CENTRO DE ESTUDOS MATEMÁTICOS

SOBRE OS CORPOS COMUTATIVOS

POR

A. ALMEIDA COSTA

FACULDADE DE CIÊNCIAS DO PORTO
1946

PUBLICAÇÕES DO CENTRO DE ESTUDOS MATEMÁTICOS
DA
FACULDADE DE CIÊNCIAS DO PORTO

N.º 17

SOBRE OS CORPOS COMUTATIVOS

SUBSIDIADA PELA JUNTA DE INVESTIGAÇÃO MATEMÁTICA

ANAIS DA FACULDADE DE CIÊNCIAS DO PORTO
Fundados por F. GOMES TEIXEIRA
e continuados sob a direcção de A. MENDES CORRÊA
Extracto do tomo XXXI.

Sobre os corpos comutativos

POR

A. ALMEIDA COSTA
Prof. ext. da Faculdade de Ciências do Porto

PORTO
Imprensa Portuguesa
108, Rua Formosa, 116
—
1946

Extracto do fasc. II do tomo XXXI
DOS
«Anais da Faculdade de Ciências do Porto

SOBRE OS CORPOS COMUTATIVOS

1) Indicações gerais — Alguns dos resultados estabelecidos por E. STEINITZ na sua célebre memória *Algebraische Theorie der Körper*, publicada em 1910 no *Journal für die reine und angewandte Mathematik* (Band 137, págs. 167 a 308), demonstram-se também utilizando certas proposições que fazem intervir a noção de «isomorfismo dos corpos $\mathfrak{L}$ e $\mathfrak{L}'$ relativo a um corpo $\mathfrak{R}$ contido naqueles dois», como pode ver-se no livro de B. L. VAN DER WAERDEN, *Moderne Algebra* (I Teil, Cap. v, págs. 86 a 122), de 1930. Pomos aqui esse facto igualmente em evidência. Damos justo relevo, pelas aplicações que fazemos, ao teorema que diz ser simples uma ampliação $\mathfrak{R}(\alpha, \beta)$, de $\mathfrak{R}$, em que β é elemento separável, e, utilizando a exposição de A. A. ALBERT, feita de págs. 32 a 35 do seu livro *Structure of algebras*, de 1939, estabelecemos certos resultados interessantes sobre ampliações inseparáveis dum corpo $\mathfrak{R}$. Julgamos novos alguns desses resultados, enquanto outros são extensões de teoremas conhecidos. Para as demonstrações de toda a doutrina sobre corpos comutativos invocada neste trabalho pode consultar-se também o nosso livro *Elementos da Teoria dos Anéis* (Cap. v, págs. 166 a 247), de 1943.

$\mathfrak{L}$ será sempre uma ampliação finita dum corpo $\mathfrak{R}$, de característica p. Se $u_1, \ldots, u_n$ constituirem uma base de $\mathfrak{L}$, escreveremos $\mathfrak{L} = \mathfrak{R}\{u_1, \ldots, u_n\}$. A notação $\mathfrak{R}(u_1, \ldots, u_n)$ fica reservada para o corpo que resulta de $\mathfrak{R}$ por adjunção algébrica dos elementos $u_1, \ldots, u_n$. Seja $\alpha \in \mathfrak{L}$. Representaremos por n o grau de α relativamente a $\mathfrak{R}$, por n_0 o seu grau reduzido e por t o expoente. $\mathfrak{L}_0$ designará a ampliação separável de $\mathfrak{R}$ contida em $\mathfrak{L}$ e poremos: $(\mathfrak{L}_0/\mathfrak{R}) = N_0 =$ grau reduzido de $\mathfrak{L}$; $(\mathfrak{L}/\mathfrak{R}) = N =$ grau

