Separability

Version 1.1 — 24. september 2013 klokken 10:28

Multiple roots and separable polynomials

Let as usual K be a field, and let a polynomial $f \in K[t]$ of degree m is given. It is convenient—and we loose nothing—to suppose that f is monic. Let Ω be a field containing K such that $\omega \in \Omega$ is a root of f. We may then write

$$f(t) = (x - \omega)^r g(x)$$

where $g(x) \in \Omega[t]$ is a polynomial not vanishing at ω and $r \geq 1$. The root is *a simple root* if $r = 1$, and in the contrary case, *i.e.,* if $r \geq 2$, we call ω *a multiple root*. One has the well known and elementary, but usfull lemma

Lemma 1 *The root ω is multiple if and only if $f'(\omega) = 0$.*

PROOF: The product rule for the derivative gives

$$f'(x) = r(x - \omega)^{r-1} g(x) + (x - \omega)^r g'(x),$$

which shows that $f'(\omega) = 0$ if and only if $r \geq 2$. ❑

If the polynomial f splits completely over Ω, there is a factorization

$$f(x) = (x - \omega_1) \cdot \cdots \cdot (x - \omega_m)$$

with all the roots ω_i in Ω. When the roots ω_i are distinct, we say f *splits simply* over Ω and call $f(x)$ a *separable polynomial*. If not, that is, if at least one root occurs at least twice, the polynomial is said to be *inseparable*.

PROBLEM 1. Verify that if f splits simply in one extension Ω of K it splits simply in any other extension Ω' where it splits. HINT: Chose a common algebraic closure of Ω and Ω'. ✸

It is of course an easy matter to find polynomials with multiple roots, but to find inseparable, *irreducible* polynomial is a lot more subtle[1]. As the proposition below will show, one has to search in positive characteristic to find such species. Among the many new and contra-intuitive phenomenon that can happen in positive characteristic, is that the derivative of a polynomial may vanishes identically without the polynomial being constant. The simplest example of a polynomial with this behavior is $t^p - a$. More generally, if $f(x) = g(x^{p^m})$, by applying the chain rule, we see that

$$f'(x) = p^m x^{p^m - 1} \cdot g'(x^{p^m}) = 0$$

since the characteristic of K is p. Now, these examples are in fact the only examples. We have:

PolyWithVanishDe

Lemma 2 *Let K be a field of characteristic p and assume $f(x)$ is a polynomial in $K[x]$ whose derivative vanishes identically. Then $f(x) = g(x^{p^n})$ for some polynomial $g(x)$ in $K[x]$ whose derivative does not vanish identically.*

PROOF: Let $f(t) = \sum_{0\le i\le r} a_i x^i$. Since the derivative $f'(x) = \sum_{0\le i\le r} i a_i t^{i-1}$ vanishes identically, $ia_i = 0$ for $0 \le i \le r$. This implies that either $a_i = 0$ or $i = 0$, the latter means that i has p as factor. Hence the only non-vanishing terms of f are those whose degree is divisible by p, and we may write $f(x) = \sum_{0\le j\le r/p} a_{pj} t^{pj}$. Or, phrased differently, $f(x) = g(x^p)$ for some polynomial g. If g has a non-vanishing derivative, we are happy, if not, we repeat the process until happiness. ❑

Proposition 1 *Let K be a field and $f(x) \in K[x]$ an irreducible polynomial. Then $f(x)$ is inseparable if and only if $f'(x)$ vanishes identically, i.e., $f'(x) = 0$ as a polynomial. In particular, $f(x)$ is separable if one of the following conditions is fulfilled:*

- ☐ *The characteristic of K is zero.*
- ☐ *The degree of $f(x)$ is prime to the characteristic of K.*

PROOF: Let E be the stem field of $f(x)$, that is $E = K[x]/(f(x))$. Then f has a root α in E, and $f(x)$ is the minimal polynomial to α. The degree of $f'(x)$ being one less than he degree of $f(x)$, it follows that if $f'(\alpha) = 0$, then $f'(x) = 0$ identically. In characteristic zero this can of course not not happen since $f(x)$ is not constant, and lemma 2 shows that in case it happens in positive characteristic, the degree of f must be divisible by the characteristic of K. ❑

PROBLEM 2. Assume that $f(x)$ is an inseparable, irreducible polynomial. Show that one may write $f(x) = g(x^{p^n})$ where $g(x)$ is separable and irreducible. Conclude that all roots of f have the same multiplicity p^n. ✸

PROBLEM 3. Let K be a field of characteristic p and let $a \in K$ be an element. Show that $x^{p^n} - a$ is irreducible over K if and only if a is not p^n-th power in K. HINT: Use that the Frobenius map $x \mapsto x^{p^n}$ is additive to show that if $a^{p^n} = b^{p^n}$ in a field of characteristic p, then $a = b$. Hence all the roots of f in a splitting field Ω are equal. ✸

Separable field extensions

Recall that giving an embedding over K of the stem field E_f of an irreducible polynomial $f(x) \in K[x]$ into a field Ω, is equivalent to giving a root of f in Ω.

