III.G. Polynomial rings

Throughout we shall assume that $R, S$ denote commutative rings. We defined polynomial rings over $R$ in an indeterminate $x$ (and in independent indeterminates $x_1, \ldots, x_n$) in III.A.3(iv). From the inductive construction there it is clear that (writing $\mathcal{I} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ and $x^\mathcal{I} := x_1^{i_1} \cdots x_n^{i_n}$)

\begin{align*}
(\text{III.G.1}) \quad 0 = \sum_\mathcal{I} a_\mathcal{I} x^\mathcal{I} \in R[x_1, \ldots, x_n] \quad \iff \quad \text{all } a_\mathcal{I} = 0.
\end{align*}

Write $\mathfrak{i}: R \hookrightarrow R[x]$ (or $R[x_1, \ldots, x_n]$).

III.G.2. Theorem. Given $\varphi: R \to S$ and $u \in S$, there exists a unique homomorphism $\tilde{\varphi}: R[x] \to S$ such that $\tilde{\varphi}(x) = u$ and $\tilde{\varphi} \circ \mathfrak{i} = \varphi$. (More generally, given $u_1, \ldots, u_n \in S$, there exists a unique $\tilde{\varphi}_n: R[x_1, \ldots, x_n] \to S$ such that $\tilde{\varphi}_n(x_i) = u_i \ (\forall i)$ and $\tilde{\varphi}_n \circ \mathfrak{i} = \varphi$.)

Proof. Uniqueness follows from the fact that $\tilde{\varphi}$ [resp. $\tilde{\varphi}_n$] is specified on generators of $R[x]$, namely $R$ and $x$ [resp. $x_1, \ldots, x_n$].

For existence of $\tilde{\varphi}$, define $\tilde{\varphi}(\sum_k a_k x^k) := \sum_k \varphi(a_k) u^k$. We have

\begin{align*}
\tilde{\varphi}(\sum_k a_k x^k) \varphi(\sum_\ell b_\ell x^\ell) &= \sum_n (\sum_{k+\ell=n} \varphi(a_k) \varphi(b_\ell) ) u^n \\
&= \sum_n \varphi(\sum_{k+\ell=n} a_k b_\ell) u^n \quad \text{[since } \varphi \text{ homom.]} \\
&= \tilde{\varphi}(\sum_n (\sum_{k+\ell=n} a_k b_\ell) x^n) \\
&= \tilde{\varphi}(\sum_k (\sum_k a_k x^k)(\sum_\ell b_\ell x^\ell)),
\end{align*}

so $\tilde{\varphi}$ is a homomorphism (the other checks being trivial).

For existence of $\tilde{\varphi}_n$, apply induction: at each stage, we extend $\tilde{\varphi}_{n-1}: R[x_1, \ldots, x_{n-1}] \to S$ to $\tilde{\varphi}_n: R[x_1, \ldots, x_{n-1}][x_n] \to S$ restricting to $\tilde{\varphi}_{n-1}$ and sending $x_n \mapsto u_n$. \qed

III.G.3. Definition. If $S \supset R$ and $\varphi$ is the inclusion, $\tilde{\varphi}$ [resp. $\tilde{\varphi}_n$] is denoted $\text{ev}_u$ [resp. $\text{ev}_u^n$], and the image by

$$
\text{ev}_u(R[x]) \ (=: R[u])
$$

[resp. $\text{ev}_u^n(R[x_1, \ldots, x_n]) \ (=: R[u_1, \ldots, u_n]$)]. Note that this image consists of polynomials in $u$ [resp. the $\{u_i\}$.]
III.G.4. COROLLARY. Writing $I_u := \ker(\text{ev}_u)$, we have

$$R[u] \cong R[x]/I_u$$

and $I_u \cap R = \{0\}$ (and the obvious analogues for $u$).