de $\mathfrak{L}$; e = expoente de $\mathfrak{L}$. Para o elemento α tem lugar $\alpha^{p^t} \in \mathfrak{L}_o$, $\alpha^{p^{t-k}} \notin \mathfrak{L}_o$, $(t \geqq k \geqq 1)$. E são válidas as igualdades $(\mathfrak{R}(\alpha)/\mathfrak{R}) = n = n_o p^t$, $(\mathfrak{R}(\alpha^{p^t})/\mathfrak{R}) = n_o$, $\big(\mathfrak{R}(\alpha)/\mathfrak{R}(\alpha^{p^t})\big) = p^t$. Desta última tira-se imediatamente que a equação $x^{p^t} - \alpha^{p^t} = 0$ é irredutível em $\mathfrak{R}(\alpha^{p^t})$. Ela é também irredutível em $\mathfrak{L}_o$, em virtude de ser $\alpha^{p^{t-1}} \notin \mathfrak{L}_o$. $\mathfrak{R}(\alpha)$ é uma ampliação inseparável simples de $\mathfrak{R}$, na qual a ampliação separável de índice zero é $\mathfrak{R}(\alpha)_o = \mathfrak{R}(\alpha^{p^t})$. Para se concluir esta última afirmação, recordemos o teorema seguinte (1): é condição necessária e suficiente, para que $\mathfrak{L}$ seja ampliação simples de $\mathfrak{R}$, que se tenha $(\mathfrak{L}/\mathfrak{R}) = N_o p^e$. No nosso caso deverá ter-se $(\mathfrak{R}(\alpha)/\mathfrak{R}) = N_o p^e = n_o p^t$, com $t \leqq e$, $n_o \leqq N_o$. Será $N_o = n_o$, $e = t$, e, portanto, $\mathfrak{R}(\alpha)_o = \mathfrak{R}(\alpha^{p^t})$, pois este último é separável e de grau N_o.

2) **Sobre as ampliações finitas dos corpos comutativos** — O grau reduzido n_o é sempre um divisor de N_o. A possibilidade de ser $n_o = N_o$ é dada pelo seguinte

TEOREMA 1: — *É condição necessária e suficiente, para que* $\alpha \in \mathfrak{L}$ *seja de grau reduzido* $n_o = N_o$, *que se tenha* $\mathfrak{L}_o(\alpha) = \mathfrak{R}(\alpha)$. Se é $n_o = N_o$, tem-se $(\mathfrak{R}(\alpha)/\mathfrak{R}) = N_o p^t$. Como é $(\mathfrak{L}_o(\alpha)/\mathfrak{L}_o) = p^t$, vem $(\mathfrak{L}_o(\alpha)/\mathfrak{R}) = p^t . N_o$, de modo que a condição é necessária. Inversamente, supondo $\mathfrak{L}_o(\alpha) = \mathfrak{R}(\alpha)$, é $(\mathfrak{R}(\alpha)/\mathfrak{R}) = n = n_o p^t = p^t . N_o$.

Existem elementos separáveis $\theta \in \mathfrak{L}$ que satisfazem ao teorema: são todos aqueles para os quais é $\mathfrak{L}_o = \mathfrak{R}(\theta)$, e apenas esses. Há também elementos inseparáveis $\mu \in \mathfrak{L}$ nas condições do teorema: são todos aqueles para os quais é $\mathfrak{R}(\mu) \supset \mathfrak{L}_o$, e apenas esses. Se supusermos $\mathfrak{L}_o = \mathfrak{R}(\theta)$, é, para cada elemento inseparável $\alpha \in \mathfrak{L}$,

$$\mathfrak{R}(\theta, \alpha) = \mathfrak{R}(\alpha, \theta) = \mathfrak{L}_o(\alpha) = \mathfrak{R}(\mu) \text{ (2)} \supset \mathfrak{L}_o.$$

(1) VAN DER WAERDEN (de futuro v. W.), pág. 118; e ALMEIDA COSTA (de futuro A. C.), pág. 212.

