A classification of detours in proofs of the generalized Nullstellensatz

D. J. Bernstein

University of Illinois at Chicago

Note: In this talk, rings are commutative and have 1.

"Ring" means a $(0, 1, +, -, \cdot)$ imitation of $\mathbf{Z}$: a set with operations $0, 1, +, -, \cdot$ satisfying every identity satisfied by $\mathbf{Z}$.

The generalized Nullstellensatz

(critical ideas: 1947 Zariski;
the theorem: independently
1951 Goldman, 1952 Krull)

Theorem: field K, subring R,
$\operatorname{gen}_R K < \infty \Rightarrow \exists q \in R - \{0\}$:
$R[1/q]$ is a field, $\operatorname{len}_{R[1/q]} K < \infty$.

"$\operatorname{gen}_R K < \infty$" means
$K = R[g_1, \ldots, g_n]$
for some $g_1, \ldots, g_n \in K$.

"$\operatorname{len}_A B < \infty$" means
B has finite dimension
as an A-vector space.

The usual Nullstellensatz

Corollary: field K, subfield F,
$\operatorname{gen}_F K < \infty \Rightarrow \operatorname{len}_F K < \infty$.
"Zariski's lemma"; usually
proven via Noether normalization.

Corollary: field K, subfield F,
F algebraically closed,
$\operatorname{gen}_F K < \infty \;\Rightarrow\; K = F$.

Corollary, classic Nullstellensatz:
F algebraically closed field,
poly ring $R = F[x_1, \ldots, x_n]$,
$\varphi : R \twoheadrightarrow K \Rightarrow \operatorname{Ker}\varphi =$
$(x_1 - \alpha_1)R + \cdots + (x_n - \alpha_n)R$
for some $\alpha_1, \ldots, \alpha_n \in F$.

Exercise: field F, poly ring $F[x]$,
$q \in F[x] - \{0\} \Rightarrow$
$F[x][1/q]$ is not a field.

Proof via Zariski's lemma:
If $K = F[x][1/q]$ is a field
then $\text{len}_F F[x] < \infty$.

Direct proof:
If $F[x][1/q]$ is a field
then $1/(1 - xq) = g/q^n$
for some $g \in F[x]$
so $q^n = (1 - xq)g$ in $F[x]$
so $1 = (1 - xq)h$ with
$h = 1 + \cdots + x^{n-1}q^{n-1} + x^n g$
so $q = 0$, contradiction.

Interlude: Integrality

Roots of monic polys in $R[x]$ are called "R-integral."

1. Field F, subring R,
F is R-integral $\Rightarrow$ R is a field.

2. Domain A, subfield F,
$\alpha \in A$, α is F-integral $\Rightarrow$
$F[\alpha]$ is a field, $\operatorname{len}_F F[\alpha] < \infty$.

3. Rings S, subring R,
R-integral $\alpha_1, \ldots, \alpha_n \in S$ $\Rightarrow$
$R[\alpha_1, \ldots, \alpha_n]$ is R-integral.

4. Field K, subfield F, $\alpha \in K$,
$q \in F[\alpha] - \{0\}$, $K = F[\alpha][1/q]$ $\Rightarrow$
α is F-integral. (Same exercise!)

Back to the generalization

Corollary: field K, subring R, $\text{gen}_R K < \infty$, Hilbert ring $H \twoheadrightarrow R$ $\Rightarrow$ R is a field, $\text{len}_R K < \infty$.

"Hilbert" ring H means: domain R, not a field, $H \twoheadrightarrow R$, $q \in R - \{0\}$ $\Rightarrow$ $R[1/q]$ not a field.

