GORDANs Finiteness Theorem
(HILBERTs proof – slightly modernized)

Klaus Pommerening

April 1975

Let k be an infinite entire ring, $V = k^2$, the free k-module of rank 2, G, the group $SL(V)$. Then G acts in a canocical way on $S^n(V^*)$, the module of binary forms of degree n, and on its affine coordinate ring $P := S(S^n(V^*)^*) = S(S^n(V))$. The ring $I := P^G$ of invariants is the classical ring of invariants of a binary form of degree n. Let

$$k_0 := \mathbb{Z}\left[\frac{1}{n!}\right] = \mathbb{Z}\left[\frac{1}{p} \mid p \leq n \text{ prime.}\right]$$

Theorem 1 (GORDAN 1868) *Let $n!$ be a unit in k. Then $I = I(k)$ is a finitely generated k-algebra, and*

$$I(k) \cong I(k_0) \otimes_{k_0} k$$

as a graduated k-algebra.

GORDAN's original proof [1] works for k a field of characteristic 0 and provides an explicit system of generators. Here we reproduce HILBERT's proof [2] that gives the theorem in the stated generality. The restriction that $n!$ is a unit will be needed only in step 3, and we also have a somewhat weaker (non-explicit) version without this restriction that however uses Emmy NOETHER's general result on finite generation of invariants under finite groups and therefore is anhistoric.

Corollary 1 *If k is an infinite noetherian entire ring (not necessarily $n!$ a unit), then I is a finitely generated k-algebra.*

Historical remark. Except for the main theorem on symmetric polynomials GORDAN's theorem is the earliest result on finite generation of invariant rings.

The proof starts with two lemmas.

Lemma 1 *Let*

$$\sum_{j=1}^{n} a_{ij}x_j = 0 \quad \textit{for } j = 1, \dots m \quad \textit{with } a_{ij} \in \mathbb{Z} \textit{ for all } i, j$$

be a system of diophantine equations. Then the semigroup of non-negative solutions (i. e. solution vectors $x = (x_1, \dots, x_n) \in \mathbb{N}^n$) is finitely generated.

This is a corollary of DICKSON's lemma for which we have a separate note [3].

Lemma 2 *Let* $\sigma_1, \ldots, \sigma_N \in k[X_1, \ldots, X_N] = k[X]$ *be the elementary symmetric polynomials. Then for each* i *the powers* X_i^j, $0 \le j < N$, *generate the* $k[\sigma]$*-module* $k[\sigma][X_i]$. *More explicitely, for each natural number* $p \in \mathbb{N}$ *there are polynomials* $g_1, \ldots, g_N \in k[\sigma_1, \ldots, \sigma_N]$ *such that*

$$X_i^p = g_1 \cdot X_i^{N-1} + \cdots + g_{N-1} \cdot X_i + g_N \quad \textit{for all } i = 1, \ldots N.$$

Proof. If $p \le N-1$, the assertion is obvious.

If $p = N$, then $X_1, \ldots, X_N$ are zeroes of the polynomial

$$(T - X_1) \cdots (T - X_N) = T^N - \sigma_1 T^{N-1} + \cdots \pm \sigma_N \in k[X][T],$$

whence $X_i^N = \sigma_1 X_i^{N-1} - \cdots \mp \sigma_N$ for $i = 1, \ldots, N$.

If $p > N$, we use induction and assume $X_i^{p-1} = g_1'(\sigma) X_i^{N-1} + \cdots + g_N'(\sigma)$ for $i = 1, \ldots, N$. Then

$$\begin{aligned} X_i^p &= g_1'(\sigma) X_i^N + \cdots + g_N'(\sigma) X_i \\ &= g_1'(\sigma) \left[\sigma_1 X_i^{N-1} - \cdots \pm \sigma_N \right] + g_2'(\sigma) X_i^{N-1} + \cdots + g_N'(\sigma) X_i \\ &= \underbrace{[g_1'(\sigma)\sigma_1 + g_2'(\sigma)]}_{=:g_1(\sigma)} X_i^{N-1} + \cdots + \underbrace{[g_N'(\sigma) \mp g_1'(\sigma)\sigma_{N-1}]}_{=:g_{N-1}(\sigma)} X_i \pm \underbrace{g_1'(\sigma)\sigma_N}_{g_N(\sigma)}, \end{aligned}$$

as was to be shown. $\diamond$

The proof of the theorem involves several rings. First let

$$S := T^n(S(V)) = S(V) \otimes \cdots \otimes S(V) = k[\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n],$$

the polynomial ring in $2n$ indeterminates. This k-algebra is canonically $\mathbb{N}^n$-graded where the homogeneous parts have the form

$$S_{\underline{d}} = S^{d_1}(V) \otimes \cdots \otimes S^{d_n}(V) \quad \text{for } \underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}^n.$$

