明解ガロア理論 [原著第３版] 学習ノート
第８章 ガロア理論の背後にあるアイディア
110 頁

> P_j はすべての j について既約であって，$P(\zeta^j t) = g(t)h(t)$ のとき $P(t) = g(\zeta^{-1}t)h(\zeta^{-1}t)$ である．

わけわからん。$P_j = P(\zeta^j t)$ が既約っていってるのにもかかわらず、$P(\zeta^j t) = g(t)h(t)$ といってるんだから。ここはきっと、$P_j = P(\zeta^j t)$ が可約なら、$P(t)$ も可約になり、矛盾してしまうよ、という背理法ではないのか。

すこし下、誤植ね

> (誤)P と P_j とは $0 \leq k \leq p-1$ であれば互いに素であると主張したい．
> (正)P_k と P_j とは $0 \leq k \leq p-1$ であれば互いに素であると主張したい．

112 頁

> とくに x は $m(t)$ の零点であるが，一方で $m(t)$ のすべての零点は L に属する．したがって $\alpha, x_0, x_2, \ldots, x_{p-1} \in L$ である．

$\alpha, x_0, x_2, \ldots, x_{p-1} \in L$ となるのがわからなかった。
ネット検索してみたら、George M. Bergman という人がこの当たり掘り下げて証明してました。
http://math.berkeley.edu/ gbergman/ug.hndts/
Corrections and Clarifications to Ian Stewart's "Galois Theory", 3rd Edition.

以下では、その George 氏の資料の翻訳をもとに、この帰結を紐解きます。

George の補題
M を L の拡大体（ $L \subseteq M$）とし、p を素数とする。
$\alpha(\neq 0), x_0, \ldots, x_{p-1} \in M$ 及び、1 の p 乗根 $\zeta(\in L)$ による以下、p 個の要素が、L に含まれるとき、$x_0, \alpha x_1, \alpha^2 x_2, \ldots, \alpha^{p-1} x_{p-1} \in L$ となる．このとき、$x_1 = 1$ であれば，$\alpha, x_0, \ldots, x_{p-1} \in L$ となる。

$$x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{p-1} x_{p-1}$$
$$x_0 + (\zeta\alpha) x_1 + (\zeta\alpha)^2 x_2 + \ldots + (\zeta\alpha)^{p-1} x_{p-1}$$

$$x_0 + (\zeta^{p-1}\alpha) x_1 + (\zeta^{p-1}\alpha)^2 x_2 + \ldots + (\zeta^{p-1}\alpha)^{p-1} x_{p-1}$$

証明. それぞれの多項式を $y_0, y_1, \ldots, y_{p-1}$ と置く。

$$y_0 = x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{p-1} x_{p-1}$$
$$y_1 = x_0 + (\zeta\alpha) x_1 + (\zeta\alpha)^2 x_2 + \ldots + (\zeta\alpha)^{p-1} x_{p-1}$$

$$y_{p-1} = x_0 + (\zeta^{p-1}\alpha) x_1 + (\zeta^{p-1}\alpha)^2 x_2 + \ldots + (\zeta^{p-1}\alpha)^{p-1} x_{p-1}$$

$1+\zeta+\ldots+\zeta^{p-1}=0$ のように一般に 1 の n 乗根の和はゼロであるので、
$m=0,\ldots,p-1$ の各 m について、

$$y_0+\zeta^{-m}y_1+\zeta^{-2m}y_2+\cdots+\zeta^{-(p-1)m}y_{p-1}=\alpha^m x_m$$

となる。ここで、$\zeta,y_0,\ldots,y_{p-1}\in L$ なので、$\alpha^m x_m\in L$ がいえる。$x_1=1$ のときは、$\alpha\in L$ であり、各 m について、$\alpha^{-m}\in L$ であり、$\alpha^{-m}\alpha^m x_m=x_m\in L$ がいえる。 □

次は、あらためて証明するまでもないかもしれないが、

補題 tnb
$m(t)$ のすべての根は，$m(t)$ を因子に持つ多項式 $f(t)$ の根となる.

証明. $f(t)$ を $m(t)$ で因数分解すると、

$$f(t)=m(t)g(t)$$

となるが、$m(t)$ を 0 にする根は、$f(t)$ も 0 にする。

□

自明でない箇所
$\alpha,x_0,X_2,\ldots,x_{p-1}\in L$ である。

証明. $x=x_0+\alpha+x_2\alpha^2+\cdots+x_{p-1}\alpha^{p-1}$ とし、係数を K に持つ方程式 $m(x)=0$ を考える。
これは、x については、K 上の方程式だが、α については、R_1 上の方程式である。
次に、$f(\alpha)=0$ を満たす $f(t)\in R_1[t]$ を考える。
この多項式 $f(t)$ は、α の最小多項式 $t^p-a\quad(a\in R_1)$ で割ることができる。
したがって、補題 tnb より、最小多項式 t^p-a のすべての根 $\alpha,\zeta\alpha,\ldots,\zeta^{p-1}\alpha$ は、$f(t)=0$ の根となる。
このことは、$x_0+(\zeta^j\alpha)x_1+(\zeta^j\alpha)^2x_2+\ldots+(\zeta^j\alpha)^{p-1}x_{p-1}(j=0,\ldots,p-1)$ はすべて $m(t)$ の根となることを意味する。
また、**補題 8.18 $q\in L$ とする．このとき q の K 上の最小多項式は L 上の 1 次因子に分解する．**
により、各 j について、$x_0+(\zeta^j\alpha)x_1+(\zeta^j\alpha)^2x_2+\ldots+(\zeta^j\alpha)^{p-1}x_{p-1}\in L$ がいえる。最後に、George の補題より、$\alpha,x_0,x_2,\ldots,x_{p-1}\in L$ がいえる。 □