course, ι^{-1} is not well-defined as a map $k^{\wedge s} \to k^s$, but it is well-defined on the image of ι, which is preserved by $G_{k^\wedge}$. We set, for $x \in k^s$, $v(x) = v(\iota x)$.

Theorem 3.5.5. *Let k be an arbitrary field with valuation v. The homomorphism $\iota_* : G_{k^\wedge} \to G_k$ is a continuous injection with image $G_v = \{x \in G_k : v^\sigma = v\}$.*

Proof. By the definition of ι_*, its image is inside G_v.

It is essentially trivial that ι_* is continuous. For, basic open sets in G_k are translates of stabilizers of elements of k^s, and the preimage of such an open set is just the stabilizer in $G_{k^\wedge}$, which is also open.

First, we prove that ι_* is injective. If $\iota_* \sigma = 1$, then "$\sigma|_{k^s}$" is the identity map. By 3.5.4, k^s is dense in $k^{\wedge s}$, which forces $\sigma = 1$.

Now we prove ι_* is surjective. If $\sigma \in G_v$, then define τ_0 on ιk^s by $\tau_0 = \iota \sigma \iota^{-1}$. Then $\tau_0 \in G_v$, so when restricted to each Galois K/k, τ_0 extends by continuity to the completion $K^\wedge$. Since $k^{\wedge s}$ is the filtered union of the $K^\wedge$, τ_0 extends by continuity to $\tau \in G_{k^\wedge}$, and clearly $\iota_* \tau = \sigma$. □

References

[1] Bourbaki, N. *Commutative algebra.*

[2] Janson, S. *Resultant and discriminant of polynomials*, `http://www2.math.uu.se/~svante/papers/sjN5.pdf`.

[3] Neukirch, J. *Algebraic number theory.*