Chapter 12

Additive polynomials

12.1 Definition and basic properties

A polynomial $f \in K[X]$ is called **additive** if

$$f(a+b) \;=\; f(a) + f(b) \tag{12.1}$$

for all elements a, b in every extension field L of K, that is, if the map induced by f on L is an endomorphism of the additive group $(L, +)$. In our definition, the field K only appears as a field which conytains the coefficients of f. It is easy to see that a polynomial which is additive on K is also additive on every extension field of K.

It follows from the definition that an additive polynomial cannot have a non-zero constant term. If $\operatorname{char} K = p > 0$, then the map $a \mapsto a^p$ is an endomorphism of K, called the **Frobenius**. Therefore, the polynomial X^p is additive over any field of characteristic p. Another famous and important additive polynomial is $\wp(X) := X^p - X$, the additive **Artin-Schreier polynomial**.

Note that there are polynomials defined over a finite field which are not additive, but satisfy the condition for all elements coming from that field. For example, we know that $a^p = a$ and thus $a^{p+1} - a^2 = 0$ for all $a \in \mathbb{F}_p$. Hence, the polynomial $g(X) := X^{p+1} - X^2$ satisfies $g(a+b) = 0 = g(a) + g(b)$ for all $a, b \in \mathbb{F}_p$. But it is not an additive polynomial. To show this, let us take an element ϑ in the algebraic closure of $\mathbb{F}_p$ such that $\vartheta^p - \vartheta = 1$. Then $g(\vartheta) = \vartheta(\vartheta^p - \vartheta) = \vartheta$. On the other hand, $g(\vartheta+1) = (\vartheta+1)((\vartheta+1)^p - (\vartheta+1)) = (\vartheta+1)(\vartheta^p + 1^p - \vartheta - 1) = \vartheta + 1 \neq \vartheta = g(\vartheta) + g(1)$. Hence, already on the extension field $\mathbb{F}_p(\vartheta)$, the polynomial g does not satisfy the additivity condition.

We will now work towards a characterization of all additive polynomials. We start with the following lemma.

Lemma 12.1 *Let p be the characteristic exponent of the field K (i.e., $p = \operatorname{char} K$ if this is positive, and $p = 1$ otherwise). Take $f \in K[X]$ and consider the following polynomial in two variables:*

$$g(X, Y) \;:=\; f(X+Y) - f(X) - f(Y)\,. \tag{12.2}$$

If there is a subset A of cardinality at least $\deg f$ in some extension field of K such that g vanishes on $A \times A$, then f is additive and of the form

$$f(X) \;=\; \sum_{i=0}^{m} c_i X^{p^i} \quad \text{with } c_i \in K\,. \tag{12.3}$$

Proof: Assume that there is a subset A of cardinality at least $\deg f$ in some extension field of K such that g vanishes on $A \times A$. Take L to be any extension field of K. By field amalgamation, we may assume that A is contained in an extension field L' of L. For all $c \in L'$, the polynomials $g(c, Y)$ and $g(X, c)$ are of lower degree than f. This follows from their Taylor expansion. Assume that there exists $c \in L$ such that $g(c, Y)$ is not identically 0. Since A has more than $\deg g(c, Y)$ many elements, it follows that there must be $a \in A$ such that $g(c, a) \neq 0$. Consequently, $g(X, a)$ is not identically 0. But since A has more than $\deg g(X, a)$ many elements, this contradicts the fact that $g(X, a)$ vanishes on A. This contradiction shows that $g(c, Y)$ is identically 0 for all $c \in L$. That is, g vanishes on $L \times L$. Since this holds for all extension fields L of K, we have proved that f is additive.

By what we have shown, $g(c, Y)$ vanishes identically for every c in any extension field of K. That means that the polynomial $g(X, Y) \in K(Y)[X]$ has infinitely many zeros. Hence, it must be identically 0. Write $f = d_n X^n + \ldots + d_0$. Then $g(X, Y)$ is the sum of the forms $d_j(X + Y)^j - d_j X^j - d_j Y^j$ of degree j, $1 \leq j \leq \deg f$. Since g is identically 0, the same must be true for each of these forms and thus for all $(X + Y)^j - X^j - Y^j$ for which $d_j \neq 0$. But $(X + Y)^j - X^j - Y^j \equiv 0$ can only hold if j is a power of the characteristic exponent of K. Hence, $d_j = 0$ if j is not a power of p. Setting $c_i := d_{p^i}$, we see that f is of the form (12.3). □

Theorem 12.2 *The additive polynomials over a field K are precisely the polynomials of the form (12.3), where p is the characteristic exponent of K.*

Proof: Suppose that $f \in K[X]$ is additive. Then the polynomial g defined in (12.2) vanishes on every extension field L of K. Choosing L to be infinite and taking $A = L$, we obtain from the foregoing lemma that f is of the form (12.3).

Conversely, for every $i \in \mathbb{N}$, the map $x \mapsto x^{p^i}$ is a homomorphism on every field of characteristic exponent p. Hence, every monomial $c_i X^{p^i}$ is additive, and so is the polynomial $\sum_{i=0}^{m} c_i X^{p^i}$. □

This theorem shows that over a field of characteristic 0, every additive polynomial is of the form cX with $c \in K$.

Corollary 12.3 *Take $f \in K[X]$.*
a) If f is additive, then the set of its roots in the algebraic closure $\tilde{K}$ of K is a subgroup of the additive group of $\tilde{K}$. Conversely, if the latter holds and f has no multiple roots, then f is additive.
b) If f satisfies condition (12.1) on a field with at least $\deg f$ many elements, then f is additive.

Proof: a): If f is additive and a, b are roots of f, then $f(a + b) = f(a) + f(b) = 0$; hence $a + b$ is also a root. Further, $f(0) = f(0 + 0) = f(0) + f(0)$ shows that $0 = f(0) = f(a - a) = f(a) + f(-a) = f(-a)$, so 0 and $-a$ are also roots. This shows that the set of roots of f form a subgroup of $(\tilde{K}, +)$.

Now assume that the set A of roots of f forms a subgroup of $(\tilde{K}, +)$, and that f has no multiple roots. The latter implies that A has exactly $\deg f$ many elements. Since $A + A = A$, the polynomial $g(X, Y) = f(X + Y) - f(X) - f(Y)$ vanishes on $A \times A$. Hence by Lemma 12.1, f is additive.

b): This is an immediate application of Lemma 12.1. □

Exercise 12.1 *a) Let K be a finite field. Give an example of a polynomial $f \in K[X]$ which is not additive but induces an additive map on $(K,+)$.*

b) Show that the second assertion in part a) of Lemma 12.3 fails if we drop the condition that f has no multiple roots. Replace this condition by a suitable condition on the multiplicity of the roots.

b) Deduce Lemma 12.3 from the theorem of Artin as cited in [LANG3], VIII, §11, Theorem 18.

12.2 Rings of additive polynomials

Throughout, assume that $\operatorname{char} K = p > 0$. Then as a map on K, X^p is equal to the Frobenius endomorphism φ. Similarly, X^{p^2} is equal to the composition of φ with itself, written as φ^2, and by induction, we can replace 2 by every integer n. On the other hand, the monomial X induces the identity map, which we may write as φ^0. Note that addition and composition of additive maps on $(K,+)$ give again additive maps (in particular, addition of additive polynomials gives additive polynomials). It remains to interpret the coefficients of additive polynomials as maps. This is easily done by viewing K as a K-vector space: the map $c\cdot$ induced by $c \in K$ is given by multiplication $a \mapsto ca$, and it is an automorphism of $(K,+)$ if $c \neq 0$. So cX^{p^n} as a map is the composition of φ^n with $c\cdot$. We will write this composition as $c\varphi^n$. Adding these monomials generates new additive maps of the form $\sum_{i=0}^m c_i\varphi^i$, and addition of such maps gives again additive maps of this form. Composition of such additive maps generates again additive maps, and the reader may compute that they can again be written in the above form. In this way, we are naturally led to considering the ring $K[\varphi]$ of all polynomials in φ over K, where multiplication is given by composition. From the above we see that this ring is a subring of the endomorphism ring of the additive group of K. The correspondence that we have worked out now reads as

$$\sum_{i=0}^m c_i X^{p^i} \quad \longleftrightarrow \quad \sum_{i=0}^m c_i\varphi^i \in K[\varphi] \tag{12.4}$$

which means that both expressions describe the same additive map on K. For instance, the additive **Artin-Schreier polynomial** $\wp(X) = X^p - X$ corresponds to $\varphi - 1$. Through the above correspondence, the ring $K[\varphi]$ may be considered as the **ring of additive polynomials over** K. Note that this ring is not commutative; in fact, we have

$$\varphi c = c^p\varphi \quad \text{for all } c \in K\ .$$

This shows that assigning $\varphi \mapsto z$ induces an isomorphism of $K[\varphi]$ onto the skew polynomial ring $K[z;\varphi]$. But we will keep the notation "$K[\varphi]$" since it is simpler.

