LECTURE 4

RITT FACTORIZATION AND SHAPIRO CONJECTURE

RITT'S WORK IS FROM 1927. HE WORKED WITH COMPLEX EXPONENTIAL FUNCTIONS, BUT IT HAS TURNED OUT THAT THE UNDERLYING ALGEBRA IS MUCH MORE GENERAL.

ORIGINAL SETTING (AT FORMAL LEVEL)

K AN E-FIELD, ALG. CLOSED.

WORK IN $K[z]^E$ WITH SUBRING $\mathcal{S}$ OF ELEMENTS OF FORM

$$\sum_{j=1}^{n} \lambda_j \cdot E(\mu_j z) \quad , \ \lambda\text{'s}, \mu\text{'s IN } K$$

FOR A NONZERO $f \in \mathcal{S}$ AS ABOVE

$\text{SUPPORT}(f) = \{\mu_j : \lambda_j \neq 0\}$.

$\langle \text{SUPPORT} \rangle(f) = \mathbb{Q}$-CLOSURE OF SUPPORT$(f)$.

$[\text{SUPPORT}(f)] = \mathbb{Z}$-CLOSURE OF SUPPORT$(f)$.

THE UNITS OF THE DOMAIN J ARE EXACTLY THE $E(\mu z)$, $\mu \in K$.

THUS EVERY NONZERO f IS UP TO A UNIT, OF FORM $\sum \lambda_j E(\mu_j z)$, ALL μ_j DISTINCT, ONE $\mu_j = 0$ WITH $\lambda_j = 1$.

A VERY BASIC LEMMA DUE TO RITT (AND WIDELY GENERALIZABLE) IS:

LEMMA If $f = g \cdot h$ THEN THERE IS A UNIT u SO THAT

$$[\mathrm{SUPP}(gu)] \subseteq \langle \mathrm{SUPP}(f) \rangle$$

$$[\mathrm{SUPP}(hu^{-1})] \subseteq \langle \mathrm{SUPP}(f) \rangle .$$

THIS GENERALIZES (EVEREST - VANDER POORTEN) TO GROUP ALGEBRAS OF TORSION-FREE DIVISIBLE ABELIAN GROUPS OVER UFD's.

WHAT THIS ACHIEVES

f GIVEN, AS BEFORE, AND ONE TRIES TO FACTOR IT, SAY

$$f = g \cdot h$$

FIRST, GET A BASIS $b_1, \ldots b_m$ OF [SUPP(f)] AND WRITE THE μ_j AS $\mathbb{Z}$-COMBINATIONS OF $b_1, \ldots b_m$.

THINK OF THE $E(b_k \cdot z)$ AS INDEPENDENT VARIABLES $X_1, \ldots X_m$.

NOW f BECOMES

$$F(X_1, \ldots X_m)$$

ALMOST A POLYNOMIAL, EXCEPT THAT IN SOME OF THE MONOMIALS AN X_k MAY HAVE A NEGATIVE EXPONENT. BUT THEN YOU REWRITE F AS A GENERALIZED MONOMIAL TIMES A POLYNOMIAL IN $X_1, \ldots X_m$ OVER K.

BUT THEN BY THE LEMMA ON SUPPORTS THE FACTORIZATION YIELDS

$$F = G \cdot H$$

WHERE G AND H ARE BOTH "FRACTIONAL GENERALIZED MONOMIALS" TIMES POLYNOMIALS IN NONNEGATIVE FRACTIONAL (RATIONAL) POWERS OF THE $X_1, \ldots X_m$

NOW, REPLACING EACH X_j BY A SUITABLE POWER AND MOVING NEGATIVE POWERS IN THE MONOMIALS ACROSS $=$, ONE GETS, IN THE UFD $K[X_1, \ldots X_m]$ AN IDENITY

$$M_1 \cdot F(X_1^{s_1}, \ldots X_m^{s_m})$$

$$= M_2 \cdot G^*(X_1, \ldots X_m) \cdot H^*(X_1, \ldots X_m)$$

M_1, M_2 MONOMIAL,
G^*, H^* POLYNOMIAL.

UNLESS F HAD MONOMIAL FACTORS (TRIVIAL CASE) ONE ENDS UP WITH A "POWER REDUCTION" OF F:

$$F = G^{\deg H} \cdot H^{\deg G}.$$

PRINCIPLE FACTORIZATIONS OF f CORRESPOND TO POWER REDUCTIONS OF F.

THIS IS PROFOUNDLY LINKED TO ZILBER'S KUMMER ARGUMENT (END OF LECTURE 3).

