## 1. Anelli, ideali, moduli.

In questo corso gli anelli possiedono sempre un elemento 1. Gli omomorfismi di anelli mandano sempre 1 in 1. In particolare, i sottoanelli di un anello $R$ contengono 1. L'immagine $f(R)$ di un omomorfismo di anelli $f : R \longrightarrow R'$ è un sottoanello di $R'$. *L'anello zero*, indicato con $R = O$, è il gruppo $R = \{0\}$ con moltiplicazione $0 \cdot 0 = 0$. Nell'anello zero si ha che $0 = 1$, mentre in ogni anello $R \neq 0$ si ha che $0 \neq 1$. Per ogni anello $R$ esiste un unico omomorfismo $R \longrightarrow 0$ ed esiste un unico omomorfismo $\mathbf{Z} \longrightarrow R$.

Indichiamo con $R[X]$ *l'anello dei polinomi* nella variabile $X$. Il *grado* $\deg f$ di un polinomio $f(X) = \sum_i a_i X^i \in R[X]$ è il più grande indice $i$ con $a_i \neq 0$. Il grado del polinomio 0 è per convenzione uguale a $-\infty$. Con $R[[X]]$ indichiamo l'anello delle serie di potenze con coefficienti in $R$. Il *prodotto* di due anelli $R_1$ ed $R_2$ è il prodotto cartesiano $R_1 \times R_2$ con il prodotto $(x, y)(u, v) = (xu, yv)$ per $x, u \in R_1$ e $y, v \in R_2$. L'identità è $(1, 1)$.

Un ideale $I$ di un anello $R$ è un sottogruppo del gruppo additivo di $R$ con la proprietà che per ogni $x \in I$ ed ogni $\lambda \in R$ gli elementi $\lambda x$ e $x\lambda$ appartengono ad $I$. Il quoziente $R/I$ è un anello con il prodotto $(x+I)(y+I) = xy+I$. Se $R$ è commutativo, allora l'ideale *generato da un sottoinsieme* $S$ di $R$ è per definizione $I = \{\sum_{s\in S} \lambda_s s : \text{con } \lambda_s \in R \text{ quasi tutti nulli}\}$. Se $S = \{s\}$, allora l'ideale $I = \{\lambda s : \lambda \in R\}$ si dice *principale* e si indica con $(s)$.

Il nucleo $\ker f$ di un omomorfismo di anelli $f : R \longrightarrow R'$ è un ideale di $R$. Per il Teorema di isomorfismo l'applicazione naturale

$$R/\ker f \xrightarrow[\cong]{f} f(R)$$

è un isomorfismo di anelli. Il teorema di omomorfismo dice che per ogni omomorfismo di anelli $f : R \longrightarrow R'$ e per ogni ideale $I \subset \ker f$, il morfismo $\overline{f} : R/I \longrightarrow R'$, dato da $\overline{F}(\overline{x}) = f(x)$, è ben definito e il seguente diagramma è commutativo.

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ & \searrow \quad \nearrow_{\overline{f}} & \\ & R/I & \end{array}$$

Il *Teorema Cinese del resto* dice che per un anello commutativo e due ideali $I, J \subset R$ con $I + J = R$, l'applicazione naturale

$$R/IJ \xrightarrow{\cong} R/I \times R/J$$

è un isomorfismo di anelli.

Un *modulo* su un anello $R$ o un *$R$-modulo*, è un gruppo abeliano $M$ dotato di moltiplicazione per gli scalari in $R$ con le seguenti proprietà

$$\begin{array}{rcll} (\lambda+\mu)x & = & \lambda x + \mu x, & \text{per ogni } \lambda, \mu \in R \text{ ed ogni } x \in M; \\ \lambda(x+y) & = & \lambda x + \lambda y, & \text{per ogni } \lambda \in R \text{ ed ogni } x, y \in M; \\ \lambda(\mu x) & = & (\lambda\mu)x, & \text{per ogni } \lambda, \mu \in R \text{ ed ogni } x \in M; \\ 1.x & = & x & \text{per ogni } x \in M. \end{array}$$

Gli ideali di un anello $R$ sono $R$-moduli. Se $R$ è un campo, un $R$-modulo si chiama anche *$R$-spazio vettoriale*. Ogni gruppo abeliano è automaticamente uno $\mathbf{Z}$-modulo. Le solite costruzioni dell'algebra lineare per spazi vettoriali su campi si generalizzano facilmente a moduli su anelli: prodotto diretto di moduli, sottomodulo, quoziente di un modulo per un suo sottomodulo, somma di sottomoduli di un $R$-modulo dato.