PROOF. Use the Fundamental Theorem together with injectivity of $\text{ev}_u|_R (= \varphi)$. □

III.G.5. COROLLARY. Given $\sigma \in S_n$, there exists a unique automorphism $\zeta(\sigma)$ of $R[x_1, \ldots, x_n]$ sending $x_i \mapsto x_{\sigma(i)}$.

PROOF. Put $S := R[x_1, \ldots, x_n]$, $u_i := x_{\sigma(i)}$, and $\zeta(\sigma) := \bar{\varphi}_n$. An inverse is provided by $\zeta(\sigma^{-1})$. □

III.G.6. DEFINITION. As in III.G.3, let $u$ or $u_1, \ldots, u_n$ be elements of a ring $S$ containing $R$.

(i) $u$ is **transcendental** over $R \iff \text{ev}_u$ is injective.

(ii) Otherwise, $u$ is **algebraic** over $R$. In this case there exists $f(x) \in I_u \setminus \{0\}$, so that $f(u) = 0$ in $S$. (That is, $u$ satisfies a polynomial equation with coefficients in $R$.)

(iii) $u_1, \ldots, u_n$ are **algebraically independent** over $R \iff \text{ev}_u$ is injective; otherwise, they are **algebraically dependent**.

As a consequence of (III.G.1), $u_1, \ldots, u_n$ are algebraically independent if, and only if,

(III.G.7) $\sum_I r_I u^I = 0 \implies \text{all } r_I = 0$.

On the other hand, if $R = F$ and $S$ are fields,\(^{19}\) and each $u_i$ algebraic over $F$, then $F[u_1, \ldots, u_n]$ is called an **algebraic extension** of $F$.

III.G.8. PROPOSITION. An algebraic extension (of a field $F$) is a field. Moreover, every element of this field is algebraic over $F$.

PROOF. We only have to prove this for $F[u]$, $u$ algebraic (since induction then yields it for $F[u_1, \ldots, u_n]$). Let $f(x) = \sum_{k=0}^n a_k x^k \in F[x]$

\(^{19}\) The argument below works for $S$ a domain. We will give a “higher-level” approach to III.G.8 when we study PIDs.
be a (nonzero) polynomial of minimal degree with \( f(u) = 0 \). (Note that this degree is \( n \).) Since \( S \) has no zero-divisors, \( f(x) \) is irreducible. In particular, \( a_0 \neq 0 \) and (rescaling) we may assume \( a_0 = 1 \). Then \((-\sum_{k=1}^{n} a_k u^{k-1}) \cdot u = 1\) shows that \( u \) is invertible in \( \mathbb{F}[u] \).

Now let \( v \in \mathbb{F}[u] \) be arbitrary. If there exists some polynomial \( g(x) = \sum_{k} b_k x^k \in \mathbb{F}[x] \) with \( g(v) = 0 \) in \( S \), then the same argument (taking \( g \) of minimal degree, \( b_0 = 1 \), etc.) produces an inverse for \( v \) in \( \mathbb{F}[u] \), namely \(-\sum_{k>0} b_k v^{k-1}\). So this will prove both statements of the Proposition.

Notice that \( \mathbb{F}[u] \) is a vector space over \( \mathbb{F} \) of dimension \( n \). Indeed, using \( f(u) = 0 \) \( (\implies u^n = -\sum_{k=0}^{n-1} a_k u^{k}) \) we can reduce the degree of any polynomial in \( u \) (i.e. element of \( \mathbb{F}[u] \)) to \( \leq n - 1 \). Moreover, if \( \sum_{k=0}^{n-1} c_k u^k = \sum_{k=0}^{n-1} c'_k u^k \in \mathbb{F}[u] \) then \( c_k = c'_k \): otherwise the difference of the two sides gives a polynomial of degree \( < n \) with \( u \) as a root, contradicting minimality of \( n \).