$=$

IRREDUCIBLE F MAY POWER REDUCE.

TRIVIAL CASE

$X - 1 \quad : \quad X^n - 1$

$n \geq 2.$

"CYCLOTOMIC CASES"

FINITENESS THEOREM (RITT - GOURIN)

SUPPOSE $F \in K[x_1, \cdots x_m]$ IS IRREDUCIBLE, AND HAS ≥ 3 TERMS. SUPPOSE F IS POWER REDUCIBLE. THEN THERE ARE FINITELY MANY m-TUPLES $(s_{11}, \cdots s_{1m}), \cdots (s_{\ell 1}, \cdots s_{\ell m})$ OF INTEGERS ≥ 1 SUCH THAT:

i) EACH $F(x_1^{s_{j1}}, \cdots x_m^{s_{jm}})$ IS REDUCIBLE;

ii) IF $F(x_1^{s_1}, \cdots x_m^{s_m})$ IS REDUCIBLE $\exists! j$

SO THAT $(s_{j1}, \cdots s_{jm}) \mid (s_1, \cdots s_m)$ COORDINATEWISE

THEN THE IRREDUCIBLE FACTORS OF $F(x_1^{s_1}, \cdots x_m^{s_m})$ ARE OF THE FORM $H(x_1^{s_1/s_{j1}}, \cdots x_m^{s_m/s_{jm}})$

H AN IRREDUCIBLE FACTOR OF $F(x_1^{s_{j1}}, \cdots x_m^{s_{jm}})$.

"ALMOST UNIQUE FACTORIZATION"

THE PRECEDING ARGUMENT IS LARGELY FORMAL AND WORKS IN ANY $R[G]$, R A CHARACTERISTIC 0 UFD, G A TORSION-FREE DIVISIBLE ABELIAN GROUP.

[NOTE THAT OUR $K[X]^E$ ARE OF THIS FORM, WITH $R = K[X]$].

THIS LEADS READILY, USING THE FINITENESS THEOREM, TO:

THEOREM (EVEREST-VAN DER POORTEN)

[$R[G]$ AS ABOVE]

ANY $f \in R[G]$ FACTORS UNIQUELY (UP TO UNITS, ETC) AS A FINITE PRODUCT OF:

i) IRREDUCIBLES OF R

ii) VARIOUS $P_i(t^{\gamma_j})$, P_i POLYNOMIAL, THE γ_j NOT $\mathbb{Q}$-DEPENDENT IN j PAIRS

iii) IRREDUCIBLES OF $R[G]$

RITT DID THE CASE OF $\mathcal{S}$.

A NEW SC (BETTER Sh C):
(SHAPIRO). IF $f, g \in \mathcal{S}$ THEN f AND g HAVE INFINITELY MANY ZEROS IN $\mathbb{C}$ IFF f, g HAVE A COMMON DIVISOR h IN $\mathcal{S}$, WITH h HAVING INFINITELY MANY ZEROS IN $\mathbb{C}$.

BY FACTORIZATION THIS REDUCES TO THE FOLLOWING CASES:

i) f A POLYNOMIAL IN SOME $E(\mu z)$, g SIMILAR

ii) f AS ABOVE, g "GENUINE" IRREDUCIBLE.

iii) f, g EACH A "GENUINE" IRREDUCIBLE.

(i) AND (ii) HAVE BEEN PROVED (VAN DER POORTEN ET AL). NOT TRIVIAL — USE OF SKOLEM-MAHLER-LECH).

SC SEEMS VERY RELEVANT FOR CASE (iii). WE (D'A, M, T) NOT QUITE READY TO ANNOUNCE

$$SC \Rightarrow Sh\,C ,$$

BUT ARE VERY OPTIMISTIC.

I SKETCH THE RECIPE.

- LET B BE A $\mathbb{Q}$-BASIS FOR THE SPACE SPANNED BY $SUPP(f) \cup SUPP(g)$. IN FACT, CHOOSE IT AS $\mathbb{Z}$-BASIS FOR GROUP GENERATED BY THE TWO SUPPORTS. REDUCE TO CASE

$$f = F(E(b_1 z), \cdots, E(b_N z))$$

$$g = G(E(b_1 z), \cdots E(b_N z))$$

F, G IRREDUCIBLE POLYNOMIALS, $b_j \in B$.

LET K_0 BE THE FIELD GENERATED BY COEFFICIENTS OF F AND G.