Let us state some basic properties of the ring $K[\varphi]$. We need the following definitions. (For deeper information about the following notions, see the comprehensive book "Free rings and their relations" by P. M. Cohn ([COHN1], [COHN2]). Let R be a ring with 1. Equipped with a function $\deg : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$, the ring R is called **left euclidean** if for all elements $s, s' \in R$, $s \neq 0$, there exist $q, r \in R$ such that

$$s' = qs + r \quad \text{with} \quad r = 0 \ \text{ or } \ \deg r < \deg s\ ,$$

and it is called **right euclidean** if the same holds with "$s' = sq + r$" in the place of "$s' = qs + r$". (Usually, the function deg is extended to 0 by setting $\deg 0 = -\infty$.) For example, polynomial rings over fields equipped with the usual degree function are both-sided euclidean rings. Further, an integral domain R is called a **left principal ideal domain** if every left ideal in R is principal (and analogously for "right" in the place of "left"). We leave it to the reader to show that every left (or right) euclidean integral domain is a left (or right) principal ideal domain. Finally, an integral domain R is called a **left Ore domain** if

$$Rr \cap Rs \neq \{0\} \quad \text{for all } r, s \in R \setminus \{0\} \ ,$$

and it is called a **right Ore domain** if $rR \cap sR \neq \{0\}$ for all $r, s \in R \setminus \{0\}$. Every left (or right) Ore domain can be embedded in a skew field (cf. [COHN1], §0.8, Corollary 8.7). The reader may prove that a left (or right) principal ideal domain is a left (or right) Ore domain.

The ring $K[\varphi]$ may be equipped with a degree function which satisfies $\deg 0 = -\infty$ and $\deg \sum_{i=0}^{m} c_i \varphi^i = m$ if $c_m \neq 0$. This degree function is a homomorphism of the multiplicative monoid of $K[\varphi] \setminus \{0\}$ onto $\mathbb{N} \cup \{0\}$ since it satisfies $\deg rs = \deg r + \deg s$. In particular, this shows that $K[\varphi]$ is an integral domain. The following theorem is due to Oystein Ore [ORE2]:

Theorem 12.4 *The ring $K[\varphi]$ is a left euclidean integral domain and thus also a left principal ideal domain and a left Ore domain. It is right euclidean if and only if K is perfect; if K is not perfect, then $K[\varphi]$ is not even right Ore.*

Proof: Take $s = \sum_{i=0}^{m} c_i \varphi^i$ and $s' = \sum_{i=0}^{n} d_i \varphi^i$. If $\deg s' < \deg s$, then we set $q = 0$ and $r = s'$. Now assume that $\deg s' = n \geq m = \deg s$. Then

$$\deg(s' - d_n c_m^{-p^{n-m}} \varphi^{n-m}\, s) \leq n - 1 < \deg s' \ .$$

Now take $q \in K[\varphi]$ such that $\deg(s' - qs)$ is minimal. Then $\deg(s' - qs) < \deg s$. Otherwise, we could apply the above to $s' - qs$ in the place of s', finding some $q' \in K[\varphi]$ such that $\deg(s' - (q + q')s) = \deg(s' - qs - q's) < \deg(s' - qs)$ contradicting the minimality of q. Setting $r = s' - qs$, we obtain $s' = qs + r$ with $\deg r < \deg s$. We have proved that $K[\varphi]$ is left euclidean. If K is perfect, hence $K = K^{p^m}$, then we also have that

$$\deg(s' - s\,(c_m^{-1} d_n)^{1/p^m} \varphi^{n-m}) \leq n - 1 < \deg s' \ ,$$

and in the same way as above one deduces that $K[\varphi]$ is right euclidean.

Now assume that K is not perfect and choose some element $c \in K$ not admitting a p-th root in K. Then $K^p \cap cK^p = \{0\}$ and

$$\varphi K[\varphi] \ \cap \ c\varphi K[\varphi] = \{0\}$$

since every nonzero additive polynomial in the set $\varphi K[\varphi]$ has coefficients in K^p whereas every nonzero additive polynomial in $c\varphi K[\varphi]$ has coefficients in cK^p. □

Example 12.5 The ring $\mathbb{F}_p[\varphi]$ is a both-sided euclidean integral domain, and every field of characteristic p is a left $\mathbb{F}_p[\varphi]$-module, where the action of φ on K is just the application of the Frobenius endomorphism. K is perfect if and only if every element of K is divisible by the ring element φ. But this does not imply that K is a divisible $\mathbb{F}_p[\varphi]$-module. For instance, if K admits Artin-Schreier extensions, that is, if $K \neq \wp(K) = (\varphi - 1)K$, then there are elements in K which are not divisible by $\varphi - 1$. On the other hand, K is a divisible $\mathbb{F}_p[\varphi]$-module if K is algebraically closed.

Observe that K is not torsion free as an $\mathbb{F}_p[\varphi]$-module. Indeed, K contains $\mathbb{F}_p$ which satisfies

$$(\varphi - 1)\mathbb{F}_p = \{0\} .$$

If k is any subfield of K, then K is also a $k[\varphi]$-module. Again, K is a divisible $K[\varphi]$-module if K is algebraically closed. ♢

Remark 12.6 Let us state some further properties of the ring $K[\varphi]$ which follow from Theorem 12.4. More generally, let R be any left principal ideal domain. Then R is a left free ideal ring (fir), and it is thus a semifir, i.e., every finitely generated left or right ideal is free of unique rank (note that this property is left-right symmetrical, cf. [COHN2], Chapter 1, Theorem 1.1). Consequently, every finitely generated submodule of a (left or right) free R-module is again free, cf. [COHN2], Chapter 1, Theorem 1.1 . On the other hand, every finitely generated torsion free (left or right) R-module is embeddable in a (finitely generated) free R-module if and only if R is right Ore, cf. [COHN2], Chapter 0, Corollary 9.5 and [GENT], Proposition 4.1 . Being a semifir, R is right Ore if and only if it is a right Bezout ring. But if R is not right Ore, then it contains free right ideals of arbitrary finite or countable rank, and R is thus not right noetherian, cf. [COHN2], Chapter 0, Proposition 8.9 and Corollary 8.10 . Every projective (left or right) R-module is free, cf. [COHN2], Chapter 1, Theorem 4.1 . A right R-module is flat if and only if it is torsion free, and a left R-module M is flat if and only if every finitely generated submodule of M is free, cf. [COHN2], Chapter 1, Corollary 4.7 and Proposition 4.5 . In view of the above, the latter is the case if and only if every finitely generated submodule of M is embeddable in a free R-module. Further, a left R-module M is flat if and only if for every $n \in \mathbb{N}$ and all right linearly independent elements $r_1, \ldots, r_n \in R$,

$$\forall x_1, \ldots, x_n \in M : \ \sum r_i x_i = 0 \ \Rightarrow \ \forall i : \ x_i = 0 ,$$

cf. [COHN1], Chapter 1, Lemma 4.3 . As a semifir, R is a coherent ring. Finally, since R is left Ore, it can be embedded in a skew field of left fractions, cf. [COHN2], Chapter 0, Corollary 8.7 .

Note that in particular, the above shows that all finitely generated torsion free (left or right) $K[\varphi]$-modules are free if and only if K is perfect, that is, $K[\varphi]$ is euclidean on both sides.