The group $G = SL(V)$ acts on S in a homogeneous way; let $R := S^G$ be the algebra of invariants. It has the induced grading

$$R = \sum_{\underline{d} \in \mathbb{N}^n} R_{\underline{d}} \quad \text{where } R_{\underline{d}} = S_{\underline{d}} \cap R.$$

Examples for homogeneous invariants are

1. $p_{ij} := \alpha_i \beta_j - \alpha_j \beta_i$ for $1 \le i < j \le n \in R_{\underline{d}}$ where

$$\underline{d} = (0, \ldots, \overset{\overset{i}{\downarrow}}{1}, \ldots, \overset{\overset{j}{\downarrow}}{1}, \ldots, 0).$$

2. For an $\mathbb{N}$-valued symmetric matrix $M = (m_{ij})$ with zero diagonal,

$$X_M := \prod_{i<j} p_{ij}^{m_{ij}} \in R_{\underline{d}} \quad \text{where } d_i = \sum_{j=1}^{n} m_{ij}.$$

Let us denote this (multi-) degree by $\underline{d} =: D(M)$.

For $d \in \mathbb{N}$ let $(d) = (d, \ldots, d) \in \mathbb{N}^n$, hence $S_{(d)} = S^d(V) \otimes \cdots \otimes S^d(V)$. Then

$$\tilde{S} := \sum_{d \in \mathbb{N}} S_{(d)}$$

is an $\mathbb{N}$-graduated subalgebra of S. Also on this algebra G operates homogeneously, and the ring of invariants is

$$\tilde{R} := \tilde{S}^G = \sum_{d \in \mathbb{N}} R_{(d)}.$$

Furthermore we have the operation $\alpha_i \mapsto \alpha_{\pi(i)}$, $\beta_i \mapsto \beta_{\pi(i)}$ for $\pi \in \mathfrak{S}_n$, of the symmetric group $\mathfrak{S}_n$ on S; it induces a homogeneous operation on $\tilde{S}$. The operations of $\mathfrak{S}_n$ and of G commute elementwise. Therefore the direct product $\mathfrak{S}_n \times G$ acts on $\tilde{S}$ homogeneously.

Lemma 3 *The graduated ring $P = S(S^n(V))$ is isomorphic with $\tilde{S}^{\mathfrak{S}_n}$.*

Proof. A short consideration will motivate the proof. Let $\{x, y\}$ be a basis of the dual space V^*. Decompose the "general binary form of degree n",

$$f = \sum_{j=0}^{n} u_j x^{n-j} y^j$$

as a product of linear factors (over a suitable ring extension $\bar{k} \supseteq k$):

$$f = \prod_{i=1}^{n} (\beta_i x + \alpha_i y)$$

– this corresponds to the decomposition of the polynomial $\frac{1}{x^n} \cdot f = \sum u_j (\frac{y}{x})^j$ into linear factors $(\frac{y}{x} + \frac{\beta_i}{\alpha_i})$. Then

$$f = \prod (\beta_i x + \alpha_i y) = \beta_1 \cdots \beta_n \cdot \prod (x + \frac{\alpha_i}{\beta_i} y) = \beta_1 \cdots \beta_n \cdot \sum x^{n-j} \sigma_j (\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_n}{\beta_n}) y^j .$$

Therefore

$$u_0 = \beta_1 \cdots \beta_n, u_1 = \beta_1 \cdots \beta_n \cdot (\frac{\alpha_1}{\beta_1} + \cdots + \frac{\alpha_n}{\beta_n}), \ldots, u_n = \alpha_1 \cdots \alpha_n.$$

The general formula is

$$(*) \quad u_j = \sum_{M \in \mathfrak{P}_j(\{1,\ldots,n\})} \alpha_M \beta_{\bar{M}}$$

(with suggestive notation).