Assume that Ω is a splitting field for f. For separable polynomials —that is, polynomials that have as many different roots in Ω as the degree n indicates—this means that there are exactly n emddings into Ω, and for the inseparable polynomials there are less. Hence

StemFieldSeparable

Proposition 2 *Suppose that K be a field and let $f(x) \in K[x]$ be an irreducible polynomial of degree n. Let Ω be a splitting field for f. Then f is separable if and only there are n different embeddings over K of the stem field E_f into Ω.*

A small, but useful, extension of this result is to the case when K is not contained in Ω, but just embedded. That is, there is given an embedding $\sigma\colon K \to \Omega$. Then the result above reads as $f(x)$ is separable if and only if there are exactly n extensions of σ to L. The proof is not difficult and left as an exercise.

Proposition 2 above may be generalized to fields not necessarily being stem fields (but in the end of the day they will be, due to what is called the "Theorem of the primitive element"). Assume that L is a field extension of K. An element $\alpha \in L$ is said to be a *separable element* if the minimal polynomial is separable. The extension is called a *separable extension* if any element in L is separable.

All this should be understood relatively to the field K. However, one has the the lemma

SepInTowers

Lemma 3 *Assume that $K \subseteq E \subseteq L$ is a tower of finite field extensions. If an element α of L is separable over K, it is separable over E.*

PROOF: Let $f(x)$ be the minimal polynomial of α over K. Then of course $f(x) \in E[x]$, but it is not necessarily irreducible there. We may therefore factor $f(x) = g(x)h(x)$ over E, where $g(x)$ is the minimal polynomial of α over E and where $h(\alpha) \neq 0$. Applying the product rule, we find

$$f'(x) = g'(x)h(x) + g(x)h'(x).$$

Hence if $f'(\alpha) \neq 0$, then $g'(\alpha) \neq 0$ (since $h(\alpha) \neq 0$ and $g(\alpha) = 0$). ❑

PROBLEM 4. Show by a (stupid) example that the converse of the lemma is not true
HINT: Take $E = L$. ✸

Proposition 3 *Let L be a finite extension of the field K. Assume that Ω is an algebraic closed field and that σ is an embedding of K in Ω. Then L is a separable extension if and only if the number of different embeddings of L in Ω extending σ equals the degree $[L\colon K]$ of L over K.*

PROOF: Pick an element $\alpha \in L$. If $L = K(\alpha)$ we are done, since then L is isomorphic to the stem field E_f and α is separable over K. If not, we have the tower $K \subseteq K(\alpha) \subseteq L$. The number of embeddings of $K(\alpha)$ in Ω equals the degree $[K(\alpha)\colon K]$, and by induction[2], each of these can be extended to L in $[L\colon K(\alpha)]$ ways since L is separable over K by lemma 3, and we are through since the degree is multiplicative in towers. ❑

[1] Just for this reason, many authors apply the terms separable and inseparable only to irreducible polynomials.

[2] In fact, we need to prove a slightly more general statement to make the induction work: Any embedding of K into Ω can be extended to L in exactly $[L\colon K]$ ways.

Corollary 1 *In a tower $K \subseteq E \subseteq L$ of field extensions, L is separable over K if and only if both E is separable over K and L is separable over L.*

PROOF: We count extensions of embedding of the fields into some algebraically closed field Ω: Assume L separable over E and E separable over K. Then by the proposition, an embedding of K into Ω can be extended to L in $[E\colon L]$ different ways, and each of these can be further extended to L in $[L\colon E]$ ways. Hence the total number of extensions to L equals $[E\colon K][L\colon E]$, and this is equal to $[L\colon K]$. The other way round is just lemma 3 above. ❏

Perfect fields

A *perfect field* is a field K having the property that any extension L of K is separable. All fields of characteristic zero are perfect, and the good news for number theorists is that all *finite* fields are perfect.

One has the following characterisation of perfect fields relating to existence of p-roots in K:

Proposition 4 *Assume that K is a field of characteristic p. Then K is perfect if and only if every one of its elements is a p-th power, i.e., every element in K has a p-th root in K.*

PROOF: Assume that every element has a p-th root, and suppose that L is an inseparable extension of K. Then there is an element $\alpha \in L$, not in K, satisfying a minimal relation

$$\alpha^{nq} + a_{n-1}\alpha^{(n-1)q} + \ldots a_1\alpha^q + a_0 = 0 \qquad (\star)$$

MinRelInSep

where $q = p^m$, and the a^i's are in K. Since every element in K has a p-root, they all have a q-th root as well, and we may find b_i's in K with $b_i^q = a_i$. The relation then takes the form

$$\alpha^{nq} + b_{n-1}^q\alpha^{(n-1)q} + \ldots b_1^q\alpha^q + b_0^q = 0,$$

but, as rising elements to q-th power is additive in characteristic p, this gives

$$(\alpha^n + b_{n-1}\alpha^{n-1} + \ldots b_1\alpha + b_0)^q = 0,$$

contradicting the minimality of the relation ⋆.