Exercise 12.2 *Describe the relation of the degree functions on $K[X]$ and $K[\varphi]$ via the correspondence (12.4), giving thereby a proof of* $\deg rs = \deg r + \deg s$. *Show that it also satisfies* $\deg r + s \leq \max\{\deg r, \deg s\}$ *with equality holding if* $\deg r \neq \deg s$. *Can it be transformed into a valuation?*

12.3 Frobenius-closed bases of function fields

If $F|K$ is an extension of fields of characteristic $p > 0$, then a K-basis B of $F|K$ will be called **Frobenius-closed** if $B^p \subset B$, where $B^p = \{b^p \mid b \in B\} = \varphi B$. We will need Frobenius-closed bases because of the following property:

Lemma 12.7 *Take a Frobenius-closed basis z_j, $j \in J$, of $F|K$. If the sum*

$$s = \sum_{i \in I} c_i z_i \,, \quad c_i \in K \,, \; I \subset J \text{ finite}$$

is a p-th power, then for every $i \in I$ with $c_i \neq 0$, the basis element z_i is a p-th power of a basis element.

Proof: Assume that

$$s = \left(\sum_{j \in J_0} c_j{}' z_j \right)^p \,, \quad c_j{}' \in K$$

where $J_0 \subset J$ is a finite index set. Then

$$\sum_{i \in I} c_i z_i = s = \sum_{j \in J_0} (c_j{}')^p z_j^p$$

where the elements z_j^p are also basis elements by hypothesis, which shows that every z_i which appears on the left hand side (i.e., $c_i \neq 0$) equals a p-th power z_j^p appearing on the right hand side. □

We will show the existence of Frobenius-closed bases for algebraic function fields of transcendence degree 1 over a perfect field of characteristic $p > 0$, provided that K is relatively algebraically closed in F. We first prove the following:

Lemma 12.8 *If F is an algebraic function field of transcendence degree 1 over an algebraically closed field K of arbitrary characteristic and q is an arbitrary natural number > 1, then there exists a basis of $F|K$ which is closed under q-th powers.*

If $F = K(x)$ is a rational function field, then our lemma follows from the **Partial Fraction Decomposition**: Every element $f \in F$ has a unique representation

$$f = c + \sum_{n>0} c_n x^n + \sum_{a \in K} \sum_{n>0} c_{a,n} \frac{1}{(x-a)^n}$$

where only finitely many of the coefficients $c, c_n, c_{a,n} \in K$ are nonzero. If we put

$$t_a = \frac{1}{x-a} \,, \quad t_\infty = x$$

then it follows that the elements

$$1, \; t_a^n \;\text{ with }\; a \in K \cup \{\infty\}, \; n \in \mathbb{N}$$

form a K-basis of F; this basis has the property that **every** power of a basis element is again a basis element.

For general function fields the Partial Fraction Decomposition remains true in a modified form (according to Helmut Hasse) that we shall describe now. At this point, we need the Riemann-Roch Theorem. In order to apply it, we have to introduce some notation. In what follows, we always assume that K is relatively algebraically closed in F. A **divisor**

of $F|K$ is an element of the (multiplicatively written) free abelian group generated by all places of $F|K$. By a place of $F|K$ we mean a place of F which is trivial on K, i.e., $P|_K = \mathrm{id}$. The places themselves are called **prime divisors**. A divisor may thus be written in the form

$$A = \prod_P P^{v_P A}$$

where the product is taken over all places of $F|K$ and the $v_P A$ are integers, only finitely many of them nonzero. Recall that we identify equivalent places. The **degree of a non-trivial place** P of $F|K$, denoted by $\deg P$, is defined to be the degree $[FP : K]$ (which is finite since $F|K$ is an algebraic function field in one variable, cf. Corollary 6.36). Accordingly, the **degree of a divisor** A, denoted by $\deg A$, is defined to be the integer $\sum_P v_P A \cdot \deg P$. The set

$$L(A) := \{f \in F \mid v_P f \geq -v_P A \text{ for all places } P \text{ of } F|K\}$$

is a K-vector space. Indeed, $0 \in L(A)$ since $v_P 0 = \infty > -v_P A$ for all places P of $F|K$. Further, $v_P(K^\times) = \{0\}$, hence $\forall c \in K^\times : \ v_P(cf) = v_P f$ for all P, so $f \in L(A)$ implies $cf \in L(A)$. Finally, if $f, g \in L(A)$, then $v_P(f-g) \geq \min\{v_P f, v_P g\} \geq -v_P A$ for all P, hence $f - g \in L(A)$. We write

$$\dim A \ := \ \dim_K L(A) \ .$$

The divisor A determines bounds for the zero and pole orders of the algebraic functions in $L(A)$. For example, if $A = P^n$ with n a natural number, then $f \in L(A)$ if and only if f has no pole at all (in which case it is a constant function) or has a pole at P of pole order at most $n = v_P A$.

Theorem 12.9 (Riemann-Roch)
Let $F|K$ be an algebraic function field in one variable with K relatively algebraically closed in F. There exists a smallest non-negative integer g, called the genus of $F|K$, such that

$$\dim A \geq \deg A - g + 1$$

for all divisors A of $F|K$. Furthermore,

$$\dim A = \deg A - g + 1$$

whenever $\deg A > 2g - 2$.

For the proof, see [DEU2].

Let P_∞ be a fixed place of $F|K$ and R^∞ the ring of all $f \in F$ which satisfy $v_P f \geq 0$ for every $P \neq P_\infty$. The following is an application of the Riemann-Roch Theorem:

Corollary 12.10 *For every $P \neq P_\infty$ there exists an element $t_P \in F$ such that*

$$\begin{aligned} v_P t_P &= -1 \\ v_Q t_P &\geq 0 \quad \text{for } Q \neq P, P_\infty \ . \end{aligned}$$

Proof: If we choose $n \in \mathbb{N}$ as large as to satisfy $n \dim P_\infty > 2g-2$, then by the Riemann-Roch Theorem,

$$\dim(P + nP_\infty) = \dim P + n \dim P_\infty - g + 1 > n \dim P_\infty - g + 1 = \dim nP_\infty \ .$$

Hence there is an element $t_P \in L(P + nP_\infty) \setminus L(nP_\infty)$. This element has the required properties. □

We return to the proof of our lemma, assuming that K is algebraically closed. Hence, K is the residue field of every place P of $F|K$ (that is, $\deg P = 1$). Every t_P of the foregoing corollary is the inverse of a uniformizing parameter for P. Every $f \in F$ can be expanded P-adically with respect to such a uniformizing parameter, and the principal part appearing in this expansion has the form

$$h_P(f) = \sum_{n>0} c_{P,n} t_P^n \ ,$$

where only finitely many of the coefficients $c_{P,n} \in K$ are nonzero, namely $n \le -v_P f$. By construction, t_P has only a single pole $\neq P_\infty$ and this pole is P; the same holds for $h_P(f)$ (if $h_P(f) \neq 0$). Consequently,

$$h = f - \sum_{P \neq P_\infty} h_P(f)$$

has no pole other than P_∞ and is thus an element of R^∞. We have shown that f has a unique representation

$$f = h + \sum_{P \neq P_\infty} \sum_{n>0} c_{P,n} t_P^n$$

with coefficients $c_{P,n} \in K$ and an element $h \in R^\infty$. This shows that the elements

$$t_P^n \ \text{ with } \ P \neq P_\infty, \ n \in \mathbb{N}$$

form a K-basis of F modulo R^∞ which has the property that every power of a basis element is again a basis element.

Now it remains to show that R^∞ admits a basis which is closed under q-th powers. An integer $n \in \mathbb{N}$ is called **pole number** of P_∞ if there exists $t_n \in R^\infty$ such that $v_{P_\infty} t_n = -n$. Let $H_\infty \subseteq \mathbb{N}$ be the set of all pole numbers. Fixing a t_n for every $n \in H_\infty$, we get a K-basis

$$1, \ t_n \ \text{ with } \ n \in H_\infty$$

of R^∞. To get a basis which is closed under q-th powers, we have to carry out our choice as follows:

Observe that H_∞ is closed under addition; in particular

$$qH_\infty \subset H_\infty \ .$$

For every $m \in H_\infty \setminus qH_\infty$ we choose an arbitrary element $t_m \in R^\infty$ with $v_{P_\infty} t_m = -m$. Every $n \in H_\infty$ can uniquely be written as

$$n = q^\nu m \ \text{ where } \ \nu \ge 0 \ \text{ and } \ m \in H_\infty \setminus qH_\infty \ .$$

Accordingly we put

$$t_n = t_m^{q^\nu}$$

which implies

$$v_{P_\infty} t_n = q^\nu \cdot v_{P_\infty} t_m = -q^\nu m = -n \ .$$

This construction produces a K-basis

$$1,\ t_m^{q^\nu} \ \text{ with } \ m \in H_\infty \setminus qH_\infty,\ \nu \geq 0$$

of R^∞, which is closed under q-th powers. This concludes the proof of our lemma.

