On coprime characteristic polynomials over finite fields

[Fragment of the paper "Additive Cellular Automata Over Finite Abelian Groups: Topological and Measure Theoretic Properties"]

Alberto Dennunzio Enrico Formenti
Darij Grinberg Luciano Margara

March 3, 2020

Contents

1. On coprime characteristic polynomials over finite fields

The following is a fragment of the paper "Additive Cellular Automata Over Finite Abelian Groups: Topological and Measure Theoretic Properties" in which we prove some purely algebraic properties of matrices and their characteristic polynomials. The fragment has been somewhat rewritten to make it self-contained.

Acknowledgments

DG thanks the Mathematisches Forschungsinstitut Oberwolfach for its hospitality during part of the writing process.

1.1. The main theorem

We shall use the following notations:

- The symbol $\mathbb{N}$ shall mean the set $\{0, 1, 2, \ldots\}$.
- If $n \in \mathbb{N}$, then the notation I_n shall always stand for an $n \times n$ identity matrix (over whatever ring we are using).
- If $\mathbb{K}$ is a commutative ring, and if $n \in \mathbb{N}$, and if $A \in \mathbb{K}^{n \times n}$ is an $n \times n$-matrix over $\mathbb{K}$, then χ_A shall denote the characteristic polynomial $\det(tI_n - A) \in \mathbb{K}[t]$ of A.
- If f and g are two univariate polynomials over a field K, then "$f \perp g$" will mean that the polynomials f and g are coprime. (This makes sense, since the polynomial ring $K[t]$ is a Euclidean domain.)

We are now ready to state the main result of this section:

Theorem 1.1. We fix a prime power q and consider the corresponding finite field $\mathbb{F}_q$. Let F be a field such that $F/\mathbb{F}_q$ is a purely transcendental field extension. (For example, F can be the field of all rational functions in a single variable over $\mathbb{F}_q$.)

Let $n \in \mathbb{N}$. Let $N \in F^{n \times n}$ be a matrix. Then, the following three assertions are equivalent:

- *Assertion $\mathcal{X}$:* We have $\det(N^k - I_n) \neq 0$ for all positive integers k.
- *Assertion $\mathcal{Y}$:* We have $\chi_N \perp t^k - 1$ for all positive integers k.
- *Assertion $\mathcal{Z}$:* We have $\chi_N \perp t^{q^i - 1} - 1$ for all $i \in \{1, 2, \ldots, n\}$.

1.2. Proof of the main theorem

Our proof of this theorem will rely on the following two lemmas:

Lemma 1.2. Let q, $\mathbb{F}_q$ and F be as in Theorem 1.1.

Let $n \in \mathbb{N}$. Let $f \in F[t]$ be a polynomial such that $\deg f \leq n$. Assume that $f \perp t^{q^i - 1} - 1$ for all $i \in \{1, 2, \ldots, n\}$. Then, $f \perp t^k - 1$ for all positive integers k.

Proof of Lemma 1.2. Let k be a positive integer. We must show that $f \perp t^k - 1$.

Indeed, assume the contrary. Then, the polynomials f and $t^k - 1$ have a non-constant common divisor $g \in F[t]$. Consider this g. Then, $g \mid f$ and $g \mid t^k - 1$.

Hence, the polynomial g is a divisor of $t^k - 1$; thus, its roots are k-th roots of unity, and therefore are algebraic over the field $\mathbb{F}_q$. Hence, the coefficients of g are algebraic over the field $\mathbb{F}_q$ as well (since these coefficients are symmetric polynomials in these roots with integer coefficients). On the other hand, these coefficients belong to F. But $F/\mathbb{F}_q$ is a purely transcendental field extension. Thus, every element of F that is algebraic over $\mathbb{F}_q$ must belong to $\mathbb{F}_q$ [1]. Thus, the coefficients of g must belong to $\mathbb{F}_q$ (since they are elements of F that are algebraic over $\mathbb{F}_q$). In other words, $g \in \mathbb{F}_q[t]$.

