Section 11.5 part 2

proof of theorem 11.7

Th 11.7 Every finitely generated separable extension is simple.

Additional assumption: the ground field F is infinite.

<u>Pf</u> $K = F(u_1, \dots, u_n)$ Wanted: $u \in K$ such that $K = F(u)$

Induction in n. The case $n=1$ is trivial: $u = u_1$.

It suffices just <u>prove $n=2$</u>, because then induction step is easy: $k-1$ to k - step

$$K = F(u_1, \dots, u_k) = F(u_1, \dots, u_{k-1})(u_k) \underset{\substack{\text{inductive}\\ \text{assumption}}}{=} F(t)(u_k) = F(t, u_k) \underset{\substack{\text{inductive}\\ \text{assumption}\\ \text{or } n=2}}{=} F(u)$$

Section 11.3 p 384 between Ex 4 and Ex 5, also proof of Th 11.10

The proof thus reduces to $n=2$ case

<u>If $K = F(v, w)$, then there exists $u \in K$ such that $K = F(u)$.</u>

Let $p \in F[x]$ be the minimal polynomial for v

$q \in F[x]$ ——— " ——— w

Let L be a splitting field of $pq \in F[x]$

Denote the roots by

$w = w_1, w_2, \ldots, w_n$ — roots of q in L

$v = v_1, v_2, \ldots, v_m$ — " — p — " —

Pick $c \in F$ such that

$$c \neq \frac{v_i - v}{w - w_j} \qquad 1 \le i \le m, \; 1 < j \le n$$

Separability guarantees $w \neq w_j$ for $j > 1$

Since F is infinite, we can certainly find such c

moreover, almost every $c \in F$ (all but finitely many)

Set $\underline{u = v + cw}$ Wanted: $K = F(u)$

$K = F(v, w)$ - given

Suffices: $v, w \in F(u)$ will imply $F(v,w) \subseteq F(u)$ also $F(v, w) \supseteq F(u)$ because $u = v + cw$

Note that

$w \in F(u)$ implies $v = u - cw \in F(u)$

thus we only need to prove that $\underline{w \in F(u)}$

Consider the polynomial

$h = p(u - cx) \in F(u)[x]$ Meaning of the notation: $p(u - cw) = p(x)\big|_{x = u - cx}$

w is a root of h (and q)

$h(w) = p(u - cw) = p(v) = 0$

other roots of q, namely $w_2, \dots w_n$ are not roots of h

because $u - cw_j \neq v_i$ i.e. $v + cw - cw_j \neq v_i$ by the choice of c

The polynomials h and q share exactly one common root in L, that is w

Let $r \in F(u)[x]$ be the minimal polynomial of w over $F(u)$

We expect that $w \in F(u)$ that is $r = x - w$

It suffices to prove that $\underline{\deg r = 1}$

$r | q$ in $F(u)[x]$ because $q(w) = 0$ (Th 11.6)

$r | h$ in $F(u)[x]$ — " — $h(w) = 0$ — " —

Thus every root of r must be also a root of both q and h

Thus, in L, r has no roots except $\underline{w}$.

Since q splits completely in L and $r | q$, the polynomial r cannot have roots outside L (also splits completely in L).

It follows that r no more roots at all except for w.

Thus $\underline{\deg r = 1}$.