(2) $\mathfrak{R}(\alpha, \theta)$ é ampliação simples de $\mathfrak{R}$; v. W., pág. 120 (ou A. C., pág. 199).

TEOREMA 2: — *Em* $\mathfrak{L}$ *há elementos simultâneamente de grau reduzido* N_o *e de expoente* t = *expoente dum elemento arbitrário* $\alpha \in \mathfrak{L}$. Ponhamos $\mathfrak{L}_o = \mathfrak{R}(\theta)$ e consideremos o corpo $\mathfrak{L}_o(\alpha) = \mathfrak{R}(\theta, \alpha) = \mathfrak{R}(\lambda)$. O elemento λ é de grau reduzido N_o. Como $\mathfrak{R}(\lambda)$ é uma ampliação simples, na qual o corpo separável relativamente a $\mathfrak{R}$ é ainda $\mathfrak{L}_o$, pode escrever-se, se e' é o seu expoente,

$$(\mathfrak{R}(\lambda) \mid \mathfrak{R}) = N_o p^{e'} = (\mathfrak{L}_o(\alpha) \mid \mathfrak{L}_o) \, . \, N_o = p^t \, . \, N_o \, ,$$

donde se conclui o teorema. Em particular, há em $\mathfrak{L}$ elementos de grau reduzido N_o e de expoente $t = e$ = expoente de $\mathfrak{L}$ (1). O número t toma, de resto, todos os valores inteiros satisfazendo a $0 \leqq t \leqq e$, visto que, se α é de expoente e, α^p é de expoente $e-1$, α^{p^2} de expoente $e-2$, etc.

Seja Ω uma ampliação algébrica de $\mathfrak{R}$. Representaremos por $\Omega^{(p)}$ o corpo que resulta de $\mathfrak{R}$ por adjunção de todas as potências ω^p dos elementos $\omega \in \Omega$. Mais geralmente, escreveremos $\Omega^{(p^r)}$ para significar o corpo que resulta de $\mathfrak{R}$ por adjunção das potências ω^{p^r}.

TEOREMA 3: — *Se* Ω *é uma ampliação separável de* $\mathfrak{R}$, *tem-se* $\Omega^{(p)} = \Omega$. De facto, tomemos $\alpha \in \Omega$. Como é $\mathfrak{R}(\alpha^p) = \mathfrak{R}(\alpha)$ (2), é $\alpha \in \mathfrak{R}(\alpha^p) \subseteq \Omega^{(p)}$, *q.e.d.*

Suponhamos $\Omega = \mathfrak{L} = \mathfrak{R}\{u_1, \ldots, u_n\}$ uma ampliação inseparável. Se fizermos a adjunção a $\mathfrak{R}$ dos elementos $u_1^{p^r}, \ldots, u_n^{p^r}$, obtém-se um corpo $\Delta = \mathfrak{R}(u_1^{p^r}, \ldots, u_n^{p^r})$, contido em $\mathfrak{L}^{(p^r)}$. Um elemento deste último pertence, porém, a um corpo $\mathfrak{R}(\xi_1^{p^r}, \ldots, \xi_s^{p^r})$, no qual se tem $\xi_i^{p^r} = u_1^{p^r} k_1^{p^r} + \ldots + u_n^{p^r} k_n^{p^r}$, pondo $\xi_i = u_1 k_1 + \ldots + u_n k_n$, $(k_i \in \mathfrak{R})$. Sendo $\mathfrak{R}(\xi_1^{p^r}, \ldots, \xi_s^{p^r}) \subseteq \Delta$, tem-se $\mathfrak{L}^{(p^r)} \subseteq \Delta$, e, portanto, $\mathfrak{L}^{(p^r)} = \Delta$. Também se demonstram relações como a seguinte: $\mathfrak{L}^{(p)(p)} = \mathfrak{L}^{(p^2)}$. Na verdade, pondo $\mathfrak{L}^{(p)} = \mathfrak{R}(u_1^p, \ldots, u_n^p) = \mathfrak{R}\{x_1, \ldots,$

(1) E. STEINITZ, *loc. cit.*, pág. 240.