Since this polynomial $g \in \mathbb{F}_q[t]$ is non-constant, it must have a monic irreducible divisor in $\mathbb{F}_q[t]$. In other words, there exists a monic irreducible $\pi \in \mathbb{F}_q[t]$ such that $\pi \mid g$. Consider this π. Let $j = \deg \pi$. Then, $j \geq 1$ (since π is irreducible) and

$$\begin{aligned} j = \deg \pi \leq \deg f \qquad & (\text{since } \pi \mid g \mid f) \\ \leq n. & \end{aligned}$$

Hence, $j \in \{1, 2, \ldots, n\}$. Thus, $f \perp t^{q^j - 1} - 1$ (since we assumed that $f \perp t^{q^i - 1} - 1$ for all $i \in \{1, 2, \ldots, n\}$). Hence, every common divisor of f and $t^{q^j - 1} - 1$ in $F[t]$ must be constant.

From $\pi \mid g \mid t^k - 1$, we conclude that $t^k \equiv 1 \bmod \pi$ in $F[t]$. If we had $\pi \mid t$ in $F[t]$, then we would have $t \equiv 0 \bmod \pi$ in $F[t]$, which would entail $t^k \equiv 0^k = 0 \bmod \pi$ and thus $0 \equiv t^k \equiv 1 \bmod \pi$, which would lead to $\pi \mid 1$, which would be absurd (since $\deg \pi = j \geq 1$). Thus, we cannot have $\pi \mid t$ in $F[t]$. Thus, we cannot have $\pi \mid t$ in $\mathbb{F}_q[t]$ either. Hence, $\pi \nmid t$ in $\mathbb{F}_q[t]$. Therefore, $\pi \mid t^{q^j - 1} - 1$ [2].

Combining $\pi \mid g \mid f$ with $\pi \mid t^{q^j - 1} - 1$, we conclude that π is a common divisor of f and $t^{q^j - 1} - 1$ in $F[t]$. Hence, π is constant (since every common divisor of f and $t^{q^j - 1} - 1$ in $F[t]$ must be constant). This contradicts the irreducibility of π. This contradiction shows that our assumption was false. Hence, Lemma 1.2 is proven. $\square$

[1] Here we are using one of the basic properties of purely transcendental field extensions: If L/K is a purely transcendental field extension, then every element of L that is algebraic over K must belong to K. (Equivalently: If L/K is a purely transcendental field extension, then every element $x \in L \setminus K$ is transcendental over K.) This is proven in [Bosch18, §7.1, Remark 10], for example.

[2] *Proof.* This is a well-known fact about irreducible polynomials in $\mathbb{F}_q[t]$ distinct from t, but for the sake of completeness let us give a proof:

For each $u \in \mathbb{F}_q[t]$, we let $\overline{u}$ denote the projection of u onto $\mathbb{F}_q[t] / (\pi)$.

We have $\pi \nmid t$ in $\mathbb{F}_q[t]$. In other words, $\overline{t} \neq 0$ in $\mathbb{F}_q[t] / (\pi)$. In other words, the element $\overline{t}$ of $\mathbb{F}_q[t] / (\pi)$ is nonzero.

The polynomial π has degree $\deg \pi = j$. Hence, the quotient ring $\mathbb{F}_q[t] / (\pi)$ is an $\mathbb{F}_q$-vector space of dimension j (indeed, it has a basis consisting of $\overline{t^0}, \overline{t^1}, \ldots, \overline{t^{j-1}}$). Hence, it has size $\left|\mathbb{F}_q[t] / (\pi)\right| = \left|\mathbb{F}_q\right|^j = q^j$ (since $\left|\mathbb{F}_q\right| = q$). Moreover, this quotient ring $\mathbb{F}_q[t] / (\pi)$ is a field (since π is irreducible). Thus, $\mathbb{F}_q[t] / (\pi)$ is a finite field of size q^j. As a consequence, its group of units is a finite group of size $q^j - 1$. Thus, Lagrange's theorem shows that $u^{q^j - 1} = 1$ for every nonzero element $u \in \mathbb{F}_q[t] / (\pi)$. Applying this to $u = \overline{t}$, we conclude that $\overline{t}^{q^j - 1} = 1$ (since the element $\overline{t}$ of $\mathbb{F}_q[t] / (\pi)$ is nonzero). Hence, $\overline{t^{q^j - 1}} = \overline{t}^{q^j - 1} = 1 = \overline{1}$, so that $t^{q^j - 1} \equiv 1 \bmod \pi$ in $\mathbb{F}_q[t]$. In other words, $\pi \mid t^{q^j - 1} - 1$, qed.

