3.B Separable polynomials and Separable Extensions

First we define separable polynomials over an (arbitrary) commutative ring. Let A be a commutative ring. For a polynomial $f \in A[X]$, let $f' = df/dx$ be the derivative of f with respect to the indeterminate X i.e. if $f = \sum_{i=0}^{n} a_i X^i$, then $f' = \sum_{i=0}^{n} i a_i X^{i-1}$.

3.B.1 Definition A polynomial $f \in A[X]$ is called Separable if f is monic and f and f' together generate the unit ideal in A[X], i.e. $A[X]f + A[X]f' = A[X]$ or equivalently, there exist polynomials $g, h \in A[X]$ such that $1 = gf + hf'$. This is equivalent to: the element $f'(x)$ in the (free) residue algebra $A[X]/A[X]f$ is a unit.

Note that if $A = k$ is a field, then a polynomial $f \in k[X]$ is separable if and only if $\gcd(f, f') = 1$. This equivalence is immediate from the fact that k[X] is a PID.

3.B.2 Examples (1) Trivial examples of (monic) separable polynomials are 1, $X-a$, $(X-a)(X-a-1)$, where a is an arbitrary element of A. In the case $f = (X-a)(X-a-1)$, $f' = 2(X-a)-1$ and hence $1 = (f')^2 - 4f$

(**Remark** For $A = \mathbb{Z}$, these are the only examples of (monic) separable polynomials. This is immediate from the following theorem of Hermite-Minkowski:

Theorem (Hermite-Minkowski) The absolute value of the discriminant of a free $\mathbb{Z}$-algebra B of rank $n>1$ which is an integral domain is bigger than 1. In particular, B is not separable over $\mathbb{Z}$.

(See also

(2) A polynomial $f = X^n - a \in A[X]$, $n \geq 2$ is separable if and only if both n and a are units in. Since in the residue algebra $A[x] = A[X]/(f)$, $f'(x) = nx^{n-1}$ is a unit $\Longleftrightarrow$ n and x are units in $A[x]$ $\Longleftrightarrow$ n and $x^n = a$ are units in A. (since $A[x]$ is a free A-module with basis $1, x, \cdots, x^{n-1}$). In particular, if $A = k$ a field. Then $X^n - a$, $n \geq 1$, $a \neq 0$ is separable $\Longleftrightarrow$ char $k \nmid n$.

(3) (Discriminants) Let $f \in A[X]$ be a monic polynomial of degree n. Then f is separable if and only if $f'(x) \in B := A[x] = A[X]/(f)$ is a unit $\Longleftrightarrow$ the norm $N_A^B(f'(x))$ is a unit in A. Recall that by definition, this norm is the resultant $R(f, f')$ of f and f'. The element

$$D(f) := (-1)^{\binom{n}{2}} R(f, f') = (-1)^{\binom{n}{2}} N_A^B(f'(x))$$

is called the discriminant of f.

3.B.3 Theorem Let $f \in A[X]$ be a monic polynomial of degree n over a ring A. Then:

(1) f is separable if and only if the discriminant $D(f)$ of f is a unit in A.

(2) Suppose that f splits into linear factors over A, i.e. $f = \prod_{i=1}^{n} (X - a_i)$ with $a_1, \dots, a_n \in A$. Then

$$D(f) = (-1)^{\binom{n}{2}} \prod_{j=1}^{n} f'(a_j) = \prod_{1 \le i < j \le n} (a_j - a_i)^2 = V(a_1, \dots, a_n)^2.$$

In particular, in this case f is separable if and only if all differences $a_j - a_i$, $i \neq j$ are units in A

Proof (1) f is separable $\iff f'(x) \in A[x]^\times \iff$

$$D(f) = (-1)^{\binom{n}{2}} N_A^{A[x]}(f'(x)) \in A^\times.$$

(2) Note that $f' = \sum_{j=1}^{n} \prod_{i \neq j} (X - a_i)$.

We now study separable polynomials over a field.

3.B.4 Lemma *Let K/k be a field extension and $f \in k[X]$. Then f is separable over k if and only if f is separable over K.*

Proof Follows from the fact that:

$$\gcd_{k[X]}(f_1,\dots,f_n) = \gcd_{K[X]}(f_1,\dots,f_n) \text{ for } f_1,\dots,f_n \in k[X]$$

(**Proof**: This is immediate from: *for $f, g \in k[X] \subseteq K[X]$, g divides f in $k[X] \iff g$ divides f in $K[X]$.* ("$\Rightarrow$" clear. For "$\le$" suppose $f = hg$ with $h \in K[X]$. We may assume $g \neq 0$. To show that $h \in k[X]$. By division algorithm there exist $q, r \in k[X]$ such that $f = qg + r$ with $\deg r < \deg g$ and hence $(h-q)g = r$. Therefore $h - q = 0$ by comparing degrees and hence $h = q \in k[X]$.)