For the generalization of this lemma to perfect ground fields of characteristic $p > 0$ we have to choose $q = p$:

Theorem 12.11 *Let F be an algebraic function field of transcendence degree 1 over a perfect field K of characteristic $p > 0$. If K is relatively algebraically closed in F, then there exists a Frobenius-closed basis for $F|K$.*

Proof: If K is not algebraically closed, we have to modify the proof of the previous lemma since not every place P of K has degree 1. (Such a modification is also necessary for the Partial Fraction Decomposition in $K(x)$ if K is not algebraically closed.) The modification reads as follows:

For every place P of $F|K$, let

$$d_P = \deg P = [FP : K]$$

be the degree of P. For every $P \neq P_\infty$ we choose elements $u_{P,i} \in R^\infty$, $1 \leq i \leq d_P$, such that their residues $u_{P,1}P, ..., u_{P,d_P}P$ form a K-basis of FP. We note that for every $\nu \geq 0$, the p^ν-th powers $u_{P,i}^{p^\nu}$ of these elements have the same property: their P-residues also form a K-basis of FP since K is perfect.
We write every $n \in \mathbb{N}$ in the form

$$n = p^\nu m \ \text{ with } \ m \in \mathbb{N},\ (p, m) = 1,\ \nu \geq 0$$

and observe that the elements

$$u_{P,i}^{p^\nu} t_P^n \ \text{ with } \ P \neq P_\infty,\ n \in \mathbb{N},\ 1 \leq i \leq d_P$$

form a Frobenius-closed K-basis of F modulo R^∞.

It remains to construct a Frobenius-closed K-basis of R^∞. This is done as follows: We consider the K-vector spaces

$$L_n = L(nP_\infty) = \{x \in F \mid v_{P_\infty} x \geq -n \text{ and } v_P(x) \geq 0 \text{ for } P \neq P_\infty\} \ .$$

By our assumption that K is relatively algebraically closed in F, we have $L_0 = K$. Further,

$$R^\infty \ = \bigcup_{n \in \mathbb{N}} L_n \ .$$

We set

$$d_{\infty,n} \ := \ \dim L_n / L_{n-1} \ \geq \ 0 \ .$$

(Note that by the Riemann-Roch Theorem, $d_{\infty,n} = [FP_\infty : K]$ holds for large enough n; cf. the proof of the above corollary.) Now for $n = 1, 2, ...$ we shall choose succesively basis elements $t_{n,i} \in L_n$ modulo L_{n-1}. Then the elements

$$1,\ t_{n,i} \quad \text{with} \quad n \in \mathbb{N},\ 1 \le i \le d_{\infty,n}$$

form a K-basis of R^∞. To obtain that this basis is Frobenius-closed, we organize our choice as follows:

If $n = pm$, the p-th powers $t_{m,i}^p \in L_n$ are linearly independent modulo $L_{p(m-1)}$ and even modulo $L_{pm-1} = L_{n-1}$. This fact follows from our hypothesis that K is perfect: the existence of nonzero elements $c_i \in K$ with $\sum c_i t_{m,i}^p \in L_{pm-1}$, i.e., $v_{P_\infty} \sum c_i t_{m,i}^p > -pm$, would yield $v_{P_\infty} \sum c_i^{1/p} t_{m,i} > -m$, hence $\ge -m+1$, showing that $\sum c_i^{1/p} t_{m,i} \in L_{m-1}$, which is a contradiction. In our choice of the elements $t_{n,i}$ we are thus free to take all the elements $t_{m,i}^p$ and to extend this set to a basis of L_n modulo L_{n-1} by arbitrary further elements, if necessary (for n large enough, the elements $t_{m,i}^p$ will already form such a basis). This procedure guarantees that the p-th power of every basis element $t_{m,i}$ is again a basis element, namely equal to $t_{pm,j}$ for suitable j. Hence a basis constructed in this way will be Frobenius-closed. □

Let $F|K$ be an arbitrary extension of fields of characteristic $p > 0$. Both F and K are $K[\varphi]$-modules, and so is the quotient module F/K. Suppose that F/K is a free $K[\varphi]$-module. Then it admits a $K[\varphi]$-basis. Let $B_0 \subset F$ be a set of representatives for such a $K[\varphi]$-basis of F/K. It follows that

$$B = \bigcup_{n=0}^{\infty} B_0^{p^n} \cup \{1\} = \bigcup_{n=0}^{\infty} \varphi^n B_0 \cup \{1\}$$

is a set of generators of the K-vector space F. By our construction of B, every K-linear combination of elements of $B \setminus \{1\}$ may be viewed as a $K[\varphi]$-linear combination of elements of B_0. This shows that the elements of B are K-linearly independent, and B is thus a Frobenius-closed basis of $F|K$. Note that B_0 is the basis of a free $K[\varphi]$-submodule M of F which satisfies $F = M \oplus K$.

The converse to this procedure would mean to extract a $K[\varphi]$-basis B_0 from a Frobenius-closed K-basis B. But B_0 can only be found if for every element $b \in B \setminus \{1\}$ there is some element b_0 which is not a p-th power in F and such that $b = b_0^{p^n}$ for some $n \in \mathbb{N} \cup \{0\}$. This will hold if no element of $F \setminus K$ has a p^n-th root for every $n \in \mathbb{N}$.

Lemma 12.12 *If $F|K$ is an algebraic function field (of arbitrary transcendence degree), and if K is relatively algebraically closed in F, then no element of $F \setminus K$ has a p^n-th root for every $n \in \mathbb{N}$.*

Proof: Let $f \in F \setminus K$. Since K is relatively algebraically closed in F, we know that f is transcendental over K. So we may choose a transcendence basis $\mathcal{T}$ of $F|K$ containing f. According to Lemma **??**, we may choose a K-rational valuation v on the rational function field $K(\mathcal{T})$ such that the values of all elements in $\mathcal{T}$ are rationally independent. This yields that $vK(\mathcal{T}) = \bigoplus_{t \in \mathcal{T}} \mathbb{Z} vt$. In particular, vf is not divisible by p in $vK(\mathcal{T})$. Since $F|K(\mathcal{T})$ is finite, the same is true for $(vF : vK(\mathcal{T}))$ by Lemma 6.13. This yields that there is some

$n \in \mathbb{N}$ such that vf is not divisible by p^n in vF. Hence, f does not admit a p^n-th root in F. □

This lemma shows that if $F|K$ is an algebraic function field with K relatively algebraically closed in F, admitting a Frobenius-closed basis B and if we let B_0 be the set of all elements in B which do not admit a p-th root in F, then we obtain $B = \bigcup_{n=0}^{\infty} B_0^{p^n} \cup \{1\}$. Since the elements of B are K-linearly independent, the elements of B_0 are $K[\varphi]$-linearly independent over K. Moreover, B_0 is a set of generators of the $K[\varphi]$-module F over K. Hence, the set B_0/K is a $K[\varphi]$-basis of F/K. We have thus proved:

Proposition 12.13 *Let $F|K$ be an algebraic function field (of arbitrary transcendence degree), and K relatively algebraically closed in F. Then F admits a Frobenius-closed K-basis if and only if F/K is a free $K[\varphi]$-module.*

Theorem 12.11 now reads as follows:

Theorem 12.14 *If F is an algebraic function field of transcendence degree 1 over a perfect field K of characteristic $p > 0$ and if K is relatively algebraically closed in F, then F/K is a free $K[\varphi]$-module.*

Open Problem 12.1 Do Theorems 12.11 and 12.14 also hold for transcendence degree > 1?