NOW CONSIDER A SOLUTION Z_0 OF

$$f = g = 0.$$

THEN $(E(b_1, Z_0), \ldots E(b_N, Z_0))$ IS A ZERO OF

$$F = G = 0.$$

CLAIM THE TRANSCENDENCE DEGREE OF THIS ZERO OVER K_0 IS $\leq N-2$ (RECALL, $N \geq 2$). (NL • G)

PROOF OTHERWISE HAS TRANS. DEG $= N-1$, AND IS THEN A COMMON GENERIC POINT OF THE VARIETIES

$$F = 0$$

AND $G = 0$.

SO f, g ASSOCIATES. □

NOW ASSUME SC FOR $\mathbb{C}$, AND $z_0 \neq 0$

$$\text{TRANS.DEG}_{\mathbb{Q}}(b_1 z_0, \cdots b_N z_0, E(b_1 z_0), \cdots E(b_N z_0)) \leq N + N - 2 + \text{TRANS.DEG}_{\mathbb{Q}}(K_0)$$

WHILE $\text{LINDIM}_{\mathbb{Q}}(b_1 z_0, \cdots b_n z_0) = N$.

THIS GIVES

$N \leq N + N - 2 + T.D_{\mathbb{Q}}(K_0)$

i.e. $N + TD_{\mathbb{Q}}(K_0) \geq 2$,

NOT USEFUL IN ISOLATION.

HOWEVER, ASSUME

(i) $TD_{\mathbb{Q}}(b_1, \cdots b_N) = 0$

(ii) $TD_{\mathbb{Q}}(K_0) = 0$

THEN YOU GET FIRST

$$TD_{\mathbb{Q}}(b_1 z_0, \cdots b_N z_0, E(b_1 z_0), \cdots E(b_N z_0)) \leq 1 + (N-2),$$ AND THEN

$N - 1 \geq N \quad \rightarrow\leftarrow$.

NOTE THAT HERE, UNDER STRONG HYPOTHESES, WE GOT A STRONG RESULT (NO COMMON ZERO $\neq 0$).

ELABORATION ONE WORKS WITH AN INFINITE SERIES $Z_0, Z_1, \ldots$ OF NONZERO SOLUTIONS, AND IT SEEMS (MANY DETAILS TO CHECK!) THAT THE $\mathbb{Q}$(LINEAR)-DIMENSION OF THE SET IS FINITE (ASSUMING SC).

IF THIS IS SO, WE PROCEED TO A CONTRACTION AS FOLLOWS:

FIX COMMON ZEROS $\Theta_1, \ldots \Theta_k$, $\mathbb{Q}$-INDEP,

SO THAT FOR INFINITELY MANY $C_1, \ldots C_k$ FROM $\mathbb{Q}$

$C_1 \cdot \Theta_1 + \cdots + C_n \cdot \Theta_n$

IS A COMMON ZERO

ALL WE NEED HENCEFORWARD IS THAT THESE ELEMENTS ARE ZEROS OF f.

LET

$$f = \sum \lambda_j \cdot E(\mu_j \cdot z)$$

IF $z = c_1 \cdot \theta_1 + \cdots + c_k \cdot \theta_k$

$$E(\mu_j \cdot z) = \prod E(c_t \cdot \mu_j \cdot \theta_t).$$

NOTE THAT THESE ELEMENTS ARE IN THE DIVISIBLE CLOSURE, IN $\mathbb{C}^*$ OF THE FINITELY GENERATED GROUP GENERATED BY THE $E(\mu_j \cdot \theta_t)$.

NOTE THAT WE ASSUME WLOG THAT SOME $\mu_j = 0$ AND $\lambda_j = 1$ (DIVISION TRICK).

WE CAN THEN APPLY A HARD THEOREM OF EVERTSE, SCHLICKEWEI AND SCHMIDT:

THIS IMPLIES THAT THERE ONLY FINITELY MANY TUPLES

$(E(\mu_1 Z), \cdots E(\mu_N Z))$

OCCURRING AS "IRREDUCIBLE" SOLUTIONS AS Z RANGES OVER COMMON ZEROS.

IF ALL SUCH ARE "IRREDUCIBLE" ONE DEDUCES

$\text{LINDIM}_{\mathbb{Q}}(\mu_1, \cdots \mu_N) = 1$

SO f NOT A "GENUINE" IRREDUCIBLE.

IF NOT, AN INDUCTIVE ARGUMENT ('ON N') WORKS.

□

<u>NOTE</u> THE INTENDED ANALYSIS WORKS FOR $\mathcal{SB}$ ALSO.