3.B.5 Theorem *Let k be a field. For $f \in k[X]$ the following statements are equivalent:*

(i) *f is separable over k.*

(ii) *f has only simple prime factors over every field extension K/k.*

(iii) *f has only simple zeros in every field extension K/k.*

(iv) *There exists a field extension K/k such that f splits into simple linear factors over K, i.e. all zeros of f are in K and each zero of f is simple.*

Proof Note that if f has a quadratic factor g^2, then g is a common divisor of f and f' ($f = g^2h$, then $f' = 2gg'h + g^2h'$). Therefore (i) $\Rightarrow$ (ii) immediate. (ii) $\Rightarrow$ (iii) clear.

(iii) $\Rightarrow$ (iv): By Kronecker's thm there exists a field extension K/k such that f splits into linear factors over K. These linear factors of f are simple by (iii).

(iv) $\Rightarrow$ (i): Immediate from 3.B.3 (2). A direct argument is also given in the lemma below which is simpler

3.B.6 Lemma Let k be a field and $f_1, \dots, f_n \in k[X]$. Then the following statements are equivalent:

(i) The product $f_1 \cdots f_n$ is separable.

(ii) The polynomials $f_1, \dots, f_n$ are separable and are pairwise relatively prime.

Proof We may assume $n=2$ and $f_1 = f$, $f_2 = g$.

(i) $\Rightarrow$ (ii): If fg is separable, then fg and $(fg)' = f'g + fg'$ are relatively prime. Then (the pairs) f, f' (resp. g, g' (and f, g)) cannot have a prime divisor.

(ii) $\Rightarrow$ (i): Let h be a prime divisor of fg and $(fg)'$. Then either $h \mid f$ or $h \mid g$. Suppose that $h \mid f$. Then, since h divides $(fg)' = f'g + fg'$, h divides $f'g$ and so either $h \mid f$ or $h \mid g$. This contradicts the assumptions $\gcd(f, f') = 1$ and $\gcd(f, g) = 1$.

3.B.7 Corollary. Every divisor of a separable polynomia $f \in k[X]$ over a field k is also separable.

3.B.8 Corollary Let k be a field and $0 \neq f \in k[X]$. Then f is separable if and only if all prime factors of f are separable and are simple.

Separability of a prime polynomial is easy to verify:

A prime polynomial $f \in k[X]$ over a field k is separable if and only if $f' \neq 0$. Since $\deg f' < \deg f$, $\gcd(f, f') \neq 1 \iff f' = 0$.

If $\operatorname{char} k = 0$, then every prime polynomial $f \in k[X]$ is separable, since $f' \neq 0$. But if $\operatorname{char} k = p > 0$, then for a polynomial $f \in k[X]$, the derivative $f' = 0 \iff f \in k[X^p]$, i.e. at most the coefficients of f of the powers $1, X^p, X^{2p}, \ldots$ of X^p are non-zero.

3.B.9 Definition A field k is called perfect if every prime polynomial in $k[X]$ is separable.

By 3.B.8 over a perfect field a non-zero polynomia is separable if and only if its prime factors are simpl Since prime polynomials over an algebraically close field are linear, they are trivially separable. Therefo

3.B.10 Theorem Every algebraically closed field is perfect. Every (field of) characteristic 0 is perfect.

In the case of fields of characteristic > 0, we hav the following important criterion:

3.B.11 Theorem A field k of characteristic $p > 0$ is perfect if and only if the Frobenius-homomorphism $k \longrightarrow k$, $x \longmapsto x^p$ is surjective.

Proof We need to show that k is perfect $\Leftrightarrow$ every element $a \in k$ is a p-th power in k $\Leftrightarrow$ every polynomial of the form $X^p - a$, $a \in k$, has a zero in k

($\Rightarrow$) Suppose that k is perfect and $X^p - a$, $a \in k$ has no zero in k. Then by the following lemma the polynomial $X^p - a$ is irreducible in $k[X]$ and is not separable, a contradiction.

($\Leftarrow$) Conversely, suppose that every element $a \in k$ is a p-th power in k and $f \in k[X]$ is a polynomial with $f' = 0$. Then $f \in k[X^p]$, i.e. $f = a_0 + a_1 X^p + \dots + a_n X^{pr}$ By assumption there are elements $b_0, \dots, b_n \in k$ such that $b_i^p = a_i$, $i = 0, \dots, n$. Then $f = b_0^p + b_1^p X^p + \dots + b_n^p X^{pn} = (b_0 + b_1 X + \dots + b_n X^n)^p$ and hence f is not a prime polynomial. This proves that prime polynomials in $k[X]$ are separable.