(2) E. STEINITZ, pág. 234 (ou A. C., pág. 194).

$x_t\}$. tem-se $\mathfrak{L}^{(p)(p)} = \mathfrak{R}(x_1^p, \ldots, x_t^p)$. Ora $u_i^{p^2}$ pertence a este último corpo, em virtude de ser $u_i^p \in \mathfrak{R}\{x_1, \ldots, x_t\}$, e, portanto, é $\mathfrak{L}^{(p^2)} \equiv \mathfrak{L}^{(p)(p)}$ (1). Inversamente, se tomarmos o polinómio nos u_k,

$$x_j = \sum b_{i_1 \ldots i_n}^{(j)} (u_1^p)^{i_1} \ldots (u_n^p)^{i_n},$$

com coeficientes em $\mathfrak{R}$, vê-se ser x_j^p um polinómio nos $\equiv_j^{p^2}$, com coeficientes em $\mathfrak{R}$, pelo que se terá $\mathfrak{L}^{(p)(p)} \equiv u\mathfrak{L}^{(p^2)}$. Podemos enunciar o seguinte

TEOREMA 4: — *Se* $\mathfrak{L} = \mathfrak{R}\{u_1, \ldots, u_n\}$ *é uma ampliação finita de* $\mathfrak{R}$, *tem-se* $\mathfrak{L}^{(p^r)} = \mathfrak{R}(u_1^{p^r}, \ldots, u_n^{p^r})$ *e* $\mathfrak{L}^{(p^{r+1})} = \mathfrak{L}^{(p^r)(p)}$. A afirmação é também válida se supusermos $\mathfrak{L} = \mathfrak{R}(u_1, \ldots, u_n)$.

TEOREMA 5: — *Se* $\mathfrak{L}$ *é inseparável, tem lugar a relação* $\mathfrak{L} \supset \mathfrak{L}^{(p)}$. Seja e o expoente de $\mathfrak{L}$. Imaginando que poderia ter-se $\mathfrak{L} = \mathfrak{L}^{(p)} = \ldots = \mathfrak{L}^{(p^e)} = \mathfrak{R}(u_1^{p^e}, \ldots, u_n^{p^e})$, como os $u_i^{p^e}$ são elementos separáveis relativamente a $\mathfrak{R}$, $\mathfrak{L}$ seria uma ampliação separável, contra a hipótese.

TEOREMA 6: — *É válida a igualdade* $\mathfrak{L}_o = \mathfrak{L}^{(p^e)}$. Já sabemos que se tem $\mathfrak{L}^{(p^e)} \equiv \mathfrak{L}_o$. A relação inversa tem também lugar, porque, se $\alpha \in \mathfrak{L}_o$, valem as igualdades $\mathfrak{R}(\alpha) = \mathfrak{R}(\alpha^p) = \ldots = \mathfrak{R}(\alpha^{p^e}) \equiv \mathfrak{L}^{(p^e)}$, o que mostra ser $\alpha \in \mathfrak{L}^{(p^e)}$.

Resulta daqui que, se considerarmos a cadeia

$$\mathfrak{L} \supset \mathfrak{L}^{(p)} \supset \mathfrak{L}^{(p^2)} \supset \ldots, \qquad (1)$$

a mesma, que é necessàriamente finita, termina na ampliação separável $\mathfrak{L}_o = \mathfrak{L}^{(p^e)}$, de $\mathfrak{R}$. O expoente e, além de poder caracterizar-se com o comprimento da cadeia (1), pode também definir-se como o máximo dos expoentes t_i

(1) Cfr. A. A. ALBERT (de futuro A. A.), *loc. cit.*, pág. 33.

dos elementos u_i, da base de $\mathfrak{L}$. Se e' for esse máximo, tem-se, com efeito, $\mathfrak{L}^{(p^{e'-1})} \supset \mathfrak{L}_o \equiv \mathfrak{L}^{(p^{e'})}$.