So to find the desired polynomial \( g \), consider the linear transformation \( \mu_v : \mathbb{F}[u] \to \mathbb{F}[u] \) given by multiplication by \( v \). (This is calculated in the basis \( 1, u, \ldots, u^{n-1} \) by using \( f(u) = 0 \).) Taking \( g \) to be the characteristic polynomial of \( \mu_v \), by Cayley-Hamilton \( 0 = g(\mu_v) = \mu_{g(v)} \). As \( S \) hence \( \mathbb{F}[u] \) has no zero-divisors, \( g(v) \) is itself zero. \( \square \)

III.G.9. Example. An algebraic field extension \( F \) of \( \mathbb{Q} \) is called a number field. By III.G.8, every \( \alpha \in F \) has \( f(x) \in \mathbb{Q}[x] \) such that \( f(\alpha) = 0 \). The ring of integers \( \mathcal{O}_F \subset F \) comprises those \( \alpha \) with an \( f \) of the form

\[(III.G.10) \quad x^m + a_{m-1}x^{m-1} + \cdots + a_0, \quad a_j \in \mathbb{Z}.\]

(Such a polynomial, with top coefficient 1, is called monic.) Checking directly that \( \mathcal{O}_F \) is a ring is too messy. We postpone that to when we have the tools for a better approach, which will show in addition that the characteristic polynomial of multiplication by \( \alpha \in \mathcal{O}_F \) (as in the above proof) is itself monic integral. Since that polynomial has degree \( n := \dim_{\mathbb{Q}}(F) \) (from the proof), we only need to consider equations (III.G.10) with \( m = n \).
Consider \( F = \mathbb{Q}[\sqrt{d}] \cong \mathbb{Q}[x]/(x^2 - d) \). What is \( \mathcal{O}_F \)? (We assume \( d \) squarefree, so that \( d \not\equiv \frac{(4)}{0} \).)

Since the above “\( n \)” is just 2 in this case, an element \( a + b\sqrt{d} \) (\( a, b \in \mathbb{Q} \)) of \( F \) belongs to \( \mathcal{O}_F \) if and only if it satisfies

\[
0 = (a + b\sqrt{d})^2 + m(a + b\sqrt{d}) + n \quad \text{for some} \quad m, n \in \mathbb{Z}.
\]

Then \( 0 = (a^2 + b^2d + ma + n) + (2ab + mb)\sqrt{d} \), and so either

(i) \( b = 0 \) and \( a^2 + ma + n = 0 \) (\( \implies a \in \mathbb{Z} \))

or

(ii) \( -2a = m \) (\( \implies a = \frac{A}{2}, A \in \mathbb{Z} \)) and 
\[
b^2 = -\frac{A^2 + 2mA + 4n}{4d} \quad (\implies b = \frac{B}{2}, B \in \mathbb{Z}).
\]

In case (ii), \( \frac{A^2 + B^2d + 2mA}{4} = -n \in \mathbb{Z} \implies A^2 + B^2d + 2mA \equiv \frac{0}{4} \).

Thus:

- if \( A \) is even, then \( B^2d \equiv \frac{0}{4} \) (and \( d \not\equiv \frac{0}{4} \)) hence \( B \) is even; while

- if \( A \) is odd, then \( m \) is odd and (noting \( 3^3, 1^2 \equiv \frac{1}{4} \))

\[
1 + B^2d + 2 \equiv 0 \quad \implies B^2d \equiv \frac{1}{4} \quad \implies B \text{ odd and } d \equiv \frac{1}{4}.
\]

This gives the “\( \subseteq \)” half of

\[
(\text{III.G.11}) \quad \mathcal{O}_F = \begin{cases} 
\mathbb{Z}[\frac{1 + \sqrt{d}}{2}], & d \equiv 1 \\
\mathbb{Z}[\sqrt{d}], & \text{otherwise}.
\end{cases}
\]

The reverse inclusion “\( \supseteq \)” is more straightforward: given \( \alpha = a + b\sqrt{d} \) on the RHS, consider \( (x - a)(x - \bar{a}) \), where \( \bar{a} = a - b\sqrt{d} \) as usual.

