

FINITE CASE PROVED (MULTIPLICA

WANT TO PROVE

$E = F[\alpha_1, \dots, \alpha_r]$ IS A FINITE

EXTENSION OF F AND

ASSUME $\alpha_2, \dots, \alpha_r$ ARE

SEPARABLE OVER F (BUT

NOT NECESSARILY α_1 ,

THEN $\exists \beta \in E$

SUCH THAT $E = F[\beta]$

MINIMAL
POLYNOMIAL
HAS NO
REPEATED
ROOTS

PRIMITIVE
ELEMENT

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] / \mathbb{Q}$$

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$$

SUFFICES TO PROVE FOR

$$R=2 \quad (X-1)^p = X^p - 1 \text{ OVER } \mathbb{Z}_p$$

$$E = F[\alpha_1, \alpha_2] \quad (\text{SIMPLE INDUCTION GIVES THE GENERAL RESULT})$$

LET $E = F[\alpha, \beta]$, β SEPARABLE

LET f, g ARE MINIMAL
POLYNOMIALS OF
 α, β OVER F .

LET $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_s$ BE
ROOTS OF f IN SOME BIG
FIELD CONTAINING E

LET $\beta_1 = \beta, \beta_2, \dots, \beta_t$ BE ROOTS

OF g

FOR $j \neq 1$, $\beta_1 \neq \beta_j$

SO

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1$$

HAS \uparrow SOLUTION $X = \frac{\alpha_1 - \alpha_j}{\beta_1 - \beta_j}$

CHOOSE $c \in F$ SUCH THAT

$$\alpha_i + c\beta_j \neq \alpha_{\hat{i}} + c\beta_{\hat{j}} \text{ UNLESS } \hat{i} = \hat{j} = 1$$

\uparrow

SINCE F IS INFINITE, SUCH

A c EXISTS. (WE CAN

AVOID ALL OF THE X SATISFYING
THE EQUATIONS ABOVE)

SET $\gamma = \alpha + c\beta$ $h(x)$
 THE $g(x)$, $f(\gamma - cx)$
 HAVE COEFFICIENTS IN
 $F[\gamma][x]$. $h(\beta)$
 $g(\beta) = 0$ $f(\gamma - c\beta) = f(\alpha) = 0$
└──────────────────────────────────┘ COMMON
└──────────────────────────────────┘ ROOT

SO $g(x)$, $h(x)$ HAVE β AS
 A COMMON ROOT.

IT'S THE ONLY COMMON ROOT

BECAUSE $\gamma - c\beta_j \neq \alpha_i$
 UNLESS $i = j = 1$

$$h(X) = f(\gamma - cX)$$

WHEN $X = \beta_j$, $\gamma - cX$ IS NOT
ONE OF THE α_i

$$\text{SO } f(\gamma - cX) \neq 0$$

SO

$$\text{gcd}(g(X), h(X)) = X - \beta$$

IN SOME BIG FIELD.

\uparrow \uparrow \uparrow
 $f(\gamma - \beta X)$

BUT gcd HAS COEFFICIENTS
IN THE FIELD WHERE THE
COEFFICIENTS OF THE
POLYNOMIALS LIE.

$$\beta \in F[\gamma]$$

BUT, THEN $\alpha = \gamma - c\beta \in F[\gamma]$

$F[\gamma] \subseteq F[\alpha, \beta]$ SINCE

$$\gamma = \alpha + c\beta$$

↑
IN F

SINCE $\beta \in F[\gamma] \Rightarrow \alpha \in F[\gamma]$

SO $F[\alpha, \beta] \subseteq F[\gamma]$

SO $F[\alpha, \beta] = F[\gamma]$