3.B.12 Lemma *Let k be a field of characteristic > 0. If $a \in k$ is not a p-th power in k, then $X^p - a$ is irreducible in $k[X]$.*

Proof Let K/k be a field extension in which $X^p - a$ has a zero $b \in K$. Then, in $K[X]$, $X^p - a = X^p - b^p = (X-b)^p$. Since $X^p - a$ is not prime in $k[X]$, it has a monic prime factor $f \in k[X]$ of degree $n < p$. Note that f is separable, since $\deg f < p$. On the other hand $f = (X-b)^n$ in $K[X]$ and hence $n = 1$ and $b \in k$ (by 3.B.5), a contradict

Let k be a field of characteristic $p > 0$. Then, since the Frobe
nius-homomorphism is injective, by 3.B.11 it is an

automorphism $\Longleftrightarrow$ k is perfect.

For a finite field k, every endomorphism is an automorphism. Therefore we have:

3.B.13 Theorem Every finite field is perfect.

3.B.14 Example A simplest example of a field which is not perfect is: let k be an arbitrary field of characteristic $p>0$. In the field of rational functions $k(X)$ the element X is not p-th power. Therefo by 3.B.11 $K=k(X)$ is not perfect.

Now, we prove generalisation of 3.B.14 and the followi connection between arbitrary prime polynomials and Separable prime polynomials.

3.B.15 Theorem Let k be a field of characteristic $p>0$ and let $f \in k[X]$ be a monic polynomial. Suppose that $f = g(X^{p^e})$ and $g \in k[X]$, $g \notin k[X^p]$ Then f is irreducible if and only if g is irreducible and if $e>0$, then not all the coefficients of g (which are the coefficients of f) are p-th powers in k. If f is irreducible, then g is separable.

Proof Suppose that f is irreducible. Then clearly g is irreducible. For, if $g=g_1g_2$, then $f=g(X^{p^e})=g_1(X^{p^e})g_2(X$ If $e>0$, then not all coefficients of g are p-th power in k, otherwise f will be a p-th power in $k[X]$ (see the second part of the proof of 3.B.11).

Conversely, suppose that g satisfies the given conditions. We shall show that $g(X^{p^e})$ is irreducible by induction on e. The case $e=0$ is trivial. Now, assume that $e>0$. Let h be a monic prime factor of $g(X^{p^e})$. Then there exists a representation $g(X^{p^e}) = h^r \cdot q$ with $r \geq 1$ and a polynomial $q \in k[X]$ which is not divisible by h. If $r=1$ and $q=1$, then $g(X^{p^e}) = h$ is irreducible. Therefore assume that either $r \geq 2$ or $q \neq 1$. Now we claim that there exists a representation of the type $g(X^{p^e}) = f_1 \cdot f_2$ with non constant polynomials $f_1, f_2 \in k[X^p]$.

First assume that r is a multiple of p. Then h^p and hence h^r is a polynomial in X^p and the same holds for q, i.e. q is a polynomial in X^p, since $0 = g(X^{p^e})' = (h^r)'q + h^r q' = h^r q'$, i.e. $q'=0$. Therefore the case $q=1$ is not possible, otherwise all coefficien of g would be p-th powers in k. Now we can take $f_1 = h^r$ and $f_2 = q$.

Now, assume that r is not a multiple of p. From $0 = g(X^{p^e})' = r h^{r-1} h' q + h^r q'$, it follows that (by cancelling h^{r-1}) h divides h', since $h \nmid q$. This is possible only in the case $h'=0$. This proves that h and hence h^r is a polynomial in X^p and the sam holds for q as well. If $q=1$, then take $f_1 = h$ and $f_2 = h^{r-1} (\neq 1)$. If $q \neq 1$, then take $f_1 = h^r$ and $f_2 = q$.

Now, let $g_i = f_i(X^p)$, $i=1,2$. Then $g(X^{p^{e-1}}) = g_1 g_2$ a contradiction to the induction hypothesis.

Let k be a field of characteristic $p>0$. If $f \in k[X$ is an irreducible polynomial and if $f = g(X^{p^e})$ is the representation of f with a polynomial $g \in k[X$, $g \notin k[X^p]$ as in 3.B.15. The integer e is called the inseparability degree of f.

3.B.16 Theorem Let k be a field of characteristic $p>0$ and let $f \in k[X]$ be a monic irreducible polynomial of degree n and the inseparability degree of f. Then each zero of f in a field extension K/k have multiplicity p^e. In particular, if K/k is a splitting field of f over k, then

$f = (X-b_1)^{p^e} \cdots (X-b_r)^{p^e}$ with $r = n/p^e$ and distinct elements $b_1, \dots, b_r \in K$.