Um teorema que pode enunciar-se é o seguinte:

TEOREMA 7: — *É condição necessária e suficiente, para que* $\mathfrak{L}$ *seja ampliação simples de* $\mathfrak{R}$, *que se tenha* $\Delta = (\mathfrak{L}^{(p^i)}/\mathfrak{L}^{(p^{i+1})}) = p$, *para cada* $i \lesseqgtr e-1$. É claro, com efeito, que o grau de Δ é uma potência de p. Por ex., de

$$(\mathfrak{L}/\mathfrak{R}) = \mathfrak{L}/\mathfrak{L}^{(p)}) \ (\mathfrak{L}^{(p)}/\mathfrak{L}_o) \ (\mathfrak{L}_o . \mathfrak{R}) = N_o \ p^f,$$

tira-se $(\mathfrak{L}/\mathfrak{L}^{(p)}) \ (\mathfrak{L}^{(p)}/\mathfrak{L}_o) = p^f$.

No caso das ampliações simples, cada corpo $\mathfrak{L}^{(p^{e-k})}$ é também o corpo $\mathfrak{L}_k$, conjunto dos elementos de $\mathfrak{L}$ de expoente $\lesseqgtr k$. Para o ver, basta notar que, na cadeia $\mathfrak{L}_o \subset \subset \mathfrak{L}_1 \subset \mathfrak{L}_2 \subset \ldots \subset \mathfrak{L}_e = \mathfrak{L}$, não pode ter lugar o sinal $=$, pois, se α é de expoente e, $\alpha^{p^e} \in \mathfrak{L}_o$; $\alpha^{p^{e-1}} \in \mathfrak{L}_1$ mas não a $\mathfrak{L}_o$, etc.; e notar ainda que o grau dum $\mathfrak{L}_i$ relativamente a $\mathfrak{L}_o$ é necessàriamente uma potência de p.

Seja Ω uma ampliação algébrica inseparável de $\mathfrak{R}$, finita ou não. Se o grau reduzido de cada elemento $\alpha \in \Omega$ for a unidade, Ω diz-se uma *ampliação inseparável pura* (abrev. ampliação pura) de $\mathfrak{R}$. Quando α pertence a $\mathfrak{R}$, é verificada a equação irredutível em $\mathfrak{R}$, $x - \alpha = 0$; mas, se $\alpha \notin \mathfrak{R}$, como a equação irredutível tem as raízes todas iguais, ela será da forma $x^{p^t} - \alpha^{p^t} = 0$. Reciprocamente, se cada elemento $\alpha \in \Omega \supset \mathfrak{R}$ verifica uma equação irredutível em $\mathfrak{R}$ da forma anterior ($t \lesseqgtr 0$), o grau reduzido de α é a unidade e a ampliação algébrica é pura. Vale o

TEOREMA 8: — *É condição necessária e suficiente, para que a ampliação algébrica* Ω, *de* $\mathfrak{R}$, *seja pura, que cada* $\alpha \in \Omega$ *verifique uma equação irredutível em* $\mathfrak{R}$ *da forma* $x^{p^t} - \alpha^{p^t} = 0$.

Quando o corpo separável Ω_o é idêntico a $\mathfrak{R}$, cada elemento $\alpha \in \Omega$ satisfaz a uma equação irredutível em $\mathfrak{R}$ da forma $x^{p^t} - \alpha^{p^t} = 0$, de modo que Ω é ampliação pura. Inversamente, se Ω é ampliação pura, um elemento $\alpha \in \Omega$

que seja separável satisfaz a $x-\alpha=0$, de sorte $\alpha \in \mathfrak{R}$, $\Omega_o=\mathfrak{R}$. Pode, pois, enunciar-se o

TEOREMA 9: — *É condição necessária e suficiente, para que a ampliação algébrica* Ω, *de* $\mathfrak{R}$, *seja pura, que se tenha* $\Omega_o=\mathfrak{R}$.