Si dice che un modulo $M$ è *generato da un sottoinsieme* $S \subset M$ è $M = \{\sum_{s\in S} \lambda_s s :$ con $\lambda_s \in R$ quasi tutti nulli$\}$. Se $S$ è finito, allora $M$ si dice *finitamente generato.* Se $S = \{s\}$ contiene un elemento solo, allora $M = \{\lambda s : \lambda \in R\}$ e si dice *ciclico.* Un modulo $M$ si dice *libero* se $M \cong R^n$ per un certo $n \in \mathbf{Z}_{\geq 0}$.

## 2. Domini.

Un elemento $x$ di un anello $R$ si dice *divisore di zero* se $x \neq 0$ e se esiste un elemento diverso da zero $y \in R$ per cui $xy = 0$ oppure $yx = 0$. Un *dominio* è un anello commutativo $R \neq O$ privo di divisori di zero. I campi sono domini. Ogni dominio ammette un campo quoziente.

**Teorema 1.** *Sia $R$ un dominio. Allora si ha che*
*(a)* $\deg fg = \deg f + \deg g$ *per ogni* $f, g \in R[X]$*;*
*(b) l'anello $R[X]$ è un dominio;*
*(c) il gruppo $R[X]^*$ è uguale a $R^*$;*
*(d) un polinomio in $R[X]$ di grado $d$ ha al più $d$ zeri in $R$.*

**Dimostrazione.** (a) Scriviamo $f = aX^n +$ termini di grado più basso con $a \in R$ non zero e similmente $g = bX^m +$ termini di grado più basso con $b \in R$ non zero. Poiché $ab \neq 0$, il polinomio $fg = abX^{n+m} +$ termini di grado più basso ha grado $n + m$ come richiesto.
(b) Se $f, g \in R$ sono non nulli, allora $\deg f, \deg g \geq 0$. Per la parte (a) il prodotto $fg$ ha grado $\geq 0$ e quindi non è zero. Similmente, se $f, g \in R[X]$ soddisfano $fg = 1$, allora per la parte (a) si ha che $\deg f = \deg g = 0$ e quindi $f, g \in R^*$. Questo implica (c).
(d) Sia $f \in R[X]$. Se $f$ non ha zeri, allora non c'è niente da dimostrare. Supponiamo quindi che $f(a) = 0$ per un elemento $a \in R$. Allora riducendo $f$ modulo $X - a$ si vede che $f \equiv 0 \pmod{X-a}$ e quindi $f = g(X - a)$ per un polinomio $g \in R[X]$. Se $b \in R$ è uno zero di $f$, abbiamo che $f(b) = g(b)(b - a)$. Poiché $R$ è un dominio, abbiamo che $b = a$ oppure $b$ è uno zero di $g$. Per induzione, il polinomio $g$ ha al più $d - 1$ zeri in $R$. Di consequenza $f$ ha al più $d$ zeri, come richiesto.

**Corollario 2.** *Sia $R$ un dominio e sia $G$ un sottogrupo finito di $R^*$. Allora $G$ è ciclico.*

**Dimostrazione.** Sia $n = \#G$. Sia $d$ un divisore di $n$ e sia $\psi(d)$ il numero di elementi di $G$ di ordine $d$. Siccome l'ordine di un qualsiasi elemento $x \in G$ è un divisore di $n$, abbiamo che $n = \sum_{d|n} \psi(d)$.