Open Problem 12.2 Do Theorems 12.11 and 12.14 also hold if the assumption that K be perfect is replaced by the assumption that $F|K$ be separable? Note that if K is not perfect, then there exist places P of $F|K$ such that $FP|K$ is not separable, even if $F|K$ is separable. In this case, the construction of the proof of Theorem 12.11 breaks down and it cannot be expected that there is a Frobenius-closed K-basis of F which is as "natural" as the ones produced by that construction.

Exercise 12.3 *Show that F/K cannot be a free $K[\varphi]$-module if K is not relatively algebraically closed in F. Does there exist an algebraic field extension which admits a Frobenius-closed basis? Prove a suitable version of Proposition 12.13 which does not use the assumption that K be relatively algebraically closed in F.*

12.4 Valued fields as valued $K[\varphi]$-modules

We have seen already that every field of characteristic $p > 0$ may be viewed as a left module over a ring of additive polynomials. If the field is valued, then by our general definition, it will be a valued module over this ring. We also have seen that the module may not be torsion free. So it cannot be expected that the valuation is compatible with the module structure in any "classical" sense.

Example 12.15 The power series field $\mathbb{F}_p((t))$ and the fields $\mathbb{F}_p(t)$ and $\mathbb{F}_p(t)^h$ are valued $\mathbb{F}_p[\varphi]$- and $\mathbb{F}_p(t)[\varphi]$-modules. None of them is torsion free since they all contain $\mathbb{F}_p$. (One could also form the ring $\mathbb{F}_p[t, \varphi]$ and view these fields as valued $\mathbb{F}_p[t, \varphi]$-modules, but it seems that we already have enough open problems ...) ♢

It was indeed this example that led to our general definition of a valued module. The idea to view $\mathbb{F}_p((t))$ as a module admitting multiplication by t and application of φ is due to L. v. d. Dries. We will discuss later the open problems in connection with the structure and model theory of $\mathbb{F}_p((t))$, and we will see why it makes sense to view $\mathbb{F}_p((t))$ as a valued module over the rings $\mathbb{F}_p[\varphi]$ and $\mathbb{F}_p(t)[\varphi]$.

In the following, let $(L|K, v)$ be an extension of valued fields of characteristic $p > 0$. We wish to consider the valued $K[\varphi]$-module (L, v). Since every element of $K[\varphi]$ is a polynomial, we can make use of the results of the last section. Lemma **??** tells us:

Theorem 12.16 *Let $(L|K, v)$ be an extension of valued fields of characteristic $p > 0$. Then (L, v) is a finitely exceptional almost value-compatible left $K[\varphi]$-module.*

It seems that this structure is an important aspect of the structure theory for valued fields in positive characteristic. As we will see, it gives us information about the properties of the power series field $(\mathbb{F}_p((t)), v_t)$ that are particularly encoded in this structure and that can not be deduced from Hensel's Lemma or the fact that it is a defectless field. To our knowledge, the structure of such valued $K[\varphi]$-modules has not yet been studied. We have made a start by treating the theory of their immediate extensions in Section 3.8 in analogy to that of valued fields. Moreover, we have developed the theory of valued modules and the results of the last three sections of Chapter 2 having in mind the valued $K[\varphi]$-modules.

Let us see what Chapter 2 can tell us in the present situation. From assertion 3) of Lemma **??** and Corollary **??**, we can deduce:

Theorem 12.17 *Every additive polynomial on a valued field of characteristic $p > 0$ is a spherically continuous map.*

From this theorem together with Corollary **??** we obtain:

Corollary 12.18 *Let f be an additive polynomial on the valued field (L, v) of characteristic $p > 0$. If (G, v) is a spherically complete subgroup of (L, v), then also $(f(G), v)$ is a spherically complete subgroup of (L, v). If in addition $(f(G), v) \subset (L, v)$ is immediate, then $f(G) = L$.*

In the special case of a perfect field L, this corollary together with the approach of the last section provides a handy criterion for an additive polynomial to be surjective on a spherically complete field (L, v), or even for a an element to lie in the subgroup $f(L)$. Indeed, if L is perfect, then all monomials in f are surjective. So the only values of interest are precisely the critical values α_ℓ for f that we have introduced in the last section. A condition like (**??**) of Corollary **??** has only to be checked if the value $v(f(b) - c)$ is a critical value. We note:

Corollary 12.19 *Let f be an additive polynomial on the perfect spherically complete field (L, v) of characteristic $p > 0$. Assume that for every critical value $\alpha_\ell \in vL$ of f and every $c \in L$ of value $vc = \alpha_\ell$ there is some $b \in L$ such that $v(f(b) - c) > vc$. Then f is surjective on L. In particular, if no critical value of f lies in vL, then f is surjective on L.*

Example 12.20 Let (L, v) be a maximal immediate extension of $(\mathbb{F}_p((t))^{1/p^\infty}, v_t)$ and consider the additive polynomial $f(X) = X^p - tX$. Its only critical value is $\frac{1}{p-1} \notin \frac{1}{p^\infty}\mathbb{Z} = vL$. Hence, f is surjective on L. The same holds if we replace t by t^n with $n \in \mathbb{Z}$ not divisible by $p - 1$. $\diamondsuit$

Even more interesting for our further studies is the application of Corollary **??**:

Theorem 12.21 *Let $f_1, \ldots, f_n$ be additive polynomials on the valued field (L, v) of characteristic $p > 0$. Further, let $G_1, \ldots, G_n$ be spherically complete subgroups of (L, v). Assume that for every $a \in f_1(G_1) + \ldots + f_n(G_n)$,*

$$\exists b_i \in G_i : \; vf_i(b_i) \geq va \; (1 \leq i \leq n) \quad \textit{and} \quad v(f_1(b_1) + \ldots + f_n(b_n) - a) > va \; . \tag{12.5}$$

Then $f_1(G_1) + \ldots + f_n(G_n)$ is a spherically complete and spherically closed subgroup of (L, v). If (12.5) holds for every $a \in L$, then

$$L = f_1(G_1) + \ldots + f_n(G_n) \; .$$

More generally, if (H, v) is a v-convex subgroup of (L, v) and if (12.5) holds for every $a \in L$ with $va < vH$, then

$$L = f_1(G_1) + \ldots + f_n(G_n) + H \; .$$

Recall that every v-convex subgroup of a spherically complete field is spherically complete. Consequently, this theorem gives quite a lot of information on spherically complete fields of characteristic $p > 0$. We wish to illustrate this by applying it to the power series field $(\mathbb{F}_p((t)), v_t)$.

12.5 Additive decompositions of power series fields

From Corollary 14.11 we know that $(\mathbb{F}_p((t)), v_t)$ has valuation p-basis $1, t, \ldots, t^{p-1}$. So let us apply Theorem 12.21 to an arbitrary spherically complete field (L, v) having this valuation p-basis. We choose the following additive polynomials f_i and subgroups G_i of L:

$f_i = t^i X$ and $G_i = L$ for $1 \leq i \leq p-1$,

$f_p = \wp(X) = X^p - X$ and $G_p = L$,

$H = \mathcal{O}_{\mathbf{L}}$.

Now let $a \in L$ such that $va < 0$. Then we write

$$a = tc_1^p + t^2 c_2^p + \ldots + t^{p-1} c_{p-1}^p + c_p^p \; ,$$

using the hypothesis that $1, t, \ldots, t^{p-1}$ is a p-basis of L. Since this is even a valuation p-basis, we know that va is equal to the minimum of the values of the summands. Now we $b_i = c_i$ for $1 \leq i \leq p$. Then

$$v(f_1(b_1) + \ldots + f_p(b_p) - a) = v(tc_1^p + t^2 c_2^p + \ldots + t^{p-1} c_{p-1}^p + c_p^p - c_p - a) = vc_p \; .$$

If $vc_p < 0$, then $vc_p > vc_p^p \geq va$. Otherwise, $vc_p \geq 0 > va$. This shows that condition (12.5) is satisfied for all $a \in L$ such that $va < 0$. Hence, an application of Theorem 12.21 gives:

Lemma 12.22 *Let (L, v) be a spherically complete field (L, v) having valuation p-basis $1, t, \ldots, t^{p-1}$. Then*

$$L = \wp(L) + \mathcal{O}_{\mathbf{L}} + tL^p + \ldots + t^{p-1} L^p \; . \tag{12.6}$$

