1　$\mathrm{Ker}(\bar{\phi})$ は極大イデアル (p.182, l.5)

簡単のため、$I = \mathrm{Ker}(\phi)$ とおく。定義から、I の元である多項式 f に θ を代入すれば 0 となる。そのため次の $\bar{\phi}$ が ϕ から自然に導かれる。

$$
\begin{array}{rccc}
\bar{\phi}: & K[x]/I & \to & K(\theta) \\
 & f(x)+I & \mapsto & f(\theta)
\end{array}
$$

補題 4.5 より、$\mathrm{Irr}(\theta, K, x)$ が既約元であることを示せば I は極大イデアルであることが分かる。そのことから次のように論理がつながる。

$$\mathrm{Im}(\bar{\phi}) \text{ が } K \text{ と}\theta\text{を含む体}^{1)} \implies \mathrm{Im}(\bar{\phi}) = K(\theta) \implies K[x]/I \text{ も体なので}\bar{\phi}\text{は } K\text{-同型}$$

まず、一変数多項式環 $K[x]$ は PID である。これは $K[x]$ がユークリッド環であること、さらにユークリッド環は PID であることから分かる。詳細は p.87 の例 4.6 と p.88 下。

I は $K[x]$ のイデアルで、しかも $K[x]$ は PID だから、I は $f(x) \in K[x]$ から生成される。この生成元 $f(x)$ は I の元の内で次数が最小のものである。なぜなら I は θ を代入すると 0 になる多項式全体で、I の元であって $f(x)$ より次数が大きい多項式[2] が生成するイデアルは $f(x)$ を含まず、I とは一致しないからである。p.88 下から、これは $f(x)$ が既約元であることを言っている。

1.1　注意: 最小多項式は唯一つ

上のような $f(x)$ を適当にとって単数倍しても同じイデアルを作るから、最高次の係数が 1 である最小多項式 $\mathrm{Irr}(\theta, K, x)$ をこれらの代表に取れる。まとめると、最小多項式の定義は次のようになる。

定義 1.1. 最小多項式とは、次の条件を満たす $f(x) \in K[x]$ のことである。

1. $f(x)$ は θ を根に持つ。
2. $f(x)$ は θ を根に持つ $K[x]$ の元の中で、次数が最小。
3. 最高次の係数が 1

仮に f, g が最小多項式であったとすると、新たな多項式 $h = f - g$ も条件 1 を満たす。しかし条件 2, 3 から $\deg(h) < \deg(f) - 1 = \deg(g) - 1$ となり、f, g の条件 2 に反する。$K(\theta)$ をベクトル空間と見ると、これは次のように表現できる。

命題 1.2. θ が次数 n の代数的数だとすると、$0 \in K(\theta)$ は $K(\theta)$ の元達 $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ の線型結合によってただ一通りに書かれる。

p.182 の命題 1.5 はさらに $K(\theta)$ の全ての元がこのように表せることを言っている。

命題 1.3 (命題 1.5)**.** θ が K の代数的数であるとき、K 上のベクトル空間 $K(\theta)$ の基底として $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ が取れる。

---

1) $x + I \in K[x]/I$ が θ に行く

2) 例えば $x \cdot f(x)$ など

1.2　命題 1.5 について

証明の概略を述べる。すでに $K[x]/I \overset{\bar{\phi}}{\simeq} K(\theta)$ を述べたのでこれを使おう。$K[x]$ を $K[x]/I$ に射影して 0 に潰れない元は、最小多項式 $\mathrm{Irr}(\theta, K, x)$ よりも次数が小さい K 上の多項式、すなわち $K + Kx + \cdots + Kx^{n-1}$ の元である。$K[x]/I = \{f + I | f \in K + Kx + \cdots + Kx^{n-1}\}$ と表せるから、

$$K + Kx + \cdots + Kx^{n-1} \overset{(\bar{\psi})^{-1}}{\simeq} K[x]/I \overset{\bar{\phi}}{\simeq} K(\theta)$$

左から右へ元がどのように写されるかを思い出すと、$f(x) \mapsto f(x) + I \mapsto f(\theta)$ となっていた。$f(x)$ は $K + Kx + \cdots + Kx^{n-1}$ の任意の元だから、命題が成り立つ。

$1 \in K(\theta)$ がただ一つの表現を持つことを示すという方針も思いつくが、最小多項式の「最高次の係数が 1」という条件は「0 は (単) 数倍しても 0」というところから来ていたことを考えれば、これは使えないと分かる。

命題 1.5 を命題 1.3 との関連で考えると、拡大 L/K が単拡大の代数拡大であった時には命題 1.3 で出てくる分母 $g(\theta)$ は（0 でない）定数に変換でき、しかも分子 $f(\theta)$ は次数が n 未満であるものに限る、と言っている。