Affermiamo che per ogni $d$ si ha che $\psi(d)$ è uguale a 0 oppure $\varphi(d)$ dove $\varphi$ è la funzione $\varphi$ di Eulero. Questo è chiaro quando non ci sono elementi di ordine $d$ in $G$. Supponiamo quindi che $x \in G$ abbia ordine $d$. Allora le potenze $x^i$ per $0 \leq i < d$ sono distinte e formano un insieme di $d$ zeri del polinomio $X^d - 1$. Per il Teorema 1 (c) ogni zero di $X^d - 1$ è quindi uguale a $x^i$ per un $i$. Ogni elemento di $G$ di ordine $d$ è quindi uguale a

$x^i$. Poiché l'ordine di $x^i$ è uguale a $d/\mathrm{mcd}(i,d)$, il numero di elementi di ordine $d$ è uguale a $\varphi(d) = \{i : \mathrm{mcd}(i,d) = 1 \text{ e } 0 \leq i < d\}$.

Per la formula di Gauss abbiamo che $n = \sum_{d|n} \varphi(d)$. Concludiamo che $\varphi(d) = \psi(d)$ per ogni $d$. In particolare, abbiamo che $\psi(n) \neq 0$ e quindi $G$ contiene necessariamente un elemento di ordine $n$ come richiesto.

## 3. Ideali primi e massimali.

Un ideale $I$ di un anello commutativo $R$ si dice *primo* se $I \neq R$ e se per ogni $x, y \in R$ con $xy \in I$ si ha che $x \in I$ oppure $y \in I$. Un ideale $I \subset R$ è primo se e solo se l'anello quoziente $R/I$ è un dominio. L'insieme degli ideali primi di $R$ si dice *lo spettro di* $R$ e si indica con $\mathrm{Spec}(R)$. Per ogni ideale $I \subset R$ sia $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) : I \subset \mathfrak{p}\}$. Gli insiemi $V(I)$ sono i chiusi della *topologia di Zariski* su $\mathrm{Spec}(R)$. Per ogni omomorfismo di anelli commutativi $f : R \longrightarrow R'$, l'applicazione $\mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R)$ data da $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$ è continua per la topologia di Zariski.

Un ideale $I$ di un anello commutativo $R$ si dice *massimale* se $I \neq R$ e se per ogni ideale $J$ con $I \subset J \subset R$ si ha che $J = I$ oppure $J = R$. Un ideale $I \subset R$ è massimale se e solo se l'anello quoziente $R/I$ è un campo. Un ideale massimale è primo. Un ideale primo $\mathfrak{p}$ di $R$ è massimale se e solo se il punto $\mathfrak{p}$ di $\mathrm{Spec}(R)$ è chiuso per la topologia di Zariski.

## 4. PID.

Un *dominio a ideali principali* (PID) è un dominio $R$ con la proprietà che ogni ideale $I \subset R$ è principale. L'anello $\mathbf{Z}$ è un anello a ideali principali.

Un elemento $\pi \neq 0$ in un dominio $R$ si dice *irriducibile* se $\pi = xy$ con $x, y \in R$ implica che $x \in R^*$ oppure $y \in R^*$. Un elemento $\pi$ in un dominio $R$ si dice *primo* se $\pi | xy$ implica che $\pi | x$ oppure $\pi | y$. Un elemento $\pi \in R$ è primo se e solo se l'ideale $(\pi)$ è un ideale primo di $R$. Un elemento primo è automaticamente irriducibile.

Il viceversa non vale in generale. Un *dominio a fattorizzazione unica* (UFD) è un dominio con la proprietà che ogni elemento $x \in R$ diverso da zero, è un prodotto

$$x = \pi_1 \cdot \pi_2 \cdots \pi_t$$

di elementi irriducibili $\pi_i \in R$. Il prodotto è unico a meno dell'ordine dei fattori e moltiplicazione per elementi invertibili. In un dominio a fattorizzazione unica, un elemento è irriducibile se e solo se è primo.