Lemma 1.3. Let $n \in \mathbb{N}$. Let K be any field. Let $N \in K^{n\times n}$ be a matrix. Let $f \in K[t]$ be any polynomial. Then, $\det(f(N)) \neq 0$ if and only if $\chi_N \perp f$.

First proof of Lemma 1.3. Pick a splitting field L of f over K. Then, we can factor f in the polynomial ring $L[t]$ as follows:

$$f = \lambda(t-a_1)(t-a_2)\cdots(t-a_k) \qquad \text{for some } \lambda \in L\setminus\{0\} \text{ and some } a_1,a_2,\ldots,a_k \in L.$$

Consider these λ and $a_1,a_2,\ldots,a_k$. Note that these k elements $a_1,a_2,\ldots,a_k$ of L are precisely the roots of f in L. Evaluating both sides of the equality $f = \lambda(t-a_1)(t-a_2)\cdots(t-a_k)$ at N, we obtain the equality

$$f(N) = \lambda(N-a_1I_n)(N-a_2I_n)\cdots(N-a_kI_n)$$

in the matrix ring $L^{n\times n}$. Hence,

$$\begin{aligned}\det(f(N)) &= \det(\lambda(N-a_1I_n)(N-a_2I_n)\cdots(N-a_kI_n)) \\ &= \lambda^n\cdot\det(N-a_1I_n)\cdot\det(N-a_2I_n)\cdot\cdots\cdot\det(N-a_kI_n).\end{aligned}$$

Thus, we have the following chain of equivalences:

$$\begin{aligned}&(\det(f(N))\neq 0)\\ \Longleftrightarrow\ &(\lambda^n\cdot\det(N-a_1I_n)\cdot\det(N-a_2I_n)\cdot\cdots\cdot\det(N-a_kI_n)\neq 0)\\ \Longleftrightarrow\ &(\det(N-a_1I_n)\cdot\det(N-a_2I_n)\cdot\cdots\cdot\det(N-a_kI_n)\neq 0)\\ &\quad(\text{since } \lambda\neq 0)\\ \Longleftrightarrow\ &(\det(N-a_iI_n)\neq 0 \text{ for each } i\in\{1,2,\ldots,k\})\\ \Longleftrightarrow\ &((a_i \text{ is not an eigenvalue of } N) \text{ for each } i\in\{1,2,\ldots,k\})\\ &\quad\left(\begin{array}{c}\text{since the statement ``}\det(N-a_iI_n)\neq 0\text{'' for any given } i\in\{1,2,\ldots,k\}\\ \text{is equivalent to ``}a_i \text{ is not an eigenvalue of } N\text{''}\end{array}\right)\\ \Longleftrightarrow\ &((a_i \text{ is not a root of } \chi_N) \text{ for each } i\in\{1,2,\ldots,k\})\\ &\quad(\text{since the eigenvalues of } N \text{ are the roots of } \chi_N)\\ \Longleftrightarrow\ &(\text{none of the } k \text{ elements } a_1,a_2,\ldots,a_k \text{ is a root of } \chi_N)\\ \Longleftrightarrow\ &(\text{none of the roots of } f \text{ in } L \text{ is a root of } \chi_N)\\ &\quad(\text{since the } k \text{ elements } a_1,a_2,\ldots,a_k \text{ are precisely the roots of } f \text{ in } L)\\ \Longleftrightarrow\ &(f\perp\chi_N).\end{aligned}$$

Here, the last equivalence sign is due to a standard argument about polynomials[3].

This chain of equivalences entails $(\det(f(N))\neq 0) \iff (f\perp\chi_N)$. Thus, Lemma 1.3 is proven. □

[3]Here is a detailed proof: We must show the equivalence

$$(\text{none of the roots of } f \text{ in } L \text{ is a root of } \chi_N) \iff (f\perp\chi_N). \tag{1}$$

We shall show its "$\Longrightarrow$" and "$\Longleftarrow$" directions separately:

$\Longrightarrow$: Assume that none of the roots of f in L is a root of χ_N. We must prove that $f\perp\chi_N$.