**Polynomial division.** Earlier we made assertions about polynomial division in \( \mathbb{F}[x] \), \( \mathbb{F} \) a field. Now it is time to be more precise. Given \( f(x) = \sum_{j=0}^{d} a_jx^j \) with \( a_j \in R \) (an arbitrary commutative ring) and \( a_d \neq 0 \), write \( \deg(f) := d \). We set \( \deg(0) := -\infty \). Then

\[
(\text{III.G.12}) \quad \deg(fg) \leq \deg(f) + \deg(g) \quad \text{(with equality if } R \text{ is a domain)}
\]
and

(III.G.13) \( \deg(f + g) \leq \max(\deg(f), \deg(g)) \).

### III.G.14. Proposition

\( R \) domain \( \implies R[x_1, \ldots, x_n] \) domain and \( R[x_1, \ldots, x_n]^* = R^* \).

**Proof.** For \( n = 1 \), \( fg = 0 \implies \deg(f) + \deg(g) = \deg(fg) = -\infty \implies f \) or \( g = 0 \) while \( fg = 1 \implies \deg(f) + \deg(g) = 0 \implies \deg(f) = 0 = \deg(g) \implies f, g \in R^* \). For \( n > 1 \), use induction. \( \square \)

For \( R \) not a domain, we need not have \( R[x]^* \) equal to \( R^* \): e.g. in \( \mathbb{Z}_9[x], (1 + 3x)(1 - 3x) = 1 \).

Now let \( R \) be any commutative ring, and

\[ f = \sum_{i=0}^{n} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j \in R[x]. \]

### III.G.15. Theorem (Polynomial long division)

There exist \( k \in \mathbb{N} \) and \( q, r \in R[x] \) such that \( \deg(r) < \deg(g) \) and \( (b_m)^k f = q g + r \). If \( b_m \in R^* \) then we have \( f = q g + r \), and \( q, r \) are unique.

**Proof.** Assume \( (n =) \deg(f) \geq \deg(g) \) (since otherwise we’re done). Writing\(^{20}\)

\[ f_1 := b_m f - a_n x^{n-m} g \quad \text{(noting } n_1 := \deg(f_1) < \deg(f)) \]

\[ f_2 := b_m f_1 - a_n^{(1)} x^{n_1-m} g =: (b_m)^2 f - p_2 g \]

\[ \vdots \]

we eventually reach

\[ r := f_k := b_m^k f - p_k g \quad \text{of degree } < \deg(g) \]

For the uniqueness statement, we are assuming \( b_m \in R^* \). If \( q_1 g + r_1 = q_2 g + r_2 \), then \( \deg((q_1 - q_2)g) = \deg(r_2 - r_1) < m \). If \( q_1 - q_2 \neq 0 \), then (since \( b_m \) is not a zero-divisor) \( \deg((q_1 - q_2)g) \geq m \) yields a contradiction. So \( q_1 = q_2 \), and thus \( r_1 = r_2 \). \( \square \)

\(^{20}\) Note: \( a_k^{(j)} \) denote coefficients of \( f_j \).
III.G.16. Corollary. Given \( f \in R[x] \) and \( a \in R \), there exist unique \( q, r \in R[x] \) such that \( f(x) = (x - a)q(x) + f(a) \). Hence, \((x - a) \mid f(x) \iff f(a) = 0 \). (Such an “a” is called a root of \( f \).)

All of this is for a general commutative ring. More narrowly:

III.G.17. Corollary. If \( R \) is a domain, then a polynomial \( f \in R[x] \) of degree \( n := \deg(f) \) has at most \( n \) roots.