Now let's prove that $\tilde{S}^{\mathfrak{S}_n} = P$. Let α_i and β_i be indeterminates, and u_j for $j = 1, \ldots, n$ be given by formula $(*)$. Then $k[u_0, \ldots, u_n] = S(S^n(V)) = P$ is the coordinate algebra of the binary forms of degree n. We have

$$S_{(d)} = \{F \in k[\alpha, \beta] \mid F \text{ homogeous of degree } d \text{ in each pair } (\alpha_i, \beta_i)\}.$$

Therefore $u_0, \ldots, u_n \in S_{(1)}$, hence $P = k[u]$ is a graduated subring of $\tilde{S}$. Moreover all $u_j \in \tilde{S}^{\mathfrak{S}_n}$ because for $\pi \in \mathfrak{S}_n$ we have

$$\pi(u_j) = \pi\left(\sum_{M \in \mathfrak{P}_j} \alpha_M \beta_{\bar{M}}\right) = \sum_{M \in \mathfrak{P}_j} \alpha_{\pi(M)} \beta_{\overline{\pi(M)}} = u_j.$$

Therefore $P \subseteq \tilde{S}^{\mathfrak{S}_n}$ even as a graduated subring.

For the opposite inclusion let $F \in S_{(d)}$ be an $\mathfrak{S}_n$-invariant, say

$$F = \sum_{m \in \mathbb{N}^n} c_m \alpha_1^{m_1} \beta_1^{d-m_1} \cdots \alpha_n^{m_n} \beta_n^{d-m_n},$$

where $c_{\pi(m)} = c_m$ for all $\pi \in \mathfrak{S}_n$. This means that $F/\beta_1^d \cdots \beta_n^d$ is a symmetric polynomial in $\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_n}{\beta_n}$ of degree $\leq d$, hence a polynomial in the elementary symmetric polynomials:

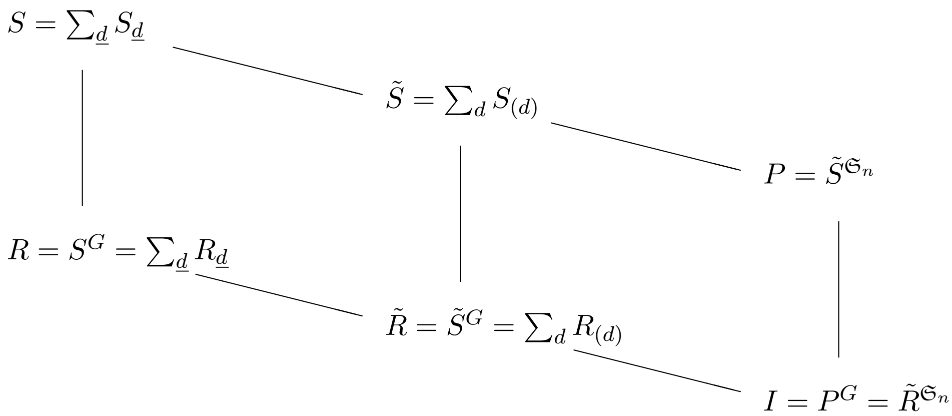
$$\frac{1}{u_0^d} \cdot F = \frac{1}{\beta_1^d \cdots \beta_n^d} \cdot F = G(\sigma_1(\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_n}{\beta_n}), \ldots, \sigma_n(\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_n}{\beta_n})) = G(\frac{u_1}{u_0}, \ldots, \frac{u_n}{u_0})$$

with $\deg(G) \leq d$, and therefore $F \in k[u]$. $\diamond$

The k-algebra whose finite generation the theorem asserts is therefore

$$I = P^G = (\tilde{S}^{\mathfrak{S}_n})^G = \tilde{S}^{\mathfrak{S}_n \times G} = (\tilde{S}^G)^{\mathfrak{S}_n} = \tilde{R}^{\mathfrak{S}_n}.$$

The following diagram shows the relations of all these rings.



Now we prove in three steps that the k-algebras R, $\tilde{R}$, and I are finitely generated.

Step 1.

Lemma 4 *For each* $\underline{d} \in \mathbb{N}^n$ *we have* $R_{\underline{d}} = \langle X_M \mid D(M) = \underline{d}\rangle$ *as a* k*-module, and* $R_{\underline{d}} = R_{\underline{d}}(k) \cong R_{\underline{d}}(\mathbb{Z}) \otimes_{\mathbb{Z}} k$.