We will soon give a second proof of Lemma 1.3, which generalizes it to arbitrary commutative rings (see Lemma 1.7 below).

Proof of Theorem 1.1. Let k be a positive integer. Then, Lemma 1.3 (applied to $K = F$ and $f = t^k - 1$) shows that $\det\left(N^k - I_n\right) \neq 0$ if and only if $\chi_N \perp t^k - 1$.

Now, forget that we fixed k. We thus have proven the equivalence $\left(\det\left(N^k - I_n\right) \neq 0\right) \iff \left(\chi_N \perp t^k - 1\right)$ for each positive integer k. Hence, Assertion $\mathcal{X}$ is equivalent to Assertion $\mathcal{Y}$.

On the other hand, $\chi_N \in F[t]$ is a polynomial with $\deg(\chi_N) = n$. Thus, Lemma 1.2 (applied to $f = \chi_N$) shows that if we have $\chi_N \perp t^{q^i - 1} - 1$ for all $i \in \{1, 2, \ldots, n\}$, then we have $\chi_N \perp t^k - 1$ for all positive integers k. In other words, Assertion $\mathcal{Z}$ implies Assertion $\mathcal{Y}$. Conversely, Assertion $\mathcal{Y}$ implies Assertion $\mathcal{Z}$ (since each $q^i - 1$ with $i \in \{1, 2, \ldots, n\}$ is a positive integer). Combining these two sentences, we conclude that Assertion $\mathcal{Y}$ is equivalent to Assertion $\mathcal{Z}$. Since we have also shown that Assertion $\mathcal{X}$ is equivalent to Assertion $\mathcal{Y}$, we thus conclude that all three Assertions $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are equivalent. Theorem 1.1 is thus proven. $\square$

Indeed, assume the contrary. Thus, the polynomials f and χ_N have a non-constant common divisor $g \in K[t]$. Consider this g. Thus, $g \mid f$ and $g \mid \chi_N$ in $K[t]$. We WLOG assume that g is monic (since we can always achieve this by scaling g). We have $g \mid f$ in $K[t]$, thus also in $L[t]$. Hence, $g \mid f = \lambda(t - a_1)(t - a_2) \cdots (t - a_k)$ in $L[t]$. Hence, g must be a product of some of the linear polynomials $t - a_1, t - a_2, \ldots, t - a_k$ (since $L[t]$ is a unique factorization domain, and g is monic). In other words, $g = \prod_{i \in I}(t - a_i)$ for some subset I of $\{1, 2, \ldots, k\}$. Consider this I. If I was empty, then we would have

$$\begin{aligned} g &= \prod_{i \in I}(t - a_i) = (\text{empty product}) \qquad (\text{since } I \text{ is empty}) \\ &= 1, \end{aligned}$$

which would contradict the fact that g is non-constant. Hence, I is nonempty. Thus, there exists some $j \in I$. Consider this j. Now, a_j is a root of f in L (since $a_1, a_2, \ldots, a_k$ are the roots of f in L), and thus is not a root of χ_N (since none of the roots of f in L is a root of χ_N). Hence, a_j is not a root of g either (since $g \mid \chi_N$). On the other hand, $g = \prod_{i \in I}(t - a_i)$ is a multiple of $t - a_j$ (since $j \in I$), and thus a_j is a root of g. This contradicts the fact that a_j is not a root of g. This contradiction shows that our assumption was false. Hence, the "$\Longrightarrow$" direction of (1) is proven.

$\Longleftarrow$: Assume that $f \perp \chi_N$. We must prove that none of the roots of f in L is a root of χ_N.

Indeed, assume the contrary. Thus, some root α of f in L is a root of χ_N. Consider this α.