É claro que Ω é sempre ampliação pura de Ω_o. No caso duma ampliação finita $\mathfrak{L}$, de $\mathfrak{R}$, podemos caracterizá-la como ampliação pura pelo

TEOREMA 10: — *É condição necessária e suficiente, para que a ampliação finita* $\mathfrak{L}$, *de* $\mathfrak{R}$, *seja pura, que o seu grau reduzido seja a unidade.*

COROLÁRIO 1: — *Se* θ *satisfaz a uma equação irredutível em* $\mathfrak{R}$ *da forma* $x^{p^t}-\theta^{p^t}=0$, *a ampliação* $\mathfrak{R}(\theta)$ *é inseparável pura.* Escrevendo, com efeito $(\mathfrak{R}(\theta)/\mathfrak{R})=N_o p^e=p^t$, $(e \gtreqless t)$, vê-se que se tem $N_o=1$.

LEMA 1: — *Se* $\varphi(x)=0$, *é uma equação do grau* $n=n_o p^t$, *irredutível em* $\mathfrak{R}$, *não pode, numa ampliação separável* $\mathfrak{M}$, *de* $\mathfrak{R}$, *ter-se* $\varphi(x)=f(x).g(x)$, *onde* $f(x)$ *é irredutível em* $\mathfrak{M}$ *e admite todas as raízes de* $\varphi(x)$. Para o caso de se ter $t=0$, o teorema é banal. Se $t \neq 0$, ponhamos

$$\varphi(x)=\prod_{i=1}^{n_o}(x-\alpha_i)^{p^t}=\prod_{i=1}^{n_o}(x^{p^t}-\alpha_i^{p^t}), \qquad (\alpha_i \neq \alpha_j).$$

Se for

$$f(x)=\prod_{i=1}^{n_o}(x-\alpha_i)^{p^{t-k}}=\prod_{i=1}^{n_o}(x^{p^{t-k}}-\beta_i) \left\{ \begin{array}{l} \beta_i=\alpha_i^{p^{t-k}} \neq \beta_j, \\ k>0, \end{array} \right.$$

consideremos o polinómio

$$F(x)=\prod_{i=1}^{n_o}(x^{p^k}-\beta_i^{p^k})=\prod_{i=1}^{n_o}(x^{p^k}-\alpha_i^{p^t}) \in \mathfrak{R}[x].$$

Vê-se que $F(x)$ é irredutível em $\mathfrak{R}$, pelo facto de se ter $F(x^{p^{t-k}})=\varphi(x)$. Nessas condições, os elementos $\beta_1, \ldots, \beta_{n_o}$ são inseparáveis relativamente a $\mathfrak{R}$. Ora a

equação $r(x)=(x-\beta_1)\ldots(x-\beta_{n_o})=0$, com coeficientes pertencentes a $\mathfrak{M}$, mostra que os elementos β_i são separáveis relativamente a $\mathfrak{R}$, visto que são separáveis relativamente a $\mathfrak{M}$ e esta é ampliação separável de $\mathfrak{R}$ (1).

TEOREMA 11: — *Se a equação* $\varphi(x)=x^{p^t}-\alpha=0$ *é irredutível em* $\mathfrak{R}$, *é irredutível em qualquer ampliação separável,* $\mathfrak{M}$, *daquele corpo.* Supondo $\varphi(x)=(x-\theta)^{p^t}$, não pode, em $\mathfrak{M}$, em virtude do lema, admitir $\varphi(x)$ um factor $f(x)$ com a raiz θ. $f(x)$ será uma constante. E conclui-se deste modo que é $(\mathfrak{M}(\theta)/\mathfrak{M})=(\mathfrak{R}(\theta)/\mathfrak{R})=p^t$.