**Teorema 3.** *Un dominio a ideali principali (PID) è un dominio a fattorizzazione unica (UFD).*

**Dimostrazione.** Procediamo per assurdo. Sia $x \in R$ un elemento diverso da zero che *non* è prodotto di elementi irriducibili. Costruiamo una successione di elementi $x_i$ di $R$ come segue. Sia $x_1 = x$. L'elemento $x$ non è irriducibile e si fattorizza come $x = yz$ dove ne $y$ ne $z$ sono invertibili. Se $y$ e $z$ fossero prodotto di elementi irriducibili di $R$, allora anche $x$ lo sarebbe. Quindi, almeno uno di questi due elementi, diciamo $y$, non è prodotto di elementi irriducibili. Sia $x_2 = y$. Adesso abbiamo una inclusione di ideali principali $(x_1) \subset (x_2)$. L'inclusione è stretta, perché $x_1 = zx_2$ e $z$ non è invertibile.

Ripetendo questa procedura, otteniamo una successione infinita di ideali

$$(x_1) \underset{\neq}{\subset} (x_2) \underset{\neq}{\subset} \dots \underset{\neq}{\subset} (x_n) \underset{\neq}{\subset} \dots$$

Sia $I = \cup_{n\geq 1}(x_n)$ l'unione degli ideali $(x_n)$. Poiché $R$ è un PID, l'ideale $I$ è principale. Sia $w$ un generatore. Allora $w \in (x_n)$ per un indice $n \geq 1$. Ne segue che $x_{n+1} \in I = (w) \subset (x_n)$. Contraddizione. Concludiamo che ogni $x \in R$ è prodotto di elementi irriducibili.

Per vedere che il prodotto è unico a meno dell'ordine dei fattori e moltiplicazione per elementi invertibili, supponiamo che per un $x \in R$ non zero valga

$$x = \prod_{i\geq 1} \pi_i \ = \ \prod_{j\geq 1} \pi'_j$$

per certi elementi irriducibili $\pi_i, \pi'_j \in R$. Allora $\pi_1$ divide il prodotto $\prod \pi'_j$. Poiché in un PID elementi irriducibili sono anche primi, segue che $\pi_1$ divide $\pi'_j$ per un indice $j$. Rinumerando gli elementi $\pi'_j$, possiamo assumere che $j = 1$. Ma allora $\pi_1 = u\pi'_j$ per un $u \in R^*$. Siccome $R$ è un dominio, possiamo cancellare $\pi_1 = u\pi'_j$ ed ottenere

$$\prod_{i\geq 2} \pi_i \ = \ u \prod_{j\geq 2} \pi'_j.$$

Ripetendo la procedura un numero finito di volte, vediamo che a meno di moltiplicazione per elementi invertibili gli elementi $\pi_i$ e $\pi'_i$ sono uguali. Questo dimostra il teorema.

**Teorema 4.** *Sia $R$ un PID. Allora per ogni $R$-modulo finitamente generato $M$ abbiamo che*

$$M \ \cong \ \prod_{i=k}^{t} R/I_k$$

*per certi ideali (possibilmente nulli) $I_k \subset R$. Il modulo $M$è di torsione se e solo se si ha che $I_k \neq 0$ per ogni $k = 1, \dots, t$.*

Un $R$-modulo si dice *di torsione* se l'ideale $\{\lambda \in R : \lambda m = 0 \text{ per ogni } m \in M\}$ non è zero. Un caso speciale del Teorema 4 si presenta per $R = \mathbf{Z}$. In questo caso gli $R$-moduli sono semplicemente i gruppi abeliani. Il teorema dice che ogni gruppo abelian finitamente generato $M$ è isomorfo a $\mathbf{Z}^r \times \prod_{i=k}^{s} \mathbf{Z}/(m_k)$ per certi $m_k \in \mathbf{Z}$ non nulli. Si ha che $r = 0$ se e solo se $M$ è un gruppo finito.

## 5. UFD.

Sia $R$ un dominio a fattorizzazione unica. Un polinomio $f \in R[X]$ si dice *primitivo* se per nessun elemento irriducibile $\pi \in R$ si ha che $\pi$ divide tutti i coefficienti di $f$. Sia $K$ il campo quoziente di $R$. Allora ogni polinomio non nullo $f \in K[X]$ si può scrivere in in modo unico come prodotto $ag$ dove $a \in K^*$ e $g \in R[X]$ è un polinomio primitivo.