The other way around, if $a \in K$ is not a p-th power, the polynomial $x^p - a$ is irreducible and the extension $E_f = K[x]/(x^p - a)$ of K is inseparable. ❏

FINITE FIELDS ARE PERFECT The fields of finite characteristic we shall meet in this course, are are almost exclusively the finite fields. They are all perfect, so we very seldom will have to cope with inseparable fields extensions—however w'll meet inseparable algebras, but that is another story we come back to later.

To see that a finite field $\mathbb{F}_q$—where $q = p^n$ is a prime power—is separable. We check that every element is a p-th power. The Frobenius map $x \mapsto x^p$ is additive (this is true in characteristic p) and injective — $x^p = 0$ obviously implies that $x = 0$. Hence it must be bijective since $\mathbb{F}^q$ is finite.

ALL THIS FUZZ ABOUT NOTHING? The reader deserves at least one example of a extension that is not separable. The easiest is probably the following. Let K be any field of characteristic p and let x be a variable. Then $K(x^p) \subseteq K(x)$ is not separable, since x^p is not a p-th power in $K(x^p)$ (any p-th power in $K(x^p)$ is of degree p^2 in $K(x)$).

Multiple roots and the discriminant

We know since childhood (at least mathematically speaking) that a quadratic polynomial $ax^2 + bx + c$ has a double root if and only if the *discriminant* $b^2 - 4ac$ vanishes. Indeed, the discriminant is the square of the difference of the two roots. The discriminant is a very convenient tool; without actually knowing the roots, one can decide if they are equal or not.

In general, if the monic polynomial $f(x)$ of degree n has the n roots $\omega_1, \ldots, \omega_n$ in splitting field Ω, one defines the discriminant of f as the product

$$\Delta_f = \prod_{1 \le i < j \le n} (\omega_i - \omega_j)^2,$$

If $f(x)$ is not monic, but has leading coefficient a, we let

$$\Delta_f = a^{2n-2} \prod_{1 \le i < j \le n} (\omega_i - \omega_j)^2.$$

Obviously Δ_j vanishes precisely when two roots coincide. The discriminant is invariant under any permutation of the roots, and thus it is a symmetric polynomial in the ω_i's. Hence by the fundamental theorem on symmetric polynomials, it may be expressed as a polynomial in the coefficients of f, just like $b^2 - 4ac$ in the quadratic case, but the actual expression is much more complicated for poly's of higher degree.

In fact the formula for the discriminat is what we call a *universal* formula. It is the same whatever the ω_i's. One can, if one wants to be 100% formal, formulate it in terms of independent indeterminants $w_1, \ldots, w_n$ and prove it over the ring $\mathbb{Z}[w_1, \ldots, w_n]$.

There are many formulas involving such a nice creature as the discriminant. We shall give two, one where we relate the discriminant to the values of the derivative of f at the roots, and one where it is related to the *van der Monde determinant*.

DISCRIMINANT AND DERIVATIVES Since $f(x) = \prod_j (x - \omega_j)$, one easily sees by applying the product rule, that $f'(\omega_i) = \prod_{j,\, j \ne i} (\omega_i - \omega_j)$. Hence

$$\prod_i f'(\omega_i) = \prod_i \left(\prod_{j,\, j \ne i} (\omega_i - \omega_j) \right) = \epsilon \prod_{i<j} (\omega_i - \omega_j)^2$$

where ϵ is a sign. After a moment of reflection one convinces one self that $\epsilon = (-1)^{n(n-1)/2}$—every one of the $n(n-1)/2$ pairs of indices i, j contributes twice to the product, once with the factor $\omega_i - \omega_j$ and once with $\omega_j - \omega_i$. Hence

$$\Delta_f = (-1)^{n(n-1)/2} \prod_i f'(\omega_i). \qquad (\bigstar)$$

In case $f(x)$ is not monic, but has leading coefficient a, we find

$$\Delta_f = (-1)^{n(n-1)/2} a^{n-2} \prod_i f'(\omega_i).$$

This relation between the discriminant and the derivative of f has nice formulation in terms of the norm. Recall that if $K \subseteq L$ is a separable extension, the norm $N_{L/K}(\alpha)$ of α equals the product $\prod_i \sigma_i(\alpha)$ of the value at α of the different embeddings σ_i of L in some sufficiently big field Ω. Let Ω be a splitting field for f and let ω be one of the roots. Then if $L = K(\omega)$, the values $\sigma_i(\omega)$ are just the different roots ω_i of f in Ω and $\sigma_i(f'(\omega)) = f'(\omega_i)$. Combining this with equation ($\bigstar$) above, we obtain