Proof Let $f = g(X^{p^e})$ with $g \in k[X]$, $g \notin k[X^p]$. Then g is irreducible and separable by 3.B.15. Let $b \in K$ be a zero of f in a field extension K/k. Then $a = b^{p^e}$ is a zero of g and hence $g = (X-a)h$, where $h(a) \neq 0$. Further, $f = (X-b)^{p^e} h(X^{p^e})$ and $h(b^{p^e}) = h(a) \neq 0$. This proves that the multiplicity of the zero b of f is p^e. Moreover, the powers $b_1^{p^e}, \dots, b_r^{p^e}$ of the elements $b_1, \dots, b_r$ are r distinct zeros of the separable polynomial g in K.

3.B.17 Exercises

1. The polynomial $f = 2X^2 - 1 \in \mathbb{Z}[X]$ and its derivative $f' = 4X$ generate the unit ideal in $\mathbb{Z}[X]$. (Since f is not monic, f is not separable) The discriminant of f is 8.

2. Let A be a (commutative) ring and let $f, g \in A[X]$ be monic polynomials. Show that the following statements are equivalent:
   (i) fg is separable.
   (ii) f and g are separable and $A[X]f + A[X]g = A[X]$.
   (Hint: For (ii) $\Rightarrow$ (i) {do calculation modulo the maximal ideals or prime ideals in $A[X]$. OR use the following ideals
   For $\mathfrak{a}_1, \dots, \mathfrak{a}_n; \mathfrak{b}_1, \dots, \mathfrak{b}_m$ in A with $\mathfrak{a}_i + \mathfrak{b}_j = A$ for all $i = 1, \dots, n$, $j = 1, \dots, m$. $\mathfrak{a}_1 \cdots \mathfrak{a}_n + \mathfrak{b}_1 \cdots \mathfrak{b}_m = A$. In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals in A, then $\mathfrak{a}^n, \mathfrak{b}^m$ are also coprime ideals in A for all n, m.)

3. Let $0 \neq B$ be a free (more generally faithfully flat) algebra over a ring A. Show that a polynomial $f \in A[X]$ is separable over A if and only if it is separable over B.

4. Let k be a field and let $f_1, \dots, f_n \in k[X]$. Show that all polynomials $f_1, \dots, f_n$ are separable if and only if $\operatorname{lcm}(f_1, \dots, f_n)$ is separable.

5. Let k be a field of characteristic $p > 0$, $f \in k[X]$ be a monic prime polynomial of inseparability

degree e and $f = g(X^{p^e})$ with the separable polynomial $g \in k[X]$, $g \notin k[X^p]$ (see 3.B.15). Further, let K be a field extension of k and let $g = g_1 \cdots g_r$ be a prime factorisation of g into monic prime factors $g_1, \cdots, g_r \in K[X]$. For $j = 1, \cdots, r$ let p^{e_j} be the biggest p-th power such that $g_j(X^{p^{e_j}})$ is a p^{e_j}-th power in $K[X]$ and let $g_j(X^{p^{e_j}}) = \pi_j^{p^{e_j}}$, $j = 1, \cdots, r$. Then show that π_j is prime in $K[X]$ with inseparability degree $e'_j = e - e_j$ and $f = \pi_1^{p^{e_1}} \cdots \pi_r^{p^{e_r}}$ is the monic prime factorisation of f in $K[X]$.

(Example Let k be a field of characteristic $p > 0$ and let $e, e_1, \cdots, e_r$ be natural numbers with $e_j \leq e$ for all $j = 1, \cdots, r$. Further, let $S_1, \cdots, S_r$ denote the elementary symmetric polynomials in the indeterminates $X_1, \cdots, X_r$ and $X_j^{1/p^{e_j}}$ be a p^{e_j}-th root of X_j in a field extension of $k(X_1, \cdots, X_r)$, $j = 1, \cdots, r$. Then the irreducible polynomial

$$f = X^{rp^e} - S_1 X^{(r-1)p^e} + \cdots + (-1)^r S_r$$

over $L := k(S_1, \cdots, S_r)$, has the prime factorisation

$$f = \left(X^{p^{e'_1}} - X_1^{1/p^{e_1}}\right)^{p^{e_1}} \cdots \left(X^{p^{e'_r}} - X_r^{1/p^{e_r}}\right)^{p^{e_r}}$$

over $K = k\left(X_1^{1/p^{e_1}}, \cdots, X_r^{1/p^{e_r}}\right)$, where $e'_j := e - e_j$ for all $j = 1, \cdots, r$

6. Let k be a field of characteristic p. Show that every polynomial $X^p - X - a \in k[X]$ with $a \notin \{x^p - x \mid x \in k\}$ is a separable prime polynomial.