But $f \perp \chi_N$. Hence, Bezout's theorem shows that there exist two polynomials $a, b \in K[t]$ such that $af + b\chi_N = 1$. Consider these a, b. Now, evaluating both sides of the equality $af + b\chi_N = 1$ at α, we obtain $a(\alpha) f(\alpha) + b(\alpha) \chi_N(\alpha) = 1$. Hence,

$$1 = a(\alpha) \underbrace{f(\alpha)}_{\substack{=0 \\ (\text{since } \alpha \text{ is a root of } f)}} + b(\alpha) \underbrace{\chi_N(\alpha)}_{\substack{=0 \\ (\text{since } \alpha \text{ is a root of } \chi_N)}} = 0 + 0 = 0.$$

This is absurd. This contradiction shows that our assumption was false. Hence, the "$\Longleftarrow$" direction of (1) is proven.

Thus, the proof of (1) is complete.

1.3. Extending Lemma 1.3 to rings

As promised, we shall now extend Lemma 1.3 to arbitrary commutative rings and re-prove it in that generality. First, we need some more lemmas:

Lemma 1.4. Let $\mathbb{K}$ be any commutative ring. Let $f \in \mathbb{K}[t]$ be any polynomial. Let $\mathbb{L}$ be any commutative $\mathbb{K}$-algebra. Let u and v be two elements of $\mathbb{L}$. Then, $u - v \mid f(u) - f(v)$ in $\mathbb{L}$.

Proof of Lemma 1.4. This is well-known in the case when $\mathbb{K} = \mathbb{Z}$ and $\mathbb{L} = \mathbb{Z}$; but the same proof applies in the general case.[4] Note that commutativity of $\mathbb{L}$ is crucial. $\square$

Lemma 1.5. Let $n \in \mathbb{N}$. Let $\mathbb{L}$ be any commutative ring. Let $A \in \mathbb{L}^{n\times n}$ be any $n \times n$-matrix. Let $\lambda \in \mathbb{L}$. Then,

$$\det(\lambda I_n + A) \equiv \det A \mod \lambda\mathbb{L}.$$

Proof of Lemma 1.5. This can be proven using the explicit formula for $\det(\lambda I_n + A)$ in terms of principal minors of A, or using the fact that the characteristic polynomial of A has constant term $(-1)^n \det A$. Here is another argument: For each $u \in \mathbb{L}$, we let $\overline{u}$ be the projection of u onto the quotient ring $\mathbb{L}/\lambda\mathbb{L}$; furthermore, for each matrix $B \in \mathbb{L}^{n\times n}$, we let $\overline{B} \in (\mathbb{L}/\lambda\mathbb{L})^{n\times n}$ be the result of projecting each entry of the matrix B onto the quotient ring $\mathbb{L}/\lambda\mathbb{L}$. Then, $\lambda \in \lambda\mathbb{L}$ and thus $\overline{\lambda} = 0$. Hence, $\overline{\lambda I_n + A} = \underbrace{\overline{\lambda I_n}}_{\substack{=0 \\ (\text{since } \overline{\lambda}=0)}} + \overline{A} = \overline{A}$. But the determinant of a matrix is a polynomial in the entries of the matrix, and thus is respected by the canonical projection $\mathbb{L} \to \mathbb{L}/\lambda\mathbb{L}$; hence,

$$\det\left(\overline{\lambda I_n + A}\right) = \overline{\det(\lambda I_n + A)} \qquad \text{and} \qquad \det \overline{A} = \overline{\det A}.$$

[4] Here is this proof:

Write the polynomial $f \in \mathbb{K}[t]$ in the form $f = \sum_{i=0}^{n} a_i t^i$ for some $n \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Then, $f(u) = \sum_{i=0}^{n} a_i u^i$ and $f(v) = \sum_{i=0}^{n} a_i v^i$. Subtracting these two equalities from each other, we obtain

$$f(u) - f(v) = \sum_{i=0}^{n} a_i u^i - \sum_{i=0}^{n} a_i v^i = \sum_{i=0}^{n} a_i \underbrace{\left(u^i - v^i\right)}_{=(u-v)\sum_{k=0}^{i-1} u^k v^{i-1-k}}$$
$$= \sum_{i=0}^{n} a_i (u-v) \sum_{k=0}^{i-1} u^k v^{i-1-k} = (u-v) \sum_{i=0}^{n} a_i \sum_{k=0}^{i-1} u^k v^{i-1-k}.$$

The right hand side of this equality is clearly divisible by $u - v$. Thus, so is the left hand side. In other words, we have $u - v \mid f(u) - f(v)$ in $\mathbb{L}$.