2　定理 2.8(1) について

2.1　代数的閉包の存在

最初の方針は任意の定数でない多項式 $f(x) \in K[x] \setminus K$ が少なくとも 1 根を持つような、K の拡大体 L_1 を作る、というものである。K と L_1 はどちらも体だから、拡大を繰り返せるだろう。

さてどうやって拡大させるかが問題である。L_1 が持つべき条件を整理して再度述べる。ただし $K[x]^* = K[x] \setminus K$ である。

(A) L_1 は K の拡大体

(B) $\forall f \in K[x]^*,\ \exists \theta_f \in L_1 \setminus \{0\},\ s.t.\ f(\theta) = 0$

(B) で θ_f と添字をつけたのは、f によってその根が決まる、という気持ちからである。

やりたいことは、以上の条件を持つ拡大体を作ることだ。似たようなことをやった例として根体の存在を示すことをした。この時は多項式環の既約多項式で生成される極大イデアルによる剰余体が根体になっていた。同様に、K に不定元を入れて極大イデアルで割りたい。

ではどのような不定元を入れて、どのような極大イデアルで割るべきか？後半から考えていこう。極大イデアルで割った後は $f(\theta) = 0$ となってほしいが、これは極大イデアルに $f(\theta)$ が入っていれば、ちょうどそのようになる!　そうなると θ は f の根に対応するものだから、$K[x]$ の既約多項式（しかも最高次の係数を 1 だとかに特定したもの）と一対一対応させるとよい。

まとめると次のようになる。簡単のために、$K[x]$ の既約多項式最高次の係数が 1 であるものの全体を $\Im$ とする。K には $f \in \Im$ に対応して不定元を入れ、$K[\{R_f\}_{f \in \Im}]$ とする。これを $\{f(R_f)\}_{f \in \Im}$ を含む極大イデアルで割れば良い。こうしてできた体は、$K[x]$ の既約多項式の根を少なくとも一つ持つ。操作を繰り返せば、$K[x]$ の既約多項式は全て 1 次式へ分解できる。

2.2 根体を作る時との違い

根体を作る時と違うのは、$\{f(R_f)\}_{f\in\Im}$ が生成するイデアルが極大イデアルかわからない、ということである。根体の時は不定元を 1 つだけ入れて $K[X]$ とし、さらに $K[X]$ が PID であることから既約多項式が生成するイデアル $(f(X))$ が極大イデアルとなることを導いた。しかし今は多数の不定元を入れたので、$K[\{R_f\}_{f\in\Im}]$ は PID ではなく、既約多項式達が作るイデアル $(\{f(R_f)\}_{f\in\Im})$ が極大かどうかはわからない。しかし $(\{f(R_f)\}_{f\in\Im})$ は真のイデアル [3] であることがわかるので、これを含む極大イデアルの存在が保証される。

3 定理 2.8(2) について

圏論的に見てみる。まず、K_1 と $\bar{K}_1$ の中間体達を以下のように並べる。ここにある射は全て埋め込み (insection) だ。

$$
\begin{tikzcd}
\bar{K}_1 & & & & \\
L_1 \arrow[u] \arrow[r] & L_2 \arrow[ul] \arrow[r] & L_3 \arrow[ull] \arrow[r] & L_4 \arrow[ulll] \arrow[r] & \cdots \arrow[ullll] \\
K_1 \arrow[u] \arrow[ur] \arrow[urr] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}
$$