**Lemma 5.** *Sia $R$ un dominio a fattorizzazione unica. Allora il prodotto di due polinomi primitivi in $R[X]$ è primitivo.*

**Dimostrazione.** Supponiamo che $\pi \in R$ sia irriducibile e divida il prodotto $fg$ di due polinomi primitivi $f, g \in R[X]$. Poiché $R$ è un UFD, $\pi$ è un elemento primo e quindi $R/(\pi)$ è un dominio. Il prodotto $\overline{f}\,\overline{g}$ è zero nel dominio $R/(\pi)[X]$. Questo implica che uno fra $\overline{f}$ e $\overline{g}$ è zero in $R/(\pi)[X]$. In altre parole, $\pi$ divide tutti i coefficienti di $f$ oppure $\pi$ divide tutti i coefficienti di $g$. Contraddizione perché $f$ e $g$ sono polinomi primitivi.

**Teorema 6.** *Se $R$ è un dominio a fattorizzazione unica (UFD), anche l'anello $R[X]$ è un dominio a fattorizzazione unica.*

**Dimostrazione.** Sia $K$ il campo quoziente di $R$. Sia $f \in R[X]$ non zero. Allora nell'anello a ideali principali $K[X]$ possiamo scrivere

$$f = p_1 \cdot p_2 \cdots p_t$$

per certi polinomi irriducibili $p_i \in K[X]$. Moltiplicando per elementi opportuni di $K^*$, possiamo supporre che ogni $p_i$ sia un polinomio *primitivo* in $R[X]$. In questo modo otteniamo una fattorizzazione

$$f = ap_1 \cdot p_2 \cdots p_t \qquad (*)$$

con $a \in K^*$ e $p_i \in R[X]$ primitivo per ogni $i$.

Poiché in $K[X]$ la fattorizzazione in elementi irriducibili è unica, questo modo di scrivere $f$ è unico a meno dell'ordine e moltiplicazione per elementi invertibili.

Per il Lemma 4 il polinomio $p_1 \cdot p_2 \cdots p_t \in R[X]$ è primitivo. Questo implica che $a$ appartiene ad $R$. Per vedere questo, scriviamo $a = u/v$ con $u, v \in R$ non nulli e senza divisori irriducibili comuni. Se $\pi \in R$ fosse un divisore irriducibile di $v$, il fatto che i coefficienti di $f$ appartengono a $R$ implicherebbe che $\pi$ divide tutti i coefficiente del polinomio primitivo $p_1 \cdot p_2 \cdots p_t$. Questo è impossibile e quindi $v$ deve essere invertibile.

Scrivendo $a = \pi_1 \cdots \pi_s$ con $\pi_i \in R$ irriducibili, otteniamo il prodotto

$$f = \pi_1 \cdots \pi_s \cdot p_1 \cdot p_2 \cdots p_t.$$

Poiché gli elementi $\pi_i$ e $p_i$ sono irriducibili anche in $R[X]$, abbiamo scritto $f$ come prodotto di elementi irriducibili di $R[X]$. Poichè $R$ è UFD e la fattorizzazione $(*)$ è unica, anche la presente fattorizzazione di $f$ è unica a meno dell'ordine dei fattori e moltiplicazione per elementi invertibili.

**Proposizione 7.** *(Lemma di Gauss) Sia $R$ un dominio a fattorizzazione unica con campo quoziente $K$. Sia $f \in R[X]$ un polinomio monico. Se esistono polinomi monici $g, h \in K[X]$ con $f = g \cdot h$, allora $g$ e $h$ appartengono a $R[X]$.*

**Dimostrazione.** Esistono $a, b \in K^*$ tali che $ag$ e $bh$ sono polinomi *primitivi* in $R[X]$. Poichè $g$ ed $h$ sono monici, si ha che $a, b \in R$. Il fatto che $f$ sia monico implica che $ab = 1$ e quindi $a, b$ sono invertibili. Questo implica che $g$ e $h$ appartengono a $R[X]$, come richiesto.

