$f = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 - 36 s_1 s_2 s_3 - 27 s_3^2$

b) $s_1 = 0$
$s_2 = p$ $\Rightarrow \Delta = -4p^3 - 27q^2$
$s_3 = -q$ discriminant

În n variabile: $R[x_1, \dots, x_n] \rightsquigarrow s_1, \dots, s_n$ polinoame simetrice fundamentale

$\forall k \geq 0$, $p_k(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i^k$

Formulele lui Newton

$k \geq n$ $p_k - s_1 p_{k-1} + s_2 p_{k-2} + \dots + (-1)^n s_n p_{k-n} = 0$

$k < n$: $p_k - s_1 p_{k-1} + \dots + (-1)^k k s_k = 0$

Eg/ $(\mathbb{Z}, +, \cdot)$ $(K[x], +, \cdot)$, K = corp comutativ

câtul și restul sunt unic determinate

	$\mathbb{Z}$	$K[x]$
prim	$p \in \mathbb{Z}, p \neq 0, \pm 1$ $p \mid a \cdot b \Rightarrow p \mid a$ sau $p \mid b$	$P \in K[x]$, $gr(P) \geq 1$ P = divizor $P \mid A \cdot B \Rightarrow P \mid A$ sau $P \mid B$
ireductibil	$p \in \mathbb{Z}, p \neq 0, \pm 1$ $p = a \cdot b \Rightarrow a = \pm 1$ sau $b = \pm 1$	$P \in K[x]$, $gr(P) \geq 1$ P = multiplu $P = A \cdot B \Rightarrow gr(A) = 0$ sau $gr\, B = 0$

Teoremă a) în $\mathbb{Z}$ nr. prim $\Leftrightarrow$ nr. ireductibil
b) în $K[x]$ elem. prim $\Leftrightarrow$ elem. ireductibil

Dem. a) „$\Rightarrow$" $p \in \mathbb{Z}$ prim
Vrem p = ireductibil

Fie $a, b \in \mathbb{Z}$ a.î. $p = a \cdot b \Rightarrow p \mid a \cdot b \Rightarrow p \mid a$ sau $p \mid b$

$p \mid a$ și $a \mid p$ deci $a \sim p \Rightarrow a = \pm p$
$a = u \cdot p$, $u \in \{1, -1\}$

$p = u \cdot p \cdot b \Rightarrow 1 = u \cdot b \Rightarrow b = \pm 1$

„$\Leftarrow$" $p \in \mathbb{Z}$, ireductibil
Vrem p = prim

$a, b \in \mathbb{Z}$ a.î. $p \mid ab \Rightarrow \exists c \in \mathbb{Z}$ a.î. $p \cdot c = a \cdot b$

Dacă $p \mid a$ ✓

Dacă $p \nmid b \Rightarrow (p,a)=1 \Rightarrow \exists\, \alpha, \beta$ a.î. $p\cdot\alpha + a\cdot\beta = 1 \mid \cdot b$

$$p b \alpha + a\cdot b\cdot\beta = b$$
$$p\cdot b\cdot\alpha \; p\cdot c\cdot\beta = b$$
$$p(b\cdot\alpha + c\cdot\beta) = b \Rightarrow$$
$$p \mid b$$

~~Dem~~ b) Fie $d \in \mathbb{Z}$, un div. comun pt a și p.

$d \mid p \Rightarrow \exists\, t \in \mathbb{Z}$ a.î. $p = t\cdot d \Rightarrow t = \pm 1$ sau $d = \pm 1$

ired.

Dacă $d = \pm 1$ ✓

Dacă $t = \pm 1 \Rightarrow d = \pm p$, $d \mid a$ $\Rightarrow \exists\, q \in \mathbb{Z}$ a.î. $a = d\cdot q = \pm p\cdot q = p(\pm q)$

$\Rightarrow p \mid a$ Ⓧ

Cum recunosc numerele ($\mathbb{Z}$) sau polinoame ($K[X]$) prime/ired?

a) $\mathbb{Z}$ ✓

b) $K[X]$ — în $\mathbb{C}[X]$ - pol. ired cu grad 1

în $\mathbb{R}[X]$ — $X^4+1 = (X^4+2X^2+1) - 2X^2$

în $\mathbb{Q}[X]$ - pol. ired ~~cu~~ grad 1 sau 2

Teoremă: Fie $P \in K[X]$, grad$(P) \geq 1$

a) Dacă grad$(P) = 1 \Rightarrow P$ ireductibil

$P = 2X+4 \in \mathbb{R}[X]$

$P = 2(X+2)$

grad$(A\cdot B)$ = grad(A) + grad(B)