In particular as a k-algebra R is generated by the $\binom{n}{2}$ elements p_{ij}, $1 \le i < j \le n$, and $R = R(k) \cong R(\mathbb{Z}) \otimes_{\mathbb{Z}} k$ as a graduated k-algebra.

We start the proof of Lemma 4 with the special case $n = 1$:

Lemma 5 $S(V)^G = k$.

Proof. Let $\{\alpha, \beta\}$ be a basis of V and $F = \sum_{i=0}^{r} c_i \alpha^{r-i}\beta^i$ with $r \ge 1$. If F is invariant under $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in G$, then $c_{r-i} = (-1)^{r-i} c_i$ for $i = 1, \ldots, r$. Now let F be also invariant under $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in G$ for all $\lambda \in k$. Then

$$\begin{aligned} F &= \sum_{i=0}^{r} c_i(\alpha + \lambda\beta)^{r-i}\beta^i = \sum_{i=0}^{r}\sum_{j=0}^{r-i} c_i \cdot \binom{r-i}{j} \alpha^{r-i-j}\lambda^j \beta^{j+i} \\ &= \sum_{i=0}^{r} \left[\sum_{j=0}^{i} \binom{r-j}{r-i} c_j \lambda^{i-j} \right] \alpha^{r-i}\beta^i \,. \end{aligned}$$

This gives equations for the coefficients c_i, for example

$$c_r = \sum_{j=0}^{r} \binom{r-j}{0} c_j \lambda^{r-j} = c_0\lambda^r + \cdots + c_r$$

for all $\lambda \in k$. Because k is an infinite entire ring, we conclude that $c_0 = \ldots = c_{r-1} = 0$ and $c_r = (-1)^r c_0 = 0$, hence $F = 0$. $\diamond$

Remark. For Lemma 5 we really need the condition that k is an infinite entire ring. As an illustration we give three counterexamples for weaker conditions.

Example 1. Let k be the finite entire ring $\mathbb{F}_2$. Then $F = \alpha^2 + \alpha\beta + \beta^2 \in S^2(V)$ is invariant under $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ that together generate G.

Example 2. Or let k be $\mathbb{F}_3$. Then $F = \alpha^6 + \alpha^4\beta^2 + \alpha^2\beta^6 + \beta^6 \in S^6(V)$ is invariant under $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, that together generate G.

Example 3. For an example where k is infinite, but has zero-divisors, take A, an infinite $\mathbb{F}_2$-module, and $k = \mathbb{F}_2 \times A$ with the multiplication $(m, a)(n, b) = (mn, ma + nb)$. (This is the well-known "adjunction of 1 to the $\mathbb{F}_2$-Algebra A with 0-multiplication".) Then $F = \alpha^4 + \alpha^2\beta^2 + \beta^4$ is invariant.

We prove Lemma 4 by induction on n. For $n = 1$ Lemma 5 gives $R = k$, and the assertion is trivial.

Therefore let $n > 1$. We make a further induction on $w := d_1 + \cdots + d_n$. If $w = 0$, we have $\underline{d} = 0$ and $R_0 = k$, and we are ready.

Now let $w > 0$, that is, $\underline{d} \neq 0$. We may assume $d_n \neq 0$ (otherwise change enumeration). If all other $d_i = 0$, we would have $S_{\underline{d}} \subseteq k[\alpha_n, \beta_n]$, and the case $n = 1$ would apply. Therefore we may assume (without loss of generality) that $d_{n-1} \neq 0$.

The substitution homomorphism

$$\varphi\colon S \longrightarrow S' = k[\alpha_1, \beta_1, \ldots, \alpha_{n-1}, \beta_{n-1}], \quad \alpha_n \mapsto \alpha_{n-1}, \beta_n \mapsto \beta_{n-1},$$

is G-equivariant, hence maps R onto $R' := (S')^G$ and $R_{\underline{d}}$ onto $R'_{\underline{d'}}$ where $d' = (d_1, \ldots, d_{n-1} + d_n) \in \mathbb{N}^{n-1}$. By induction $R'_{\underline{d'}} \cong R'_{\underline{d'}}(\mathbb{Z}) \otimes k$ is spanned by the $X_{M'}$ with $D(M') = \underline{d}'$. Each such $X_{M'}$ has $d_{n-1} + d_n$ factors of type $p_{i,n-1}$; if we replace any d_n of these by p_{in}, then we get an inverse image X_M of $X_{M'}$ under φ. Therefore $\varphi\colon R_{\underline{d}} \longrightarrow R'_{\underline{d'}}$ is surjective.