中間体達の間ではこのような挿入射だけを考える。ここは poset になる。

さらに K_2 と $\bar{K}_2$ が現れる。この図は可換になっていることに注意。

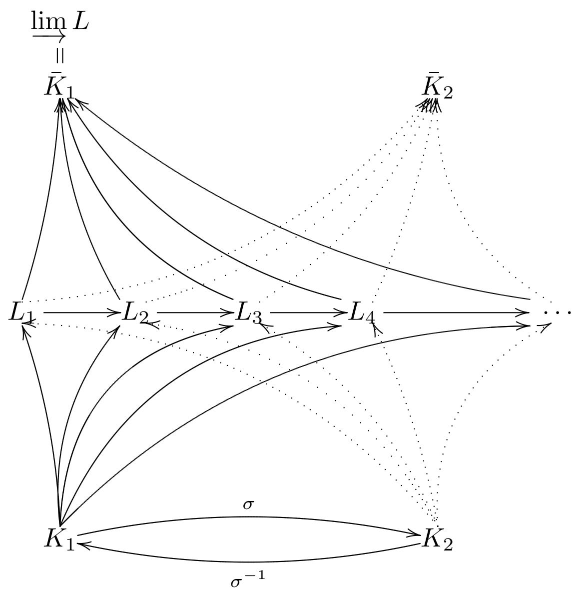
$$
\begin{tikzcd}
\bar{K}_1 & & & \bar{K}_2 & \\
L_1 \arrow[u] \arrow[r] \arrow[urrr, dotted] & L_2 \arrow[ul] \arrow[r] \arrow[urr, dotted] & L_3 \arrow[ull] \arrow[r] \arrow[ur, dotted] & L_4 \arrow[ulll] \arrow[r] \arrow[u, dotted] & \cdots \arrow[ullll] \arrow[ul, dotted] \\
K_1 \arrow[u] \arrow[ur] \arrow[urr] \arrow[urrr] \arrow[urrrr] \arrow[rrr, bend left, "\sigma"] & & & K_2 \arrow[lll, bend left, "\sigma^{-1}"] \arrow[ulll, dotted] \arrow[ull, dotted] \arrow[ul, dotted] \arrow[u, dotted] \arrow[ur, dotted] &
\end{tikzcd}
$$

---

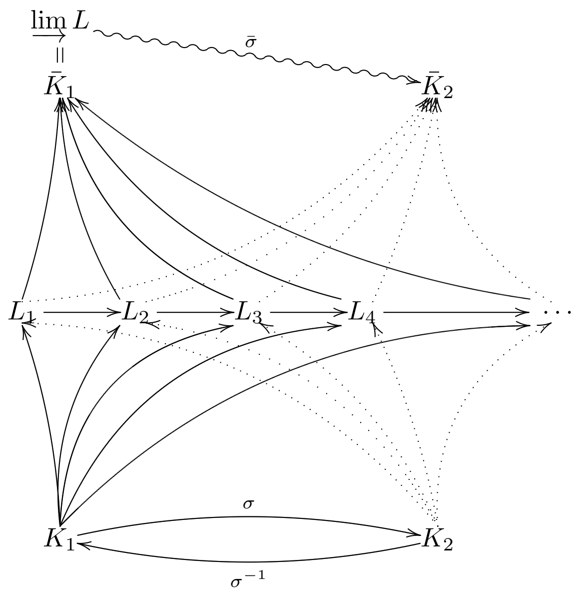
[3] $(\{f(R_f)\}_{f\in\Im}) \neq K[\{R_f\}_{f\in\Im}]$

煩雑であったため、挿入射を表す矢印の根本のカールは取り除いた。この図にある点線は準同型を表していて、具体的な内容は σ によって決まる。しかし σ と点線の合成は K_1 から中間体への挿入射に等しいので、ほとんど挿入射に近い。また、この時点で射を追っても、同型射の拡張は言えない。中間体への射は全て準同型だからである。

さて、中間体達は poset となっているから、この構造を反映した関手 $L : \mathbf{Pos} \to \mathbf{Field}$ をとり、余極限 $\varinjlim L$ を見る。これは中間体の poset が帰納的順序集合であることからその存在が出る中間体の極大元である。すると詳細な議論から $\varinjlim L = \bar{K}_1$ が分かる。つまり $\bar{K}_1$ は Cocone(D) の終対象としての UMP を持つのである。



$\varinjlim L$ の UMP から、$\varinjlim L$ から $\bar{K}_2$ へ、すでに有る射を可換にする射がただ一つ存在する。中間体達から $\bar{K}_2$ への射（母線）は σ によって定まるから、この射も σ によって定まる。



最後に、$\bar{K}_1$ と $\bar{K}_2$ が共に代数的閉包であることを用いる。まず、$\bar{\sigma}(\varinjlim L) \simeq \bar{K}_1$ から $\bar{\sigma}(\varinjlim D)$ は代数的閉包。図式の射は全て準同型だから $\bar{\sigma}(\varinjlim L) \subset \bar{K}_2$ となる。この二つと $\bar{\sigma}(\varinjlim D)$,$\bar{K}_2$ が

特に代数閉体であることから、$\bar{\sigma}(\varinjlim L) = \bar{K}_2$ が分かる [4]。よって $\bar{\sigma}$ は全射。体同士の準同型は単射であったから、とくに同型射。

4　定理 5.1(1) について

4.1　「明らかに $\sigma \in G$ はこれらを全体として保つ」

$$\sigma \in G = \mathrm{Aut}(L/K) = \{\sigma : L \to L\}$$

より明らかに $\sigma(\theta) \in L$ である。さらに $\theta \in L$ の (K 上の) 共役元は群 $\mathrm{Aut}(L/K)$ による θ の軌道 $\theta\,\mathrm{Aut}(L/K)$ の元。なので $\theta \in L$ の共役元 $\theta_i \in L$ は $\sigma \in \mathrm{Aut}(L/K)$ によって L に属すような θ の共役元へ写る。