But note that Theorem 12.21 does not require that (L, v) be spherically complete. Even if it is not, it may have interesting valued subgroups which are spherically complete. For example, every subgroup with finite value set is spherically complete. More generally, if (G, v) is a valued subgroup such that vG admits no infinite ascending sequences, then (G, v) is spherically complete (cf. Section 1.3). Let us choose a group complement $\mathbf{A}$ for the valuation ring $\mathcal{O}_\mathbf{L}$ in the abelian group L (cf. our use of such group complements in Section 10.3, page 255. We leave it to the reader to prove that $v\mathbf{A}$ admits no infinite ascending sequences if and only if $vL = \{0\}$ or $vL \cong \mathbb{Z}$. In the latter case, we have that $v\mathbf{A} = \{n \in \mathbb{Z} \mid n < 0\}$, and $(\mathbf{A}, v)$ is spherically complete. Given $a \in L$ with $va < 0$, we choose c_i as before. Now we can choose $c_i' \in \mathbf{A}$ such that $c_i - c_i' \in \mathcal{O}_\mathbf{L}$. With $b_i = c_i'$, we obtain:

$$f_1(b_1) + \ldots + f_p(b_p) - a \equiv tc_1^p + t^2c_2^p + \ldots + t^{p-1}c_{p-1}^p + c_p^p - c_p - a = c_p \pmod{\mathcal{O}_\mathbf{L}},$$

which again shows that condition (12.5) is satisfied for all $a \in L$ such that $va < 0$. From Theorem 12.21, we obtain:

$$L = \wp(\mathbf{A}) + \mathcal{O}_\mathbf{L} + t\mathbf{A}^p + \ldots + t^{p-1}\mathbf{A}^p .$$

In particular:

Lemma 12.23 *The decomposition (12.6) also holds for all valued fields (L, v) with value group $vL \cong \mathbb{Z}$.*

Corollary 12.24 *The decomposition (12.6) holds if (L, v) is one of the fields $(\mathbb{F}_p(t), v_t)$, $(\mathbb{F}_p(t), v_t)^h$ or $(\mathbb{F}_p((t)), v_t)$ (or any intermediate field).*

If the field (L, v) is henselian (which it is if it is spherically complete), then $\mathcal{M}_\mathbf{L} \subset \wp(L)$ by Lemma 9.4. Hence in this case, (12.6) is equivalent to

$$L = \wp(L) + (\mathcal{O}_\mathbf{L}^\times \cup \{0\}) + tL^p + \ldots + t^{p-1}L^p . \tag{12.7}$$

If the residue field $\overline{L}$ is Artin-Schreier closed, then Lemma 9.4 tells us that $\mathcal{O}_\mathbf{L} \subset \wp(L)$, showing that (12.7) in turn is equivalent to

$$L = \wp(L) + tL^p + \ldots + t^{p-1}L^p \tag{12.8}$$

It was this decomposition in the case of an Artin-Schreier closed residue field that was noticed by L. v. d. Dries and led us to the consideration of such decompositions.

More generally, one can deduce decompositions like the following. Assume again that (L, v) is a spherically complete field of degree of inseparability p. Then the extension $(L|L^{p^n}, v)$ is of degree p^n and admits a valuation basis t_i, $1 \leq i \leq p^n$. Let $f_i \in \mathcal{O}_\mathbf{L}[X]$, $1 \leq i \leq p^n$, be monic additive polynomials of degree p^n. Then the following decomposition holds:

$$L = t_1 f_1(L) + \ldots + t_{p^n} f_{p^n}(L) + \mathcal{O}_L .$$

We do not know whether the decompositions deduced from Theorem 12.21 are stable under algebraic or finite extensions, but this seems unlikely. For instance, we have shown in Example 12.20 that the additive polynomial $X^p - tX$ is surjective on a maximal immediate extension (L, v) of the perfect hull of $(\mathbb{F}_p((t)), v)$. But if we adjoin a root s of the polynomial

$X^{p-1} - t$, which gives a maximal immediate extension of the perfect hull of the power series field $\mathbb{F}_p((s))$, then $s^p = st$, and st is not in the range of $X^p - tX$ on $L(s)$, because $X^p - X - 1$ is irreducible over $\mathbb{F}_p$. It seems more likely that the spherical closedness of subgroups as asserted by Theorem 12.21 is stable under finite extensions, perhaps under additional conditions.

We also do not know whether the decompositions deduced from Theorem 12.21 are the only properties of this type of the power series field $\mathbb{F}_p((t))$. For instance, we do not know whether all similar properties involving arbitrary polynomials are consequences of Theorem 12.21 and the fact that $(\mathbb{F}_p((t)), v)$ is henselian defectless. Model theoretically speaking, we do not know all elementary properties of $\mathbb{F}_p((t))$. See Section 23 for further details. Let us only mention here that the structural information given by Theorem 12.21 is certainly of relevance for the examination of the elementary properties of $\mathbb{F}_p((t))$. In contrast to this open problem, we are able to describe the model theory of perfect valued fields (cf. Section 21.5). Probably it is more accessible because for perfect fields, the structure described by Theorem 12.21 is less complex. Note that if $L = L^p$ is perfect, then $t \in L$, yielding that $L = tL^p$ and that the above decompositions are trivially true.

12.6 Field extensions generated by p-polynomials

In this section, let K be a field of characteristic $p > 0$. A polynomial is called a **p-polynomial** if it is of the form $\mathcal{A}(X) + c$ where $\mathcal{A}(X)$ is an additive polynomial and c is a constant. Important examples for p-polynomials are the polynomials of the form $X^p - X - c$ which we have met already. If such a polynomial is irreducible, then each of its roots generates an Artin-Schreier extension. p-polynomials play an important role in valuation theory in positive characteristic, as we will see in several later chapters of this book.

A field extension $L|K$ is called **p-elementary extension** if it is a finite Galois extension and its Galois group is an elementary-abelian p-group, that is, an abelian p-group in which every non-zero element has order p. In particular, $[L : K]$ is a power of p.

In this section, we will consider the following larger class of all extensions $L|K$ which satisfy the following condition:

$$\left.\begin{array}{l}\text{there exists a Galois extension } K'|K \text{ which is linearly disjoint from } L|K,\\ \text{such that } L.K'|K' \text{ is a } p\text{-elementary extension}\\ \text{and also } L.K'|K \text{ is a Galois extension.}\end{array}\right\} \qquad (12.9)$$

From the linear disjointness it follows that $\operatorname{Gal} L.K'|L \cong \operatorname{Gal} K'|K$ and that $[L : K] = [L.K' : K']$ which yields that $[L : K] = p^n$ for some natural number n. For a further investigation of this situation, we will use the following notation. We set

$$L' := L.K'$$

and define

$G := \operatorname{Gal} L'|K$,
$N := \operatorname{Gal} L'|K' \lhd G$,
$H := \operatorname{Gal} L'|L \cong \operatorname{Gal} K'|K \cong G/N$.

The group N is abelian of order p^n. Since $K'|K$ is assumed to be a Galois extension, N is a normal subgroup of G. That is, N is a right G-module with scalar multiplication given

by conjugation:

$$(\sigma,\tau) \;\mapsto\; \sigma^\tau = \tau^{-1}\sigma\tau \quad \text{for all } \sigma \in N\,,\ \tau \in G\,.$$

Since $L.K' = L'$ and $L \cap K' = K$, we have that $H \cap N = 1$ and $G = HN$, that is, H is a group complement for N in G. As we have seen in the last section, every element $\sigma \in G$ admits a unique representation

$$\sigma = \sigma_H\sigma_N \quad \text{with } \ \sigma_H \in H\,,\ \sigma_N \in N\,. \tag{12.10}$$

Since N is abelian, the scalar multiplication of the G-module N reads as

$$\sigma^\tau = \tau_N^{-1}(\tau_H^{-1}\sigma\tau_H)\tau_N = \tau_H^{-1}\sigma\tau_H = \sigma^{\tau_H}\,. \tag{12.11}$$

The projection $\sigma \mapsto \sigma_N$ is a crossed homomorphism from G onto N, satisfying (24.11); it induces the identity on N, and its kernel is H.