Next let us determine the kernel of φ. Let $F \in R_{\underline{d}}$ with $\varphi(F) = 0$. Then $\frac{1}{\beta_1^{d_1} \cdots \beta_n^{d_n}} \cdot F$ is a polynomial over $k\left[\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_{n-1}}{\beta_{n-1}}\right]$ in the indeterminate $\frac{\alpha_n}{\beta_n}$, and has $\frac{\alpha_{n-1}}{\beta_{n-1}}$ as a zero. Therefore $\left(\frac{\alpha_n}{\beta_n} - \frac{\alpha_{n-1}}{\beta_{n-1}}\right) | \frac{1}{\beta_1^{d_1} \cdots \beta_n^{d_n}} \cdot F$, and $p_{n-1,n} | F$. Thus there is an $F_0 \in R_{\underline{\tilde{d}}}$ with $\tilde{d} = (d_1, \ldots, d_{n-1} - 1, d_n - 1)$, such that $F = p_{n-1,n} F_0$. Therefore $\ker \varphi = p_{n-1,n} \cdot R_{\underline{\tilde{d}}}$ as a k-module (because R has no zero divisors). This gives the exact sequence

$$0 \longrightarrow R_{\underline{\tilde{d}}} \longrightarrow R_{\underline{d}} \longrightarrow R'_{\underline{d'}} \longrightarrow 0\,.$$

By induction on w the module $R_{\underline{\tilde{d}}} \cong R_{\underline{\tilde{d}}}(\mathbb{Z}) \otimes k$ is spanned by the X_M with $D(M) = \underline{\tilde{d}}$. Because the sequence

$$0 \longrightarrow R_{\underline{\tilde{d}}} \longrightarrow \langle X_M \mid D(M) = \underline{d} \rangle \longrightarrow R'_{\underline{d'}} \longrightarrow 0$$

is also exact, general nonsense (the five lemma) gives $R_{\underline{d}} = \langle X_M \mid D(M) = \underline{d} \rangle$. The exact sequence

$$0 \longrightarrow R_{\underline{\tilde{d}}}(\mathbb{Z}) \longrightarrow R_{\underline{d}}(\mathbb{Z}) \longrightarrow R'_{\underline{d'}}(\mathbb{Z}) \longrightarrow 0$$

consists of free $\mathbb{Z}$-modules. The following diagram has exact rows and canonical vertical arrows. The two isomorphisms follow by induction. By the five lemma also the middle arrow is an isomorphism.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R_{\underline{\tilde{d}}}(\mathbb{Z}) \otimes k & \longrightarrow & R_{\underline{d}}(\mathbb{Z}) \otimes k & \longrightarrow & R_{\underline{d'}}(\mathbb{Z}) \otimes k & \longrightarrow & 0 \\
 & & \downarrow \cong & & \downarrow & & \downarrow \cong & & \\
0 & \longrightarrow & R_{\underline{\tilde{d}}} & \longrightarrow & R_{\underline{d}} & \longrightarrow & R_{\underline{d'}} & \longrightarrow & 0
\end{array}$$

Step 2.

Lemma 6 *$\tilde{R}$ is a finitely generated k-algebra, and $\tilde{R} = \tilde{R}(k) \cong \tilde{R}(\mathbb{Z}) \otimes_{\mathbb{Z}} k$.*

Proof. The module $R_{(d)}$ is spanned by the $X(M)$ with $\sum_{j=1}^{n} m_{ij} = d$ for all $i = 1, \ldots, n$. Therefore R is spanned by the X_M with $\sum_{j=1}^{n} m_{1j} = \ldots = \sum_{j=1}^{n} m_{nj}$. This is a homogeneous system of diophantine equations for the m_{ij}. By Lemma 1 its solutions form a finitely generated subsemigroup of $\mathbb{N}^q$ (where $q = n(n-1)/2$). Let $\{M^{(1)}, \ldots, M^{(r)}\}$ be a system of generators. If $M = \sum_{l=1}^{r} a_l M^{(l)}$, then

$$X_M = \prod_{i<j} p_{ij}^{m_{ij}} = \left(\prod_{i<j} p_{ij}^{m_{ij^{(1)}}} \right)^{a_1} \cdots\cdots = X_{M_1}^{a_1} \cdots X_{M_r}^{a_r}.$$

Therefore the $X_1 := X_{M_1}, \ldots, X_r := X_{M_r}$ generate the k-algebra $\tilde{R}$. The isomorphism in the lemma follows because by Lemma 4 it holds on all homogeneous components. $\diamond$

Step 3.