Proof. Let \( a_1, \ldots, a_r \) be distinct roots of \( f \). We have \((x - a_1) \mid f\) by III.G.16. Assume inductively \((x - a_1) \cdots (x - a_{k-1}) \mid f\). Then
\[
0 = f(a_k) = (a_k - a_1) \cdots (a_k - a_{k-1})g(a_k)_{\neq 0}
\]
\[
0 = g(a_k) \quad \text{(since } R \text{ is a domain)}
\]
\[
g(x) = (x - a_k)h(x) \quad \text{(for some } h \in R[x])
\]
\[
(x - a_1) \cdots (x - a_k) \mid f.
\]

So in fact, \( f(x) = H(x) \prod_{j=1}^r (x - a_i) \) (for some \( H \in R[x] \)) hence \( n \geq r \). \( \square \)

What if \( R \) is not a domain? Consider, say, polynomials over \( \mathbb{Z}_6 \): \( f(x) = 3x \) has \( \bar{0}, \bar{2}, \) and \( \bar{4} \) as roots. So III.G.17 fails.

Turning to the case where \( R \) is a field, we have the famous

III.G.18. Theorem. The multiplicative group of a finite field is cyclic. More generally, any finite subgroup \( G \) of the multiplicative group of a field \( F \) is cyclic.

Proof. Recall from II.D.15 that since \( G \) is abelian, \( G \) is cyclic \( \iff \exp(G) = |G| \). This was based on the fact that there exists an element of order \( \exp(G) := \min\{e \in \mathbb{N} \mid g^e = 1 \ (\forall g \in G)\} \). In general, \( \exp(G) \leq |G| \) since \( g^{[G]} = 1 \) for all \( g \in G \).

Now every \( g \in G \) satisfies \( g^{\exp(G)} - 1 = 0 \). But III.G.17 \( \implies x^{\exp(G)} - 1 \) has at most \( \exp(G) \) roots. So \( |G| \leq \exp(G) \). \( \square \)

III.G.19. Example. This says \( \mathbb{Z}_{17}^* \cong \mathbb{Z}_{16} \), and not \( \mathbb{Z}_2^4 \), \( \mathbb{Z}_8 \times \mathbb{Z}_2 \), etc. — this beats trying to find a generator!
III.G.20. REMARK. Assuming the structure theorem for finitely generated abelian groups, we can give a different proof of III.G.18 as follows. The structure theorem tells us that $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ where $m_1 > 1$ and $m_1 | m_2 | \cdots | m_k$. So every $g \in G$ is a root of $x^{m_k} - 1$, hence $|G| \leq m_k$ (by III.G.17), whence $k = 1$.

As we shall see later, there exist finite fields of prime power order (for any prime power).

III.G.21. COROLLARY. If $F$ is a finite field, then $F \cong \mathbb{Z}_p[u]$ where $\mathbb{Z}_p$ is its prime subfield and $u$ is algebraic over $\mathbb{Z}_p$.

PROOF. Let $u$ be a generator of the multiplicative group $F^* = F \setminus \{0\}$. □

Polynomial functions. Let $F$ be a field, $F^n := F \times \cdots \times F$ ($n$ times).

Consider a different kind of evaluation map:

(III.G.22)

$$\Phi_{n,F}: F[x_1,\ldots,x_n] \longrightarrow F^{F^n} = \prod_{u \in F^n} F \left( =: \text{ring of } F\text{-valued functions over } F^n \right)$$

$$f(x) \longmapsto \{f(u)\}_{u \in F^n}$$

The image $\Phi_{n,F}(F[x_1,\ldots,x_n]) =: \mathcal{P}_n(F)$ is called the ring of $(F$-valued) polynomial functions over $F^n$. We write $s_i$ for $\Phi_{n,F}(x_i)$, the $i$th coordinate function, and clearly $\mathcal{P}_n(F) = F[s_1,\ldots,s_n]$. Two questions arise:

- Are all functions polynomial functions? (i.e. is $\Phi_{n,F}$ surjective?)
- Do distinct polynomials yield distinct functions? (i.e. is $\Phi_{n,F}$ injective? Note that this would imply that $\mathcal{P}_n(F) \cong F[x_1,\ldots,x_n]$.)