Lemma 12.25 *If $L|K$ satisfies condition (12.9) then w.l.o.g., the extension $K'|K$ may assumed to be finite (which yields that also $L'|K$ is finite).*

Proof: Suppose that $K'|K$ is an arbitrary algebraic extension such that (12.9) holds. Let $N_0 := \{\tau \in G \mid \forall \sigma_N \in N:\ \tau^{-1}\sigma_N\tau = \sigma_N\}$ be the subgroup of all automorphisms in G whose action on N is trivial (i.e., N_0 is the centralizer of N in G). Since N is abelian, it is contained in N_0. Consequently, the fixed field K_0 of N_0 in L' is contained in K' (which is the fixed field of N in L' by definition of N). Since N is a normal subgroup of G, also its centralizer N_0 is a normal subgroup of G, showing that $K_0|K$ is a Galois extension. We set $H_0 := G/N_0$. By our choice of N_0, the action of G on N induces an action of H_0 on N which is given by $\rho^{-1}\sigma_N\rho = \tau^{-1}\sigma_N\tau$ for $\rho = \tau N_0 \in H_0$. Consequently, H_0 must be finite, being a group of automorphisms of the finite group N. This proves that $K_0|K$ is a finite Galois extension with Galois group H_0. Recall that it follows from (12.9) that also $L|K$ is finite.

We claim that $H \cap N_0$ is a normal subgroup of G. Let $\tau \in H \cap N_0$ and $\sigma \in G$; we want to show that $\tau^\sigma \in H \cap N_0$. Write $\sigma = \sigma_H\sigma_N$ according to (12.10). Then $\tau^\sigma = \sigma_N^{-1}(\sigma_H^{-1}\tau\sigma_H)\sigma_N$; since $\sigma_H \in H$ and $N_0 \lhd G$, we find that $\tau' := \sigma_H^{-1}\tau\sigma_H \in H \cap N_0$. In particular, τ' lies in the centralizer of N. In view of $\sigma_N \in N$ we obtain $\tau^\sigma = \sigma_N^{-1}\tau'\sigma_N = \sigma_N^{-1}\sigma_N\tau' = \tau' \in H \cap N_0$. We have proved that $H \cap N_0$ is a normal subgroup of G. With L_0 the fixed field of $H \cap N_0$ in L', we hence obtain a Galois extension $L_0|K$. Since $L_0 = L.K_0$, the extension $L_0|K$ is finite.

Finally, it remains to show that $\mathrm{Gal}\, L_0|K_0 \cong \mathrm{Gal}\, L'|K'$ which also yields that $L_0|K_0$ is p-elementary. Observe that $HN_0 = G$ since it contains $HN = G$. Now we compute: $\mathrm{Gal}\, L_0|K_0 = \mathrm{Gal}\, L'|K_0\,/\,\mathrm{Gal}\, L'|L_0 = N_0/(H \cap N_0) \cong H.N_0/H = G/H \cong N = \mathrm{Gal}\, L'|K'$. We have proved that condition (12.9) also holds with K_0, L_0 in the place of K', L'. $\square$

In view of this lemma, we will assume in the sequel that all field extensions are finite.

Like N, also the additive group $(L',+)$ is a right G-module, the scalar multiplication given by

$$(a,\tau) \;\mapsto\; a^\tau := \tau^{-1}a \quad \text{for all } a \in L'\,,\ \tau \in G\,.$$

Let us show:

Lemma 12.26 *There is an embedding $\phi : N \longrightarrow (L', +)$ of right G-modules.*

Proof: By the Normal Basis Theorem [LANG3], VIII, §12, Theorem 20, the finite Galois extension $K'|K$ admits a normal basis. That is, there exists $b \in K'$ such that b^ρ, $\rho \in \operatorname{Gal} K'|K$, is a basis of K' over K. Since H is a set of representatives in G for $\operatorname{Gal} K'|K$, we may represent these conjugates as b^ρ, $\rho \in H$. Let $\psi : N \to (K, +)$ be any homomorphism of groups (there is always at least the trivial one), and set

$$\phi(\sigma_N) := \sum_{\rho \in H} \psi(\rho \sigma_N \rho^{-1})\, b^\rho \quad \text{for all } \sigma_N \in N\,. \tag{12.12}$$

Since ψ is a group homomorphism from N into $(L', +)$, the same is true for ϕ. Given $\tau \in G$, we write $\tau = \tau_H \tau_N$; then $b^{\rho\tau} = (b^{\rho\tau_H})^{\tau_N} = b^{\rho\tau_H}$ since $b^{\rho\tau_H} \in K'$ and $\tau_N \in N = \operatorname{Gal} L'|K'$. Observing also that $H = H\tau_H$ and using (24.10), we compute:

$$\begin{aligned} \phi(\sigma_N)^\tau &= \sum_{\rho \in H} \psi(\rho \sigma_N \rho^{-1})\, b^{\rho\tau} = \sum_{\rho \in H} \psi(\rho \tau_H^{-1} \sigma_N (\rho \tau_H^{-1})^{-1})\, b^\rho \\ &= \sum_{\rho \in H} \psi(\rho \sigma_N^{\tau_H} \rho^{-1})\, b^\rho = \phi(\sigma_N^{\tau_H}) = \phi(\sigma_N^\tau) \end{aligned}$$

which shows that ϕ is a homomorphism of right G-modules.

Now we have to choose ψ so well as to guarantee that ϕ becomes injective. If $\phi(\sigma_N) = 0$ then $\psi(\rho \sigma_N \rho^{-1}) = 0$ for all $\rho \in H$ since by our choice of b, the conjugates b^ρ, $\rho \in H$, are linearly independent over K. In particular, $\phi(\sigma_N) = 0$ implies $\psi(\sigma_N) = 0$. Hence, ϕ will be injective if we are able to choose ψ to be injective. This is done as follows. The elementary-abelian p-group N may be viewed as a finite-dimensional $\mathbb{F}_p$-vector space. If K is an infinite field (which by our general assumption has characteristic p), then it contains $\mathbb{F}_p$-vector spaces of arbitrary finite dimension; so there exists an embedding ψ of N into $(K, +)$. If K is a finite field, then all finite extensions of K are cyclic, their Galois groups being generated by a suitable power of the Frobenius φ (as we have mentioned in Section 24.1); consequently, N must be cyclic. Since it is also elementary-abelian, N is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ which is the additive group of $\mathbb{F}_p \subset K$. Hence also in this case, N admits an embedding ψ into $(K, +)$. □

By composition with ϕ, the crossed homomorphism $\sigma \mapsto \sigma_N$ is turned into a map $\sigma \mapsto \phi(\sigma_N)$ from G into $(L', +)$. We shall write $\phi(\sigma)$ instead of $\phi(\sigma_N)$, thereby considering the G-module homomorphism $\phi : N \to (L', +)$ as being extended to $\phi : G \to (L', +)$. By construction, the latter has kernel H and is injective on N. Further, it satisfies $\phi(\sigma\tau) = \phi((\sigma\tau)_N) = \phi(\sigma_N^\tau \tau_N) = \phi(\sigma_N)^\tau + \phi(\tau_N) = \phi(\sigma)^\tau + \phi(\tau)$ showing that ϕ is a crossed homomorphism in the following sense:

$$\phi(\sigma\tau) = \phi(\sigma)^\tau + \phi(\tau) \quad \text{for all } \sigma, \tau \in G\,. \tag{12.13}$$

We claim that there exists an element $\vartheta \in L'$ such that

$$\vartheta^\tau = \vartheta + \phi(\tau) \quad \text{for all } \tau \in G\,. \tag{12.14}$$

Note that (12.14) determines ϑ up to addition of elements from K. (Indeed, ϑ' satisfies the same equation if and only if $(\vartheta - \vartheta')^\tau = \vartheta - \vartheta'$, i.e., if and only if $\vartheta - \vartheta' \in K$.)