4.2　$f \in K[x] \implies f = \mathrm{Irr}(\theta, K, x)$

「$f(x)$ の係数は $K = F(G)$ に入る」から「θ の任意の K 上の共役元は $f(x) \in K[x]$ の根となり」の導出をまとめるとこのようになる。しかしこれは $\deg f \leq \deg \mathrm{Irr}(\theta, K, x)$ と、$\mathrm{Irr}(\theta, K, x)$ が θ を根に持つ K 係数の多項式として次数が最小のものであることから自明である。$\deg f \leq \deg \mathrm{Irr}(\theta, K, x)$ は、$f(x)$ の根が θ の K 上の共役元であり、したがって $\mathrm{Irr}(\theta, K, x)$ よりも根が少ないか等しいことから分かる。

正規拡大であることの証明として以下のような方針もありうる。まず $\mathrm{Aut}(\bar{K}/K)$ の元の定義域を L に制限し、$\sigma : L \to \bar{L} = \bar{K}$ とする。証明することは命題 3.1 の (2)、すなわち任意の L の元を σ で写した時に L からはみ出さないことである。$\alpha \in L$ の K 上の共役元全体を Θ_α とおく。すでに述べたとおり、

$$\sigma(\Theta_\alpha \cap L) = \Theta_\alpha \cap L$$

である。このことから、

$$\bigcup_{\alpha \in L} \Theta_\alpha = L$$

が示せれば十分。

5　定理 5.2(2) について

5.1　「$\tilde{r}$ は全射」

シュタイニッツの定理より、$\mathrm{Gal}(L/K)$ の元 $\sigma : L \to L(K-\text{同型})$ は $\mathrm{Aut}(\bar{K}/K)$ の元 $\bar{\sigma} : \bar{K} \to \bar{K}(K-\text{同型})$ に拡張される。よって $\tilde{r}$ は全射。

[4] 定理 2.8 の直前に有る「K が代数閉体で $K \subset L$ なら $\bar{K}_L = K$」という記述はこのことを言っている。表現をこれに合わせると、「$\bar{K}_2$ の任意の代数拡大体 L について $\overline{(\bar{\sigma}(\varinjlim L))}_L = \bar{K}_2 = \overline{(\bar{K}_2)}_L$」

5.2 M/K が正規拡大 $\Longleftrightarrow$ ...

$$\begin{aligned} & M/K \text{ が正規拡大} \\ \Longleftrightarrow \quad & \forall\sigma \in Aut(\bar{K}/K), \sigma(M) = M \\ \Longleftrightarrow \quad & \forall\sigma \in Aut(\bar{K}/K), \phi(\sigma(M)) = \phi(M) \end{aligned}$$

二行目はシュタイニッツの定理より。三行目は ϕ の単射性より。

5.3 系 3.3 について

シュタイニッツの定理より、$\sigma : L \to \bar{K}$ は $\bar{\sigma} : \bar{L} = \bar{K} \to \bar{K}$ に拡張される。しかも命題 3.1(2) より $\bar{\sigma}(L) = L$ である。

5.4 「$r : Aut(L/K) \to Gal(M/K)$ は全射」

$\sigma \in \mathrm{Gal}(M/K)$ を任意にとる。σは $M \to M$ の K-同型だから、シュタイニッツの定理よりこれは K-同型 $\bar{\sigma} : \bar{M} \to \bar{M}$ に拡張される。これを L に制限すると、これがさらに K-同型 $\bar{\sigma}|_L : L \to L$ となる。これが K-同型であることは、K-同型の定義 $\bar{\sigma}|_K = id_K$ と $K \subset L$ より。以上より、$\mathrm{Gal}(M/K)$ の各元に対して $\mathrm{Aut}(L/K)$ の元 $\bar{\sigma}|_L$ が存在する。よって r は全射。

5.5 $\sigma|_L : L \to L$

写像 $\sigma : \bar{K} \to \bar{K}$ は制限で $\sigma|_L : L \to L$ になるか？つまり、$\sigma(L) = L$ か？これは L/K が正規拡大であることと命題 3.1(2) より真。

6 命題 5.4 について

6.1 L/K が有限かつ分離的拡大なら L'/K' もそうか？

$L'/L/(L\cap K')$ と $L'/K'/(L\cap K')$ とを考える。まず、仮定と命題 4.5(1) より $L/L\cap K'$ は分離的拡大。系 4.6 を分離的拡大 $L/(L\cap K')$ と適当な拡大 $K'/(L\cap K')$ について用いて、$(L\cdot K' =)L'/K'$ が分離的拡大であることが出る。