We can give a surprisingly clear answer to both questions with the aid of the following

---

21 This will be discussed and proved in the context of modules where it belongs.
22 Note that the group operation is being written multiplicatively, because $G$ is a multiplicative group inside a field. In “additive” terms, $g^{m_k} - 1 = 0$ reads $m_kg = 0$.
23 Obviously $\mathbb{Z}_p^n$ isn’t a field, so that won’t cut it!
III.G. POLYNOMIAL RINGS

III.G.23. **Lemma.** Assume $|\mathbb{F}| = \infty$. Then for each $f \in \mathbb{F}[x_1, \ldots, x_n]$ other than the zero polynomial, there exists $u \in \mathbb{F}^n$ with $f(u) \neq 0$.

**Proof.** For $n = 1$: any $f \in \mathbb{F}[x]$ has at most $\deg(f) (< \infty)$ roots, so $\Phi_{n,\mathbb{F}}(f) \neq 0$. Next, assuming the result for $n - 1$ indeterminates, let $f_n \in \mathbb{F}[x_1, \ldots, x_{n-1}][x_n]$. Writing $f_n = g_0 + g_1 x_n + \cdots + g_d x_n^d$, let $u' \in \mathbb{F}^{n-1}$ be such that $g_d(u') \neq 0$. Then $f_n(u',x_n)$ is a nontrivial polynomial in $x_n$, and we get $u_n \in \mathbb{F}$ such that $f_n(u',u_n) \neq 0$. □

III.G.24. **Theorem.** $\Phi_{n,\mathbb{F}}$ is injective $\iff |\mathbb{F}| = \infty$.

**Proof.** If $|\mathbb{F}| = q < \infty$, then $|\mathbb{F}^n| = q - 1$ and so $a^{q-1} = 1 \implies a^q = a$ ($\forall a \in \mathbb{F}$) $\implies x_1^q - x_1 \in \ker(\Phi_{n,\mathbb{F}})$. If $|\mathbb{F}| = \infty$, the lemma implies that no nonzero $f \in \mathbb{F}[x_1, \ldots, x_n]$ is sent to the zero function. □

III.G.25. **Theorem.** If $|\mathbb{F}| < \infty$, then $\Phi_{n,\mathbb{F}}$ is surjective.

**Proof.** The proof of III.G.23 shows that when $\deg_{x_i}(f) < q := |\mathbb{F}|$ for all $i$, there exists $u \in \mathbb{F}^n$ such that $f(u) \neq 0$. This is because at each stage of the induction, the number of roots of $f_n$ in $x_n$ is less than the number of elements of $\mathbb{F}$.

On the other hand, the functions $x_i^q - x_i$ in the proof of III.G.24 belong to $\ker(\Phi_{n,\mathbb{F}})$. By the division algorithm, for every $k \geq q$ we get $x_i^k = (x_i^q - x_i)Q(x_i) + R(x_i)$ with $\deg(R) < q$, and so any $f \in \mathbb{F}[x_1, \ldots, x_n]$ is of the form

$$\sum_{i=1}^n g_i(x)(x_i^q - x_i) + g(x), \quad \text{with } \deg_{x_i}(g) < q \ (\forall i).$$

Hence $f \in \ker(\Phi_{n,\mathbb{F}}) \iff g(x) = 0$, which yields

(III.G.26) $\mathcal{P}_n(F) \cong \mathbb{F}[x_1, \ldots, x_n]/(x_1^q - x_1, \ldots, x_n^q - x_n)$.

But $|\mathbb{F}^\mathbb{F}| = q^{q^n}$, and

$$|\mathcal{P}_n(F)| = \#\{\text{choices for } g(x) = \sum_{i_1, \ldots, i_n=0}^{q-1} a_{i_1} x_1^{i_1} \} = q^{q^n}$$

as well. □
Symmetric polynomials. Looking back at III.G.5, the automorphisms \( \zeta(\sigma) \) of \( F[x_1, \ldots, x_n] \) produce a group homomorphism

\[
\zeta : S_n \to \text{Aut}(F[x_1, \ldots, x_n]).
\]

We will write \( F[x_1, \ldots, x_n]^{S_n} \) for the subring of \( \zeta(S_n) \)-invariant elements, i.e. the symmetric polynomials. Also note that a polynomial is called \textbf{homogeneous} if all its monomial terms have the same total degree (= sum of exponents).