We show that I is finitely generated, if $n!$ is a unit in k, and $I(k) \cong I(k_0) \otimes_{k_0} k$ as a graduated k-algebra.

Proof. Consider the linear map

$$\mu_d \colon R_{(d)} \longrightarrow R_{(d)}, \quad \mu_d := \sum_{\pi \in \mathfrak{S}_n} \pi.$$

Then $I_{(d)} := I \cap R_{(d)} = \mu_d(R_{(d)})$, because $n!$ is a unit in k. In I there are for example the following elements:

- (a) $\mu(X_1^{a_1} \cdots X_r^{a_r}) = \sum_{\pi \in \mathfrak{S}_n} \pi(X_1)^{a_1} \cdots \pi(X_r)^{a_r}$ where $a_1, \ldots, a_r \in \mathbb{N}$,
- (b) the elementary symmetric functions in the $\pi(X_i)$ for each $i = 1, \ldots, r$,

$$\sigma_j(\rho(X_i)_{\rho \in \mathfrak{S}_n}) = \sum_{A \in \mathfrak{P}_j(\mathfrak{S}_n)} \left(\prod_{\rho \in A} \rho(X_i) \right)$$

  for $j = 1, \ldots, n!$ because each $\pi \in \mathfrak{S}_n$ only permutes the summands.

Claim: The finite set $Z = \{(\text{a}) \mid \text{all } a_i < n!\} \cup \{(\text{b})\}$ generates the k-algebra I.

Each element of I is a linear combination of elements of the form

$$\begin{aligned} F &= \sum_{\pi \in \mathfrak{S}_n} \pi(X_1)^{a_1} \cdots \pi(X_r)^{a_r} = \sum_{\pi \in \mathfrak{S}_n} \left(\sum_{j=1}^{n!-1} g_j^{(1)} \pi(X_1)^j \right) \cdots \left(\sum_{j=1}^{n!-1} g_j^{(r)} \pi(X_r)^j \right) \\ &= \sum_{j_1, \ldots, j_r = 0}^{n!-1} g_{j_1}^{(1)} \cdots g_{j_r}^{(r)} \cdot \left(\sum_{\pi \in \mathfrak{S}_n} \pi(X_1)^{j_1} \cdots \pi(X_r)^{j_r} \right) \end{aligned}$$

with terms in $k[Z]$. Therefore $F \in k[Z]$ and $I = k[Z]$.

For the second statement, the isomorphism, we note that because $n!$ is a unit in k the $k[\mathfrak{S}_n]$-module $R_{(d)}$ is semisimple. Therfore the submodule $I_{(d)}$ has a direct complement $H_{(d)}$, and we have two exact direct sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H_{(d)} & \longrightarrow & R_{(d)} & \longrightarrow & I_{(d)} & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow \cong & & \uparrow & & \\
0 & \longrightarrow & H_{(d)}(k_0) \otimes k & \longrightarrow & R_{(d)}(k_0) \otimes k & \longrightarrow & I_{(d)}(k_0) \otimes k & \longrightarrow & 0
\end{array}$$

The diagram is commutative. We already know by Lemma 4 that the middle vertical arrow is an isomorphism. Because the rows are exact direct, also the two other vertical arrows are isomorphisms. Therefore $I \cong I(k_0) \otimes k$ as a graduated ring. $\diamond$

Step 3a.

We finally show that I is finitely generated, if k is noetherian, but $n!$ not necessarily a unit. This simply follows because I is the ring of invariants of the finitely generated k-algebra $\tilde{R}$ under the finite group $\mathfrak{S}_n$.

References

[1] P. Gordan: Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coeffizienten einer endlichen Anzahl solcher Formen ist. J. reine angew. Math. 69 (1868), 323–354.

[2] D. Hilbert: Über die Endlichkeit des Invariantensystems für binäre Grundformen. Math. Ann. 33 (1889), 223–226.

[3] K. Pommerening: A remark on subsemigroups (Dickson's lemma). Online: http://www.staff.uni-mainz.de/pommeren/MathMisc/Dickson.pdf