TEOREMA 12: — *Se for* $\mathfrak{M} \supset \Omega \supset \mathfrak{R}$, *é condição necessária e suficiente, para que* $\mathfrak{M}$ *seja ampliação pura de* $\mathfrak{R}$, *que* Ω *seja ampliação pura de* $\mathfrak{R}$ *e* $\mathfrak{M}$ *ampliação pura de* Ω. É imediato que a condição é necessária. Para se ver que é suficiente, suponhamos que $\alpha \in \mathfrak{M}$ satisfaz a uma equação $x^{p^t}-\omega=0$, irredutível em Ω. Como $\omega \in \Omega$ satisfaz a uma equação $x^{p^s}-k=0$, irredutível em $\mathfrak{R}$, vê-se que α satisfaz à equação de $\mathfrak{R}[x]$, $x^{p^{t+s}}-k=0$. α tem, pois, relativamente a $\mathfrak{R}$, um grau reduzido igual à unidade, como se quer. Podemos precisar, dizendo *o expoente de* α *relativamente a* $\mathfrak{R}$ *é a soma dos expoentes* t *e* s. Se pudesse ser $\alpha^{p^{t+s-j}} \in \mathfrak{R}$, $(j \gtrless 1)$, como é $\alpha^{p^t}=\omega$, ter-se-ia $\omega^{p^{s-j}} \in \mathfrak{R}$, o que é absurdo.

COROLÁRIO 3: — *É condição necessária e suficiente, para que uma ampliação finita* $\mathfrak{L}$, *de* $\mathfrak{R}$, *seja pura, que o único isomorfismo relativo de* $\mathfrak{L}$ *com respeito a* $\mathfrak{R}$ *seja o isomorfismo idêntico* (2). Se $\mathfrak{L}$ é ampliação pura, os graus reduzidos n_i, referidos no teorema dado em nota, são todos iguais à unidade. Inversamente, se os n_i são todos iguais à unidade, pondo $\mathfrak{L}=\mathfrak{R}(\theta_1, \ldots, \theta_r)$, é $\mathfrak{R}(\theta_1)$ ampliação pura de

---

(1) E. STEINITZ, pág. 235 (ou A. C., pág. 203).

(2) Em v. W., pág. 116 (ou A. C., pág. 200), encontra-se demonstrado o seguinte teorema: *Se* $\theta_1, \ldots, \theta_r$ *são elementos algébricos relativamente a* $\mathfrak{R}$, *de tal sorte que* θ_i *seja do grau reduzido* n_i *relativamente a* $\mathfrak{R}(\theta_1, \ldots, \theta_{i-1})$, *é possível construir um corpo* $\Omega \supseteq \mathfrak{L}=\mathfrak{R}(\theta_1, \ldots, \theta_r)$, *no qual* $\mathfrak{L}$ *admite* $T=\prod_{i=1}^{r} n_i$ *isomorfismos relativos com respeito a* $\mathfrak{R}$, *não existindo corpo contendo* $\mathfrak{R}$ *e* $\mathfrak{L}$ *onde haja mais do que esse número de isomorfismos relativos.*

$\mathfrak{R}$; $\mathfrak{R}(\theta_1, \theta_2)$ ampliação pura de $\mathfrak{R}(\theta_1)$, e, portanto, de $\mathfrak{R}$, etc.

TEOREMA 13: — *O grupo* $\mathfrak{g}$, *dos automorfismos de* $\mathfrak{L}$ *com respeito a* $\mathfrak{R}$, *é subgrupo do grupo de automorfismos* $\mathfrak{G}$, *de* $\mathfrak{L}_o$ *com respeito a* $\mathfrak{R}$, *e a ordem dum elemento* $g' \in \mathfrak{g}$ *divide os