III.G.27. \textbf{Definition.} (i) The \textbf{elementary symmetric polynomials}\(^{24}\) are

\[
e_1(x) = \sum_i x_i, \quad e_2(x) = \sum_{i < j} x_i x_j, \quad \ldots, \quad e_n(x) = x_1 \cdots x_n.
\]

(ii) The \textbf{Newton symmetric polynomials} are

\[
s_1(x) = \sum_i x_i, \quad s_2(x) = \sum_i x_i^2, \quad \ldots, \quad s_n(x) = \sum_i x_i^n.
\]

Both sets belong to \( F[x_1, \ldots, x_n]^{S_n} \), which is easiest to see for the \( \{e_i\} \) by writing formally

(III.G.28)  \[
\prod_{i=1}^n (y - x_i) = \sum_{j=0}^n (-1)^j e_j(x) y^{n-j}.
\]

We shall prove below that the \( e_i \) “span” \( F[x_1, \ldots, x_n]^{S_n} \). (More precisely, III.G.29 means that there is one and only one way to write each symmetric polynomial in the form \( \sum_{D \in \mathbb{N}^n} a_D e_D \), where \( e_D := e_1(x)^{d_1} \cdots e_n(x)^{d_n} \).) As you will show in HW, the \( s_i \) also “span the symmetric polynomials” if \( n! \neq 0 \) in \( F \).

Consider the ring homomorphism

\[
\mathcal{E}_n : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]^{S_n}
\]

\[
x_i \mapsto e_i(x)
\]

with image \( F[e_1, \ldots, e_n] \).

III.G.29. \textbf{Theorem.} \( \mathcal{E}_n \) \textit{is an isomorphism}.

\(^{24}\)Note that \( e_k(x) \) has \( \binom{n}{k} \) monomial terms.
PROOF. We begin with surjectivity. Since every symmetric polynomial is a sum of homogeneous symmetric polynomials, it suffices to prove that every homogeneous symmetric polynomial is a polynomial in the \( \{ e_i \} \).

Under the lexicographic ordering on monomials, let \( a_K x_1^{k_1} \cdots x_n^{k_n} \) be the highest-order term in some given symmetric \( f \); since \( f \) contains all permutations of each monomial, we have \( k_1 \geq k_2 \geq \cdots \geq k_n \). The highest monomial in \( e_1^{k_1-k_2} e_2^{k_2-k_3} \cdots e_n^{k_n} \) is

\[
(x_1)^{k_1-k_2} (x_1 x_2)^{k_2-k_3} (x_1 x_2 x_3)^{k_3-k_4} \cdots (x_1 \cdots x_n)^{k_n} = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}.
\]

Hence \( f - a_K e_1^{k_1-k_2} \cdots e_n^{k_n} \) has lower highest monomial than \( f \), and continuing on in this manner we eventually reach the zero polynomial.

Turning to injectivity, consider a finite sum \( \sum_D a_D x_1^{i_1} \cdots x_n^{i_n} \) (with not all \( a_D \) zero). For each \( D \in \mathbb{N}^n \), write (for \( i = 1, \ldots, n \)) \( k_i = d_i + \cdots + d_n \), and consider those (nonzero) \( a_D x_1^{i_1} \cdots x_n^{i_n} \) with largest \( |K| := \sum_i k_i \). The highest monomial in each is \( a_D x_1^{i_1} \cdots x_n^{i_n} \), and these are all distinct \( (D \neq D' \implies K \neq K') \). Taking the (unique) \( a_D x_1^{i_1} \cdots x_n^{i_n} \) with “highest highest” monomial, we see that this monomial occurs once, with a nonzero coefficient. Hence \( \sum_D a_D x_1^{i_1} \cdots x_n^{i_n} \neq 0 \). \( \square \)