Proposition 5 *Let $f(x)$ be a monic polynomial in $K[x]$ and let $\omega_1, \ldots, \omega_n$ be the roots of f in some splitting field Ω. Then*

$$\Delta_f = (-1)^{n(n-1)/2} N_{K(\omega)/K}(f'(\omega)).$$

THE CASE OF THE TRINOME $x^n + ax + b$ Computing discriminants by hand can be a challenge, but luckily, to day one has software that can can do the dirty jobs for us. However, in the special case of the the trinomes $x^n + ax + b$, the computations—with some cleverness—are not horrible at all, and is a classic. So we shall do it. This furnishes us we many examples, and it reminds us that cumputation by hand sometimes is an option, and probably most importantly, you have a chance to become wiser by doing the calculatuons your self and not only pushing the button.

So let a and b be elements of the field K and let $f(x) = x^n + ax + b$. Let ω be a root of f. The derivative is given as $f'(\omega) = n\omega^{n-1} + a$. Now $\omega^{n-1} = -a - b\omega^{-1}$, so renaming the derivative x and using $x = -(n-1)a - nb\omega^{-1}$, we can solve for ω and obtain

$$\omega = \frac{-nb}{x + (n-1)a}.$$

This shows that

$$f(\frac{-nb}{x + (n-1)a}) = 0.$$

Clearing the denominator, we get

$$(x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n b^{n-1} n^n = 0.$$

Interpreting x as a variable, the left side is the minimal polynomial of $f'(\omega)$, and the norm of $f'(\omega)$, which we are looking for, is the constant term with the factor $(-1)^n$. The binomial theorem and some cleaning up gives

$$\Delta_f = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n)$$

Specializing to case of a cubic $x^3 + ax + b$, one gets the ubiquious formula for the cubic discrimant

$$\Delta_f = -27b^2 - 4a^3$$

PROBLEM 5. Compute the discriminant of the two cubic polynomials x^3+x+1 and x^3-x-1. ✸

PROBLEM 6. Let $g(x)=x^3+ax^2+b$ show that $\Delta_g=-27b^2-4a^3b$. HINT: Relate Δ_g to the discriminat of $f(x)=x^3g(x^{-1})$ ✸

PROBLEM 7. Compute the discriminat of x^3-2x^2+2. ✸

PROBLEM 8. The aim of this exercise is to show that if x^3+ax+b is cubic polnomial whose discriminant is negative, then it has a unique real root given by

$$\omega=\sqrt[3]{(-b+\delta/3\sqrt{-3})/2}+\sqrt[3]{(-b-\delta/3\sqrt{-3})/2} \qquad (✪)$$

where δ is a square root of the discrimant $-4a^3-27b^2$.

RealRoot

a) Let ξ be a primitive third root of unity. Show that there are real numbers s and t such that $s\xi+t\bar{\xi}$ and $s\bar{\xi}+t\xi$ are the two complex roots of $f(x)$.

b) Show that the real root equals $s+t$. HINT: The sum of the roots is zero.

c) Show that $-b=s^3+t^3$. HINT: The product of the roots is $-b$.

d) Show that the product of the differences of the roots (*i.e.*, Δ) is $\pm3\sqrt{-3}(s^3-t^3)$.

e) Show the formula (✪). HINT: Solve for s and t.

✸

PROBLEM 9. If $f(x)=ax^3+bx^2+cx+d$, show that $\Delta_f=b^2c^2-4ac^3-4b^3d-27a^2d^2+18abcd$. ✸

THE VAN DER MONDE DETERMINANT To treat the van der Monde determinant we do it generically, as we did with the discriminant. We use n independent variables $w_1,\dots,w_n$ be variables, so the formulas we obtain are valid in the polynomial ring $\mathbb{Z}[w_1,\dots,w_n]$. Subsequently one may substitute for the w_i whatever elements one wants, as long as they are elements of a commutative ring, hence the formulas are universally valid.

$$V_n=V_n(w_1,\dots,w_n)=\begin{vmatrix} 1 & 1 & \dots & \dots & 1 \\ w_1 & w_2 & \dots & \dots & w_n \\ w_1^2 & w_2^2 & \dots & \dots & w_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ w_1^{n-1} & w_1^{n-1} & \dots & \dots & w_n^{n-1} \end{vmatrix}$$

Setting $w_i=w_j$ kills the determinant two columns then being equal. This means that w_i-w_j divides V (and this is where we use the ring $\mathbb{Z}[w_1,\dots,w_n]$ and that it is a UFD). It follows that the product $P_n=\prod_{i>j}(w_i-w_j)$ is a factor of V.