The left hand sides of these two equalities are equal (since $\overline{\lambda I_n + A} = \overline{A}$). Thus, the right hand sides are equal as well. In other words, $\overline{\det(\lambda I_n + A)} = \overline{\det A}$. In other words, $\det(\lambda I_n + A) \equiv \det A \bmod \lambda\mathbb{L}$. This proves Lemma 1.5. $\square$

> **Lemma 1.6.** Let $n \in \mathbb{N}$. Let $\mathbb{K}$ be any commutative ring. Let $f \in \mathbb{K}[t]$ be any polynomial. Let $N \in \mathbb{K}^{n\times n}$ be any $n \times n$-matrix. Then, there exist two polynomials $a, b \in \mathbb{K}[t]$ such that
>
> $$\det(f(N)) = fa + \chi_N b \qquad \text{in } \mathbb{K}[t].$$
>
> (Note that the left hand side of this equality is a constant polynomial, since $f(N) \in \mathbb{K}^{n\times n}$.)

Proof of Lemma 1.6. Consider N as a matrix over the polynomial ring $\mathbb{K}[t]$ (via the standard embedding $\mathbb{K}^{n\times n} \to (\mathbb{K}[t])^{n\times n}$). The $\mathbb{K}$-subalgebra $(\mathbb{K}[t])[N]$ of $(\mathbb{K}[t])^{n\times n}$ is commutative (since it is generated by the single element N over the commutative ring $\mathbb{K}[t]$).

Hence, Lemma 1.4 (applied to $\mathbb{L} = (\mathbb{K}[t])[N]$ and $u = tI_n$ and $v = N$) shows that $tI_n - N \mid f(tI_n) - f(N)$ in $(\mathbb{K}[t])[N]$. In other words, there exists some $U \in (\mathbb{K}[t])[N]$ such that

$$f(tI_n) - f(N) = (tI_n - N) \cdot U. \tag{2}$$

Consider this U. Taking determinants on both sides of the equality (2), we find

$$\det(f(tI_n) - f(N)) = \det((tI_n - N) \cdot U) = \underbrace{\det(tI_n - N)}_{\substack{=\chi_N \\ \text{(by the definition of } \chi_N)}} \cdot \det U$$
$$= \chi_N \cdot \det U.$$

In view of $f(tI_n) = f(t) \cdot I_n$, this rewrites as

$$\det(f(t) \cdot I_n - f(N)) = \chi_N \cdot \det U.$$

Hence,

$$\begin{aligned}
&\chi_N \cdot \det U \\
&= \det \underbrace{(f(t) \cdot I_n - f(N))}_{=f(t)\cdot I_n + (-f(N))} = \det(f(t) \cdot I_n + (-f(N))) \\
&\equiv \det(-f(N)) \qquad \left(\begin{array}{c}\text{by Lemma 1.5, applied to } \mathbb{L} = \mathbb{K}[t], \lambda = f(t) \\ \text{and } A = -f(N)\end{array}\right) \\
&= (-1)^n \det(f(N)) \bmod f(t)\,\mathbb{K}[t].
\end{aligned}$$

Multiplying this congruence by $(-1)^n$, we obtain

$$(-1)^n \chi_N \cdot \det U \equiv \underbrace{(-1)^n (-1)^n}_{=1} \det(f(N)) = \det(f(N)) \bmod f(t)\,\mathbb{K}[t].$$

In other words, $(-1)^n \chi_N \cdot \det U - \det(f(N)) \in f(t)\mathbb{K}[t]$. In other words, there exists a polynomial $c \in \mathbb{K}[t]$ such that

$$(-1)^n \chi_N \cdot \det U - \det(f(N)) = f(t)\, c. \tag{3}$$

Consider this c. Solving the equality (3) for $\det(f(N))$, we find

$$\begin{aligned}\det(f(N)) &= (-1)^n \chi_N \cdot \det U - \underbrace{f(t)}_{=f} c = (-1)^n \chi_N \cdot \det U - fc \\ &= f \cdot (-c) + \chi_N \cdot (-1)^n \det U.\end{aligned}$$