1 = grad(A) + grad(B)

Dem: $P = A\cdot B$, $A, B \in K[X]$

b) Dacă P are o răd. în K, ~~și~~ gr$(P) \geq 2$

atunci P este ireductibil $X - x_1 \mid P$

$x_1 \in K$, răd. pt. $P \Rightarrow P(x_1) = 0 \Rightarrow X - x_1 \mid P$

Deci $P = (X - x_1)\cdot F$, grad$(F) \geq 1 \Rightarrow P$ nu este ireductibil

c) Dacă grad$(P) = 2$ sau 3 și dacă P nu are răd. în K,

atunci P este ireductibil ♡

Dem.: P.A. $p \in K[x]$, $gr(p) = 2$ sau 3, p nu are răd. în K
p = reductibil $\Rightarrow \exists F, G \in K[x]$, $gr(F) \geq 1$, $gr(G) \geq 1$
$p = F \cdot G \Rightarrow$ unul din factori (de ex. F) are grad $= 1$
$F = aX + b \quad a \neq 0, \ a, b \in K$
are o răd. în K

Teoremă: a) în $\mathbb{Z}$, orice număr $\neq 0, \pm 1$ se scrie unic ca produs de numere prime
b) în $K[x]$, orice polinom de grad ≥ 1 se scrie unic ca produs de pol. ired.

$6 = 2 \cdot 3 = (-2) \cdot (-3)$
$x^2 - 1 = (x-1)(x+1) = (2x-2)(0{,}5x + 0{,}5)$

Dem.: a) $n \in \mathbb{N}, n \geq 2$
Dacă n = ireductibil —
Dacă n = reductibil $\Rightarrow n = a \cdot b$, $a, b \in \mathbb{N}$, $a, b \geq 2$
$a, b < n$
$n = p_1 \cdot p_2 \cdot \ldots \cdot p_t = q_1 \cdot q_2 \cdot \ldots \cdot q_s$, p_i, q_j = ireductibile/prime
$p_t \mid q_1 \cdot q_2 \cdot \ldots \cdot q_s$; Să pp. $p_t \mid q_s \Rightarrow \exists c \in \mathbb{Z}$
$q_s = p_t \cdot c$
p_t = ireductibil (prim)
$\Rightarrow c = \pm 1$
$\Rightarrow q_s = \pm p_t$

$\Rightarrow p_1 \cdot p_2 \cdot \ldots \cdot p_{t-1} = (\pm q_1) q_2 \cdot \ldots \cdot q_{s-1}$

P.A. $1 = q_1 \cdot q_2 \cdot q_3$

b) $N \in K[x]$, polinom de grad ≥ 1
dacă N ired —
dacă N reduct. $\Rightarrow N = A \cdot B$, $A, B \in K[x]$
pol. de grad ≥ 1

ex.: $a = 2^3 \cdot 5^2 \cdot 7^{11}$
$b = 2^4 \cdot 5 \cdot 3^2 \cdot 7^{16}$

P nu are răd. în K

gr(G)≥1

grad=1

se scrie unic ca

de grad ≥1 se

$a, b \geq 2$

reductibile/prime

$] c \in \mathbb{Z}$

$s = p_t \cdot c$

$[X]$

ad ≥1

$(a,b) = 2^3 \cdot 5^1 \cdot 7^{10}$

$[a,b] = 2^4 \cdot 5^2 \cdot 3^2 \cdot 7^{11}$

Prop.: a) în $\mathbb{Z}$:

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}$

$d = q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$

$d | a \iff \{q_1, \ldots, q_s\} \subseteq \{p_1, \ldots, p_t\}$

de ex $q_1 = p_1, \ldots, q_s = p_s$, $t \geq s$

și $\beta_1 \leq \alpha_1, \ldots, \beta_s \leq \alpha_s$

b) în $K[X]$ la fel!

<u>Teoremă (Euclid)</u>

a) în $\mathbb{Z}$, există o infinitate de nr. prime

b) în $K[X]$ există o inf. de pol. ireductibile

Dem.: a) P.A. $p_1, p_2, \ldots, p_{100}$

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_{100} + 1$

n = prim, $n \neq p_1, p_2, \ldots, p_{100}$

n nu e prim $\Rightarrow$ n are un divizor q = nr. prim

$q \neq p_1, q \neq p_2, \ldots, q \neq p_{100}$