This product and the van der Monde are both polynomials of the same degree. Indeed, every term of the van der Monde is of degree $\sum_{i=0}^{n-1} i = n(n+1)/2$, and the product has as many (linear) factors as there are pairs with $i > j$, that is $n(n+1)/2$. Hence the two expressions agree up to a scalar factor, say ϵ_n. Setting $w_n = 0$ and developing V_n along the last column gives $V_n|_{w_n=0} = (-1)^{n-1} w_1 \cdot \cdots \cdot w_{n-1} V_{n-1}$ and similarly $P_n|_{w_n=0} = (-1)^{n-1} w_1 \cdot \cdots \cdot w_{n-1} V_{n-1}$. Hence $\epsilon_n = \epsilon_{n-1}$, and of course $\epsilon_2 = 1$, so the scalars ϵ_n all reduce to 1.

We have established the following:

Proposition 6 *Assume that $f(t)$ is a polynomial of degree n whose roots are $\omega_1, \ldots, \omega_n$ in some extension field Ω of K. Then we have the following relation between he discriminant of f and the van der Monde determinant made out of the roots:*

$$\Delta_f = V_n^2(\omega_1, \ldots, \omega_n)$$

Nilpotency and trace

There is a close connection between nilpotency of a linear operator A on a vector space and the tracelessness of all the powers of A. In fact, over a field of characteristic zero, A being nilpotent is equivalent to the vanishing of the traces $\operatorname{tr} A^i$ for $i \geq 1$. If the ground field is of positive characteristic, however , the situation is a little more complicated due to the fact that there are non-constant polynomials with a vanishing derivative.

Even if our main objects of study—rings of algebraic integers in number fields—all live in characteristic zero, we have a great interest in considering the case of positive characteristic. The reason is as follows. If $A \subseteq B$ is an extension of say number rings—for example could B be the integtral closure of A in some finite field extension of the fraction fielsd of A—and $\mathfrak{p} \subseteq \mathbb{A}$ a prime ideal, we are certainly interested in getting a hand on the set of prime ideals $\mathfrak{q}$ in B with $\mathfrak{q} \cap A = \mathfrak{p}$—that is, the *fibre* of the map $\operatorname{spec} B \to \operatorname{spec} A$ over $\mathfrak{p}$. This fibre is in one-to-one-correspondence with the primes in the ring $B/\mathfrak{p}B$, and this ring is an algebra over the finite field $A/\mathfrak{p}$.

The lesson is: We are also interested in finite dimensional algebras over finite fields!

EXAMPLE 1. An illustrative example is when B is generated by one element over A; to be concrete, say $A = \mathbb{Z}$ and $B = \mathbb{Z}[\alpha]$ where α belongs to some finite extension L of $\mathbb{Q}$, and α is integral over $\mathbb{Z}$. Then $B = \mathbb{Z}[x]/(F(x))$ where $F(x)$ is the minimal polynomial of α over $\mathbb{Q}$, and this polynomial has integral coefficients, α being integral. If now $p \in \mathbb{Z}$ is a rational prime, we can perform the following small computation

$$B/pB = \mathbb{Z}[x]/(F(x), p) = \mathbb{F}_p[x]/(f(x)),$$

where $f(x) \in \mathbb{F}_p[x]$ denotes the polynomial obtained from F by reducing all coefficients mod p. Of course, $f(x)$ is not necessarily irreducible (even if F is). Some times it is and some times not.

If $f(x) = g_1(x)^{v_1} \cdot \cdots \cdot g_r(x)^{v_r}$ is a factorization of f where the $g_i(x)$'s are different irreducible poly's in $\mathbb{F}_p[x]$, then by some well known chinese theorem

$$B/pB = \mathbb{F}_p[x]/(g_1(x)^{v_1} \cdot \cdots \cdot g_r(x)^{v_r}) = \prod \mathbb{F}_p[x]/(g_i(x)^{v_i})$$

Each factor $\mathbb{F}_p[x]/(g_i(x)^{v_i})$ is an algebra over $\mathbb{F}_p$, and it is a *field* if and only if $v_i = 1$, that is, if and only if it is without nilpotent elements. So we see that nilpotency is couple to multiple factors of f, or in case the factors are linear, to multiple roots of f. Poly's with multiple roots in some extension of the base field, are the *inseparable poly's*, so the lesson is: Nilpotency is coupled to inseparability. ❄

PROBLEM 10. Show that $x^2 + 1$ is irreducible mod p if and only if $p \equiv 1 \mod 4$. ✸

Linear operators

Coming back to linear operators, we fix a field K and a linear operator A on the finite dimensional vector space V over K. The characteristic polynomial of A is, as we know, defined by $P_A(t) = \det(t \cdot I - A)$. Over some extension L of K the characteristic polynomial splits into a product $P(t) = \prod_i (t - \lambda_i)$ of linear factors. The λ_i's are the *eigenvalues* of A in λ.