The element ϑ can be constructed as follows. We choose an element $a \in L'$ such that the trace $s := \mathrm{Tr}_{L'|K}(a) = \sum_{\sigma\in G} \sigma a = \sum_{\sigma\in G} a^\sigma$ is not zero (we have seen in the foregoing proof that such an element exists: we could choose a to be the generator of a normal basis of $L'|K$; the linear independence will then force the trace to be nonzero). We set

$$\vartheta := -\frac{1}{s}\sum_{\sigma\in G} \phi(\sigma)\, a^\sigma \ . \tag{12.15}$$

Given $\tau \in G$, we have $G\tau = G$ and

$$1 = \frac{1}{s}\sum_{\sigma\in G} a^\sigma = \frac{1}{s}\sum_{\sigma\in G} a^{\sigma\tau}$$

which we use to compute

$$\begin{aligned}
\vartheta^\tau &= -\frac{1}{s}\sum_{\sigma\in G} \phi(\sigma)^\tau a^{\sigma\tau} \ = \ -\frac{1}{s}\sum_{\sigma\in G} ((\phi(\sigma)^\tau + \phi(\tau))a^{\sigma\tau} - \phi(\tau)a^{\sigma\tau}) \\
&= -\frac{1}{s}\sum_{\sigma\in G} \phi(\sigma\tau)a^{\sigma\tau} + \phi(\tau)\frac{1}{s}\sum_{\sigma\in G} a^{\sigma\tau} \\
&= -\frac{1}{s}\sum_{\sigma\in G} \phi(\sigma)a^{\sigma} + \phi(\tau)\frac{1}{s}\sum_{\sigma\in G} a^{\sigma} \ = \ \vartheta + \phi(\tau) \ .
\end{aligned}$$

This proves that ϑ indeed satisfies (12.14).

Remark 12.27 The additive analogue of Hilbert's Satz 90 (cf. [LANG3], VIII, §10 or [JAC], chapter 1, section 15) says that $\mathrm{H}^1(G,(L',+)) = 0$. Since the crossed homomorphism $\phi : \ G \to (L',+)$ may be interpreted as a 1-cocycle, this implies that ϕ splits, which indicates the existence of ϑ. Replacing the crossed homomorphism ϕ by an arbitrary 1-cocycle in our above computation provides a proof of this additive analogue.

Since H is the kernel of ϕ, (12.14) yields that H is the group of all automorphisms of $L'|K$ which fix ϑ. Since on the other hand, by definition of $H = \mathrm{Gal}\, L'|L$ the fixed field of H in L' is L, we know from Galois theory that $L = K(\vartheta)$. Let us now compute the minimal polynomial f of ϑ over K. The group N may be viewed as a system of representatives for the left cosets of G modulo H. Consequently, the elements ϑ^τ, $\tau \in N$, are precisely all conjugates of ϑ over K. So

$$f(X) = \prod_{\tau\in N}(X - \vartheta^\tau) = \prod_{\tau\in N}(X - \vartheta - \phi(\tau)) = \mathcal{A}(X - \vartheta) \ ,$$

where

$$\mathcal{A}(X) := \prod_{\tau\in N}(X - \phi(\tau)) \ .$$

The roots of $\mathcal{A}$ form the additive group $\phi(N)$. Since we have chosen ϕ to be injective, we have $|\phi(N)| = |N| = \deg \mathcal{A}$. By part a) of Lemma 12.3 it follows that $\mathcal{A}$ is an additive polynomial. In particular,

$$f(X) \ = \ \mathcal{A}(X - \vartheta) \ = \ \mathcal{A}(X) - \mathcal{A}(\vartheta) \ .$$

Since $f(X) \in K[X]$, we have $\mathcal{A}(X) \in K[X]$ and $\mathcal{A}(\vartheta) \in K$. Since $\deg f = \deg \mathcal{A} = |N| = [L:K] = [K(\vartheta):K]$, f is the minimal polynomial of ϑ over K.

We have proved:

Theorem 12.28 *Let $L|K$ be an extension which satisfies condition (12.9). Then there exist an additive polynomial $\mathcal{A}(X) \in K[X]$ and an element $\vartheta \in L$ such that $L = K(\vartheta)$ and $\mathcal{A}(X) - \mathcal{A}(\vartheta) \in K[X]$ is the minimal polynomial of ϑ over K.*

As an example, let us discuss an important special case. Let us assume that $L|K$ is a Galois extension of degree p. Then its Galois group is just $\mathbb{Z}/p\mathbb{Z}$, and the extension is thus p-elementary. In the above setting, we may then choose $K' = K$ which yields $L' = L$, $G = N = \mathbb{Z}/p\mathbb{Z}$ and $H = 1$. The embedding $\phi : N \longrightarrow (L', +)$ may be chosen "by hand" to be the most natural one: $N = \mathbb{Z}/p\mathbb{Z} = (\mathbb{F}_p, +) \subset (L', +)$. We obtain

$$\mathcal{A}(X) = \prod_{i \in \mathbb{F}_p} (X - i) = X^p - X$$

since the latter is the unique polynomial of degree p which vanishes on all elements of $\mathbb{F}_p$. The extension $L|K$ is thus generated by the root ϑ of the polynomial $f(X) = X^p - X - \mathcal{A}(\vartheta)$ which is called an **Artin-Schreier polynomial**. The extension $L|K$ is called an **Artin-Schreier extension**, and ϑ is called an **Artin-Schreier root**. So we have shown:

Theorem 12.29 *Every Galois extension of degree p of a field of characteristic $p > 0$ is an Artin-Schreier extension.*

Inspired by this special case, we want to investigate whether we can get more information about the additive polynomial $\mathcal{A}$ if we strengthen the hypotheses. For instance, ϕ may be injective even if ψ is not. In our special case, $N = \mathbb{Z}/p\mathbb{Z}$ was an irreducible G-module, that is, it did not admit any proper nonzero G-submodule. But if N is an irreducible G-module, then every G-module homomorphism ϕ can only have kernel 0 or N, so if it does not vanish, then it is injective. For ϕ as defined in (12.12), we obtain $\phi \neq 0$ if $\psi \neq 0$. So it will suffice to take $\psi : N \to (\mathbb{F}_p, +)$ as a nonzero (additive) character; it exists since N is a non-trivial p-group. With this choice of ψ, we obtain

$$\phi(N) \subset \sum_{\rho \in H} \mathbb{F}_p \, b^\rho = \sum_{\rho \in H} \mathbb{F}_p \, \rho b \, .$$

Since the coefficients of the polynomial $\mathcal{A}$ are the elementary symmetric polynomials of the elements $\phi(\tau)$, $\tau \in N$, they lie in the ring $\mathbb{F}_p[\, \rho b \mid \rho \in H]$.

The condition that N be an irreducible G-module has turned out to be of certain importance. It is satisfied in the following special case:

Lemma 12.30 *Assume that $L|K$ is minimal with the property (12.9), that is, there is no proper non-trivial subextension with the same property. Then N is an irreducible G-module.*

Proof: Assume that M is a G-submodule of N, that is, M is a normal subgroup of G. Then HM is a subgroup of G containing H. In view of the unique representation (12.10), we have $HM = H$ if and only if $M = 1$ and $HM = G$ if and only if $M = N$. Note that the fixed field L_1' of M in L' is a Galois extension of K containing K'. Further, the fixed field L_1 of HM is contained in L, and it satisfies $L_1.K' = L_1'$ since $HM \cap N = M \cap N = M$. Consequently, also $L_1|K$ has property (12.9).

Suppose now that $L|K$ is minimal with the property (12.9). Then $L_1 = L$ or $L_1 = K$. Hence $HM = H$ or $HM = G$, that is, $M = 1$ or $M = N$, showing that the G-module N is irreducible. □

We summarize our preceding discussion in the following

Lemma 12.31 *Let the situation be as in Lemma 12.28. Assume in addition that $L|K$ is minimal with the property (12.9). We may assume w.l.o.g. that the extension $K'|K$ is finite. For every $b \in K'$ generating a normal basis of $K'|K$, and for every nonzero additive character $\psi : N \to (\mathbb{F}_p, +)$, the G-module homomorphism ϕ defined in (12.12) is injective. Moreover, the coefficients of the correponding additive polynomial $\mathcal{A}(X)$ lie in the ring*

$$K \cap \mathbb{F}_p[\,\rho b \mid \rho \in H\,] \,.$$

Exercise 12.4 *Since we may take $\psi : N \to (\mathbb{F}_p\,, +)$, it will also suffice to choose $b \in K'$ such that the conjugates σb are linearly independent over $\mathbb{F}_p$. Does this yield more freedom in the choice of b?*

Exercise 12.5 *Give additional conditions under which the converse of Lemma 12.30 holds.*