**Proposizione 8.** *(Criterio di Eisenstein) Sia $R$ un dominio a fattorizzazione unica e sia $\pi \in R$ un elemento irriducibile. Sia $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ un polinomio primitivo con la proprietà che*

$$\pi \not| a_n, \qquad p|a_i \text{ per } i = 0, 1, \ldots, n-1, \quad e \quad \pi^2 \not| a_0.$$

*Allora $f$ è un elemento irriducibile di $R[X]$.*

**Dimostrazione.** Supponiamo che $f$ non sia irriducibile e scriviamo $f = g \cdot h$ con $g, h \in R[X]$ non invertibili. Poiché $f$ è primitivo, questo implica che $g$ e $h$ non sono polinomi costanti. Riducendo modulo $\pi$ troviamo che $\overline{g} \cdot \overline{g} = \overline{a_n} X^n$ in $K[X]$ dove $K$ è il campo quoziente del dominio $R/(\pi)$. Siccome $K[X]$ è un PID e quindi anche un UFD, abbiamo che $\overline{g} = \overline{c} X^k$ e $\overline{h} = \overline{c'} X^{n-k}$ per certi $c, c'$ non nulli in $R$. Poiché $g$ e $h$ non sono costanti, abbiamo che $1 \leq k \leq n-1$ e vediamo che i termini noti di $g$ e $h$ sono divisibili per $\pi$. Questo implica che $\pi^2$ divide $a_0$. Questa contraddizione implica la proposizione.

## 6. Polinomi simmetrici.

Sia $R$ un anello commutativo. Un polinomio $f \in R[X_1, \ldots, X_n]$ si dice *simmetrico* se $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n)$ per ogni permutazione $\sigma \in S_n$. I *polinomi simmetrici elementari* $s_1, \ldots, s_n \in \mathbf{Z}[X_1, \ldots, X_n]$ sono dati dei coefficienti del polinomio in $T$

$$(T - X_1) \cdots (T - X_n) = T^n - s_1 T^{n-1} + \ldots + (-1)^n s_n.$$

Si ha che $s_1 = X_1 + \cdots + X_n$ e $s_n = X_1 \cdots X_n$. In generale si ha che

$$s_k = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n} X_{i_1} X_{i_2} \cdots X_{i_k}.$$

Il polinomio $s_k$ è omogeneo di grado $k$.

**Teorema 9.** *Sia $R$ un anello commutativo. Ogni polinomio simmetrico $f \in R[X_1, \ldots, X_n]$ si scrive in modo unico come polinomio nei polinomi simmetrici.*

**Dimostrazione.** Ordiniamo i monomi $X_1^{e_1} \cdots X_n^{e_n}$ lessicograficamente: si ha che

$$X_1^{e_1} \cdots X_n^{e_n} \;>\; X_1^{f_1} \cdots X_n^{f_n}$$

quando $e_1 > f_1$ oppure quando $e_1 = f_1$ ma $e_2 > f_2$, oppure quando $e_1 = f_1$, $e_2 = f_2$, ma $e_3 > f_3$ ... ecc. Sia $cX_1^{e_1} \cdots X_n^{e_n}$ il monomio "più grande" in $f$. Allora $e_1 + e_2 + \ldots + e_n$ è al più $\deg f$. Poiché $f$ è simmetrico questo implica che $e_1 \geq e_2 \geq \ldots \geq e_n$. Consideriamo adesso il polinomio

$$g \;=\; c s_1^{e_1 - e_2} s_2^{e_2 - e_3} \cdots s_{n-1}^{e_n - e_{n-1}} s_n^{e_n} \quad \in R[X_1, \ldots, X_n].$$

Il grado di $g$ è

$$\begin{aligned} &(e_1 - e_2) + 2(e_2 - e_3) + 3(e_3 - e_4) + \ldots + (n-1)(e_{n-1} - e_n) + n e_n, \\ =&e_1 + e_2 + \ldots + e_n \leq \deg f. \end{aligned}$$

Poiché $s_k = X_1X_2\cdots X_k+$ termini lessicograficamente più bassi, il monomio più grande in $g$ è $X_1^{e_1}\cdots X_n^{e_n}$. Consideriamo il polinomio $f-g$. Per costruzione il suo monomio più grande è più piccolo di quello di $f$. Il grado totale di $f-M$ è al più $\deg f$.