In addition to the characteristic polynomial we shall make use of the following associated polynomial:

$$Q_A(t) = \prod (1 - \lambda_i t) = t^n P_A(t^{-1})$$

It still has coefficients in K. The degree of Q_A may drop compared to the degree of P_A. It is equal to the number of non-zero eigenvalues of A. In fact, the roots of Q are the inverses of the non-vanishing eigenvalues of A. A consequence of Cayley-Hamilton is that the operator A is nilpotent if and only if Q_A is constant.

Our next lemma is completely elementary, on the level of a first course in calculus, but will be very usual:

FundFormel

Lemma 4 *Assume that $Q(t) = \prod_{1 \le i \le n}(1 - \lambda_i t)$ is a polynomial where the λ_i's are in some commutative ring A. Then the formula below holds true in the power series ring $A[[t]]$:*

$$\frac{Q'(t)}{Q(t)} = -\sum_{1 \le i \le n, k \le 1} \lambda_i^k t^{k-1}$$

The identity in the lemma is completely formal. That is, we may assume that λ_i's are independent variable, and the identity holds in the ring of formal power series[3] $\mathbb{Z}[\lambda_1, \ldots, \lambda_n][[t]]$. It is therefore valid whenever the two sides have a meaning.

PROOF: The product rule gives $Q(t)' = \sum_i (-\lambda_i) \prod_{j \ne i} (1 - \lambda_j t)$. Then

$$\frac{Q'(t)}{Q(t)} = \sum_i \frac{-\lambda_i}{1 - t\lambda_i}$$

and the lemma follows from the the ubiquitous formula for the sum of a geometric series. ❑

[3] Admittedly, this formulation is not very much first-calculus-course-ish.

Lemma 5 *If A is an operator on a finite dimensional vector space V of dimension n over the field K, then*

$$\frac{Q'_A(t)}{Q_A(t)} = -\sum_{1\leq k} \operatorname{tr} A^k t^{k-1}$$

holds in the power series ring $K[[t]]$, where $Q_A(t) = t^n P_A(t^{-1})$ and $P_A(t)$ denotes the characteristic polynomial of A.

PROOF: If the λ_i's with $1 \leq i \leq n$ are the eigenvalues of A, then one has $Q_A(t) = \prod_i (1-\lambda_i t)$ and $\operatorname{tr} A^k = \sum_i \lambda_i^k$. ❑

Proposition 7 *For the operator A, the two following conditions are equivalent*

- ☐ *For all $k \leq 1$, the trace of A^k vanishes, i.e., $\operatorname{tr} A^k = 0$.*
- ☐ $Q_A(t)' = 0$

The trace form and separability

We have now come to main theorem of this section. Let as usual K be a field and L a finite extension of K. The trace gives us a *bilinear* and *symmetric* form on L with values in K , namely the form $(x, y) = \operatorname{tr}_{L/K}(xy)$ for $x, y \in L$. Indeed $tr_{L/K}(xy)$ is clearly symmetric, and the product being linear in each variable, $\operatorname{tr}_{L/K}(xy)$ is bilinear. This form is very useful since it detects inseparability; more precisely the trace form is non-degenerate if and only if the extension L of K is separable:

TraceFormNondegerate

Theorem 1 *Let $K \subseteq L$ be a finite separable field extension. Then the bilinear form $\operatorname{tr}_{L/K}(xy)$ is non degenerate if and only if the extension L of K is separable.*

PROOF: Assume first that L is separable over K.

We use induction on $n = [L\colon K]$, and let L be a counter example of least degree over K. The field L being a counter example, there is an element $x \in L$ not in K with $\operatorname{tr}_{L/K}(xy) = 0$ for all y. Hence $L = K(x)$ since L was the smallest bad guy; indeed $K(x)$ is separable over K, and, of course, $\operatorname{tr}_{K/L} xy = 0$ for all $y \in K(x)$.

By putting $y = x^{k-1}$ we see that $\operatorname{tr}_{L/K}(x^k) = 0$ for all k. Since

$$x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

with the a_i's in K, and $a_0 \neq 0$, this gives $\operatorname{tr} a_0 = n a_0 = 0$, and n must be divisible by the characteristic p of K.

Let now $Q(t) = t^n P(t^{-1})$ where $P(t)$ denotes the characteristic polynomial of the multiplication map ρ_x. Then by lemma 4 we have

$$\frac{Q'(t)}{Q(t)} = -\sum_{k\geq 1} \operatorname{tr}_{L/K}(x^k) t^{k-1} = 0,$$

and Q' vanishes identically. Now

$$0 = Q(t)' = nt^{n-1}P(t^{-1}) + t^{n-2}P'(t^{-1}) = t^{n-2}P'(t^{-1})$$

as p divides n. Hence P' vanishes identically. But the characteristic and the minimal polynomial of x coincide (since $L = K(x)$), and by consequence x is not separable over K.