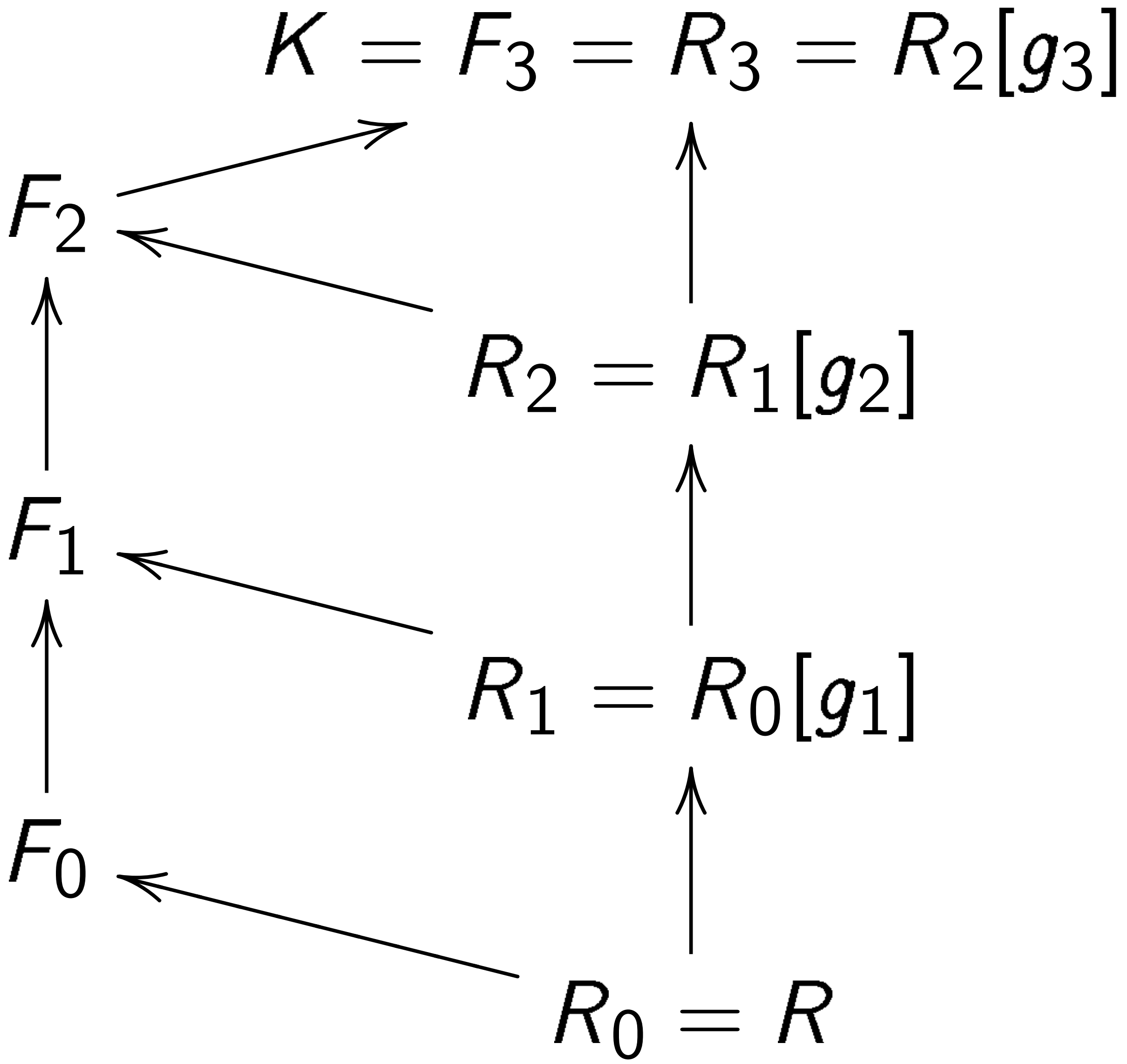
e.g. $F[x]$ is a Hilbert ring. (The same exercise again!)

e.g. **Z** is a Hilbert ring. Corollary: Every finitely generated field is a finite field. (1940 Malcev)

How is it proven?

Proof for, e.g., $K = R[g_1, g_2, g_3]$:

Define $R_0 = R$; $R_1 = R[g_1]$;
$R_2 = R[g_1,g_2]$; $R_3 = R[g_1,g_2,g_3]$;
F_i = subfield of K gen by R_i.



The main point of the proof:
Can obtain each F_i
by inverting one element of R_i.

Will construct successively
$q_3 \in R_3 - \{0\}$ with $F_3 = R_3[1/q_3]$;
$q_2 \in R_2 - \{0\}$ with $F_2 = R_2[1/q_2]$;
$q_1 \in R_1 - \{0\}$ with $F_1 = R_1[1/q_1]$;
$q_0 \in R_0 - \{0\}$ with $F_0 = R_0[1/q_0]$.

Will also see that
$\operatorname{len}_{F_3} K < \infty$; $\operatorname{len}_{F_2} F_3 < \infty$;
$\operatorname{len}_{F_1} F_2 < \infty$; $\operatorname{len}_{F_0} F_1 < \infty$.
Thus $\operatorname{len}_{F_0} K < \infty$ as claimed.

Core task: Build q_0 from q_1,
while showing that $\operatorname{len}_{F_0} F_1 < \infty$.

$q_1 \in R_1 = R_0[g_1] \subseteq F_0[g_1]$.
$R_0[g_1][1/q_1] = R_1[1/q_1] = F_1$
so $F_0[g_1][1/q_1] = F_1$.
By the exercise, g_1 is F_0-integral.
$F_0[g_1]$ is a field; $\text{len}_{F_0} F_0[g_1] < \infty$.

$1/q_1 \in F_0[g_1]$ so $F_1 = F_0[g_1]$ so
$\text{len}_{F_0} F_1 < \infty$; $1/q_1$ is F_0-integral.

Clear denominators:
g_1 and $1/q_1$ are $R_0[1/q_0]$-integral
for some $q_0 \in R_0 - \{0\}$.

$F_1 = R_0[1/q_0][g_1][1/q_1]$
is $R_0[1/q_0]$-integral,
so $R_0[1/q_0]$ is a field,
so $F_0 = R_0[1/q_0]$. Done!

Common detours (häufig mit Zorn)

Detour $\cap$: Define Hilbert ring as "every prime ideal is an intersection of maximal ideals."

Detour $\sum$: Merge polynomial manipulations into the proof, instead of highlighting integrality.

Detour $/$: Work with $R_0, R_1, \ldots$ as quotients of polynomial rings, instead of working inside K.

Detour ∞: Prove the exercise by proving that there are infinitely many maximal ideals in $F[x]$.

Examples of these detours:

Proof	Detours
1951 Goldman	$\cap$, $\sum$, $/$, ∞
1995 Eisenbud	$\cap$, $\sum$, $/$, ∞
1998 Bernstein	none
2000 Stallings	$\cap$, $/$, ∞
2001 Grayson	∞
2006 Swan	$/$