Adesso ripetiamo la procedura. Poichè il numero di monomi di grado totale limitato è finito, questo processo deve terminare. Alla fine abbiamo scritto $f$ come polinomio nei polinomi simmetrici $s_1,\ldots,s_n$.

Per vedere che questa scrittura di $f$ è unica, dimostriamo che non esiste un polinomio non nullo $g \in R[Y_1,\ldots,Y_n]$ con $g(s_1,\ldots,s_n)=0$. Per ogni monomio $\mu$ di $g$ introduciamo esponenti $e_1,\ldots,e_n \in \mathbf{Z}_{\geq 0}$ tali che $\mu = cY_1^{e_1-e_2}Y_2^{e_2-e_3}\cdots Y_{n-1}^{e_n-e_{n-1}}Y_n^{e_n}$ per un certo $c \in R$ non nullo. Adesso scriviamo $g(s_1,\ldots,s_n)$ come polinomio negli $X_1,\ldots,X_n$. Sia $(e_1,\ldots,e_n)$ la $n$-tupla lessicograficamente più grande. Allora il monomio $X_1^{e_1}\cdots X_n^{e_n}$ in $g(s_1,\ldots,s_n)$ ha coefficiente $c$ e quindi $g(s_1,\ldots,s_n)\neq 0$.

Questo dimostra il teorema.

Il *discriminante* $\Delta_n$ del generico polinomio

$$(T-X_1)(T-X_2)\cdots(T-X_n)$$

di grado $n$ è dato da

$$\Delta_n \;=\; \prod_{1\leq i<j\leq n}(X_i-X_j)^2.$$

Per ogni polinomio $f \in \mathbf{C}[X_1,\ldots,X_n]$ abbiamo che

$$f = (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$$

per certi $\alpha_i \in \mathbf{C}$. Definiamo il discriminante $\mathrm{Disc}(f)$ di $f$ come $\Delta_n(\alpha_1,\ldots,\alpha_n)$. Per il Teorema 7, $\mathrm{Disc}(f)$ è un'espressione polinomiale nei coefficienti di $f$. Per esempio $\mathrm{Disc}(X^2+aX+b) = a^2-4b$.

Sia $R$ un dominio. Il *risultante* $\mathrm{Ris}(f,g)$ di due polinomio $f = a\prod_{i=1}^n(X-\alpha_i)$ e $g = b\prod_{j=1}^m(X-\beta_j)$ in $R[X]$ è dato da

$$\mathrm{Ris}(f,g) \;=\; a^m b^n \prod_{i=1}^n\prod_{j=1}^m(\alpha_i-\beta_j).$$

**Proposizione 10.** *Siano $f$ e $g$ come sopra. Allora*
*(a)* $\mathrm{Ris}(f,g) = (-1)^{nm}\mathrm{Ris}(g,f)$;
*(b)* $\mathrm{Ris}(f,g) = a^m\prod_{i=1}^n g(\alpha_i)$;
*(c) Siano $g_1,g_2 \in R[X]$ di grado $m_1$ e $m_2$, con $g_1 \equiv g_2 \pmod f$. Allora si ha che* $\mathrm{Ris}(f,g_1) = a^{m_1-m_2}\mathrm{Ris}(f,g_2)$.

**Dimostrazione.** (a) e (b) seguono direttamente dalla definizione del risultante. La parte (c) segue dalla parte (b).

Sia $f'$ il polinomio derivato di $f$. La regola di Leibniz implica che $f'(\alpha_i) = \prod_j(\alpha_i-\alpha_j)$ dove $j \in 1,\ldots,n$ è diverso da $i$. Tenendo conto dei segni, questo implica che

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}\mathrm{Ris}(f,f').$$