For the proof of the implication in the other direction, assume that L is not separable, and let $x \in L$ be inseparable over K. We first look at the extension $K(x)$ generated by x. If $P(t)$ is the characteristic polynomial (which is equal to the minimal polynomial of x over K) of multiplication by x in $K(x)$, then $P' = 0$. Hence $Q' = 0$, and by what we just did, $\mathrm{tr}_{K(x)/x}(y) = 0$ for all $y \in K(x)$. It follows that $\mathrm{tr}_{L/K} = \mathrm{tr}_{K(x)/L} \circ \mathrm{tr}_{L/K(x)} = 0$. ❑

Just one remark about this proof. Most of it is there to deal with the characteristic p case. In characteristic zero, one concludes immediately from the fact that $\mathrm{tr}_{L/K}(x^k) =$ for all $k \geq 1$, that $Q' = 0$, hence $Q(t)$ constant, *i.e.,* that x is nilpotent, which means that $x = 0$ since K is a field. And thus the trace form is non-degenerate.

The dual basis and finiteness of the integral closure

Assume that $v_1, \ldots, v_n$ is a K basis for the sperable extension L of K. Then by the general theory of non-degenerate quadratic forms, there exsists a *dual basis*. This is a basis $v_1', \ldots, v_n'$ such that

$$\mathrm{tr}_{L/K}(v_i v_j') = \delta_{ij}.$$

The proof of the following result illustrates the usefulness of the dual basis. The result is really the basis for the whole algebraic number theory. It is fundamental that the integral closure of a Dedekind ring in a finite extension of the field of fraction, still is Dedekind. The main ingredient in the proof of this result, and the only subtle one, is that the integral closure remains noetherian. This follows from our next proposition.

Proposition 8 *Let A be noetherian domain, integrally and closed in its fields of fractions K. Assume that L is a finite extension of K such that the bilinear form $\mathrm{tr}_{L/K}(xy)$ is non-degenerate. Then integral closure B of A in L is a finitely generated module over A.*

PROOF: Let $v_1, \ldots, v_n$ be a basis for L over K. We may assume that the v_i's are contained in B (multiplied by a common denominator, they still constitute a basis). Let $v_1', \ldots, v_n'$ be the dual basis with respect to the bilinear form $\mathrm{tr}_{L/K}(xy)$. Then we claim that B is contained in the A-submodule of L generated by the v_i's. This submodule is by definition finitely generated, and A being notherian, it follows that B is finitely generated.

Since $v_1', \ldots, v_n'$ is a K-basis for L, any $\beta \in B$ may be written as $\beta = a_1 v_1' + \cdots + a_n v_n'$ with $a_i \in K$. Our task is to verify that the a_i's are in A. Now

$$\mathrm{tr}_{L/K}(\beta v_j) = \sum a_i \, \mathrm{tr}_{L/K}(v_i' v_j) = a_j$$

and since both β and v_i are in B their product is, and hence $\mathrm{tr}_{L/K}(\beta v_i) \in A$ by proposition 7 on 6 in the section Norms and Traces.. ❏

Theorem 2 *Let $A \subseteq K$ be a dedekind ring and its field of fractions. Let L be a finite, separable extension of K and denote by B the integral closure of A in B. Then B is a Dedekind ring.*

PROOF: We know that B is integrally closed and finitely generated as an A-module. Hence it is noetherian and of the same Krull-dimension as A (It is generally true that if B is an A-algebra which is finitely generated as an A-module, then if one of A and B is noteherian, the other is, and they have the same Krull-dimension). ❏

Without the hypothesis that L be separable over K, the domain B need not be finite over A, but it will be noetherian and of Krull dimension one. This is called the Krull-Akizuki-theorem, and we shall not prove it. So, the theorem remains true even if we skip the assumption that L is separable over K.

Etale or separable algebras

One of the main problems in algebraic number theory is to describe how a rational prime p factorizes in the ring A of integers in an algebraic number field K. As part of this, it is of great importance to decide which primes p have a *multiple* factor in A. Such primes are said to *ramify in A*.

One way of attacking this problem, is to study the $\mathbb{F}_p$-algebra A/pA.

Lemma 6 *The prime p ramifies in A if and only if A/pA has non-zero nilpotent elements*

PROOF: If $pA = \prod_i \mathfrak{p}^{\nu_i}$ the chinese theorem gives

$$A/pA = \prod_i A/\mathfrak{p}^{\nu_i}$$

which clearly is without nilpotents if and only if *all* the non-zero ν_i's are equal to one. ❏

In the case that A is geneated by one element over $\mathbb{Z}$, that is, of the form $\mathbb{Z}[x]/(f(x))$ we could test nilpotency in A/pA by testing $f(x)$ for multiple roots mod p. This happends if and only if the discriminant of f has p has a factor. However not all rings of integers are generated by one element! Hence we something more general than just the discriminant of a polynomial.

Let A be an algebra a field K, which is equivalent of finite dimension as a vector space over K. One may, just as for fields, define the trace $\mathrm{tr}_{A/k}(x)$ of an element x in A as the trace of the multiplication map $\rho_x \colon A \to A$. And we can define the *trace form* as $\mathrm{tr}_{A/K}(xy)$.