Hence, there exist two polynomials $a, b \in \mathbb{K}[t]$ such that $\det(f(N)) = fa + \chi_N b$ in $\mathbb{K}[t]$ (namely, $a = -c$ and $b = (-1)^n \det U$). This proves Lemma 1.6. □

We can now generalize Lemma 1.3 to arbitrary rings:

Lemma 1.7. Let $n \in \mathbb{N}$. Let $\mathbb{K}$ be any commutative ring. Let $N \in \mathbb{K}^{n\times n}$ be a matrix. Let $f \in \mathbb{K}[t]$ be any polynomial. Then, $\det(f(N)) \in \mathbb{K}$ is invertible if and only if there exist polynomials $a, b \in \mathbb{K}[t]$ such that $fa + \chi_N b = 1$.

Proof of Lemma 1.7. $\Longrightarrow$: Assume that $\det(f(N)) \in \mathbb{K}$ is invertible. Thus, there exists some $c \in \mathbb{K}$ such that $\det(f(N)) \cdot c = 1$. Consider this c.

Lemma 1.6 shows that there exist two polynomials $a, b \in \mathbb{K}[t]$ such that $\det(f(N)) = fa + \chi_N b$ in $\mathbb{K}[t]$. Consider these a and b, and denote them by a_0 and b_0. Thus, a_0 and b_0 are two polynomials in $\mathbb{K}[t]$ such that $\det(f(N)) = fa_0 + \chi_N b_0$. Now, comparing $\det(f(N)) \cdot c = 1$ with

$$\underbrace{\det(f(N))}_{=fa_0+\chi_N b_0} \cdot c = (fa_0 + \chi_N b_0) \cdot c = fa_0 c + \chi_N b_0 c,$$

we obtain $fa_0 c + \chi_N b_0 c = 1$. Thus, there exist polynomials $a, b \in \mathbb{K}[t]$ such that $fa + \chi_N b = 1$ (namely, $a = a_0 c$ and $b = b_0 c$). This proves the "$\Longrightarrow$" direction of Lemma 1.7.

$\Longleftarrow$: Assume that there exist polynomials $a, b \in \mathbb{K}[t]$ such that $fa + \chi_N b = 1$. Consider these a and b. Now, evaluating both sides of the equality $fa + \chi_N b = 1$ at N, we obtain

$$f(N)\, a(N) + \chi_N(N)\, b(N) = I_n.$$

Hence,

$$I_n = f(N)\, a(N) + \underbrace{\chi_N(N)}_{\substack{=0 \\ \text{(by the Cayley–Hamilton} \\ \text{theorem)}}} b(N) = f(N)\, a(N).$$

Taking determinants on both sides of this equality, we find

$$\det(I_n) = \det(f(N)\, a(N)) = \det(f(N)) \cdot \det(a(N)).$$

Thus,

$$\det(f(N)) \cdot \det(a(N)) = \det(I_n) = 1.$$

Hence, $\det(f(N)) \in \mathbb{K}$ is invertible (and its inverse is $\det(a(N))$). This proves the "$\Longleftarrow$" direction of Lemma 1.7. $\square$

Second proof of Lemma 1.3. Lemma 1.7 (applied to $\mathbb{K} = K$) shows that $\det(f(N)) \in K$ is invertible if and only if there exist polynomials $a, b \in K[t]$ such that $fa + \chi_N b = 1$. But this is precisely the statement of Lemma 1.3, because:

- the element $\det(f(N)) \in K$ is invertible if and only if $\det(f(N)) \neq 0$ (because K is a field), and
- there exist polynomials $a, b \in K[t]$ such that $fa + \chi_N b = 1$ if and only if $\chi_N \perp f$ (by Bezout's theorem).

Thus, Lemma 1.3 is proven again. $\square$

References

[Bosch18] Siegfried Bosch, *Algebra*, From the Viewpoint of Galois Theory, Springer 2018.
`https://doi.org/10.1007/978-3-319-95177-5`