We know from commutative algebra that A is a product of local algebras, *i.e.,* $A = \prod_i A_i$. Clearly this is an orthogonal decomposition of A with respect to the trace

form, *i.e.*, $\operatorname{tr}(xy) = 0$ if $x \in A_i$ and $y \in A_j$ and $i \neq j$. Indeed, it is allready orthogonal for the product! The trace form is therefore non-degenerate if and only if the trace form $\operatorname{tr}_{A_i/k}$ of each factor is non-degenerate.

Proposition 9 *The trace form $\operatorname{tr}_{A/K}(xy)$ is nondegenerate if and only if A is isomorphic to a product of fields L_i, all being separable over K.*

PROOF: After what we just said, we assume that A is a local algebra, and must show that $\operatorname{tr}_{A/K}(xy)$ is non-degenerate if and only if A is a separable field extension of K. Assume that the trace form is no-degenerate. Then A has no nilpotents, since if x is nilpotent, xy is nilpotent for all y, hence $\operatorname{tr}_{A/K}(xy) = 0$ for all y. Therefor A is a field and by xxx it is separable. ❏

The discriminant of a field extension

Let $K \subseteq L$ be a finite, separable field extension. To every K-basis $v_1, \ldots, v_n$, wich we call $\mathcal{B}$, we assosiate the determinant

$$\delta_{\mathcal{B}} = \det(\operatorname{tr}_{L/K}(v_i v_j)).$$

It is called *the discriminant* of the basis $\mathcal{B}$.

Of course, the dicriminant depends on the basis $\mathcal{B}$. Assume that $v'_1, \ldots, v'_n$ is another basis, and let V denote the transition matrix between the two basises. As with any quadratic form, the matrix of the quadratic form transformss as $(\operatorname{tr}_{L/K}(v_i v_j)) = V(\operatorname{tr}_{L/K}(v'_i v'_j))V^t$. Hence taking determinants, we see that

$$\delta_{\mathcal{B}} = (\det V)^2 \delta_{\mathcal{B}'}$$

RELATION TO THE DEDEKIND DETERMINANT The setting is as usual witk $K \subseteq L$ a separable field extension and Ω a sufficiently big extension field of K, more spesifically, we assume that the number of embeddings of L in Ω is equal to n, the different embeddings being $\sigma_1, \ldots, \sigma_n$. For any K-basis $v_1, \ldots, v_n$ for L, we may concider the matrix $(\sigma_j(v_i))$, Dedekind showed this matrix to be invertible and its determinant is closely related to the discriminant:

Proposition 10 $\delta_{\mathcal{B}} = \det(\sigma_j(v_i))^2$

PROOF: One calculates the matrix product:

$$MM^t = (\sigma_j(v_i))(\sigma_i(v_j)) = (\sum_k \sigma_k(v_i)\sigma_k(v_j)) = (\sum_k \sigma_k(v_i v_j)) = (\operatorname{tr}_{K/L}(v_i v_j))$$

whetre the last equality holds since $\operatorname{tr}_{K/L}(\alpha) = \sum_k \sigma_k(\alpha)$ by theorem xxx. The proposition follows. ❏

THE CASE OF A PRIMITIVE ELEMENT If α is a generator for the field L over K, the discriminat is closely related to the van der Monde determinant—at least to the discriminant of the canonical basis $\mathcal{A}$ consisting of the powers $1, \alpha, \ldots, \alpha^{n-1}$—and thus to the minimal polynomial of α. In fact, closely related is an understatement, the discriminant of the basis $\mathcal{A}$ is equal to the discriminant of the minimal polynomial of α. And they are both equal to the square of the van der Monde.

We let σ_j be the different embeddings of $K(\alpha)$ in Ω and let $\alpha_j = \sigma_j(\alpha)$. For the van der Monde matrix V we have $V = (\alpha_j^{i-1})_{1\leq i,j\leq n}$. Hence computing VV^t, we get

$$VV^t = (\sum_k \alpha_k^{i-1}\alpha_k^{j-1}) = (\sum_k \alpha_k^{i+j-2}) = (\mathrm{tr}_{L/K}(\alpha^{i-1}\alpha^{j-1}))$$

, and hence

Proposition 11 *Assume that $L = K(\alpha)$ is of degree n, and let $\mathcal{A}$ be the natural basis $1, \alpha, \ldots, \alpha^{n-1}$. Then if V denotes the van der Monde matrix $(\alpha^{i-1}\alpha^{j-1})$, then*

$$\delta_{\mathcal{A}} = (\det V)^2.$$

If $f(x)$ denotes the minimal polynomial of α, then the discriminant of f and of the basis $\mathcal{A}$ coincide:

$$\Delta_f = \delta_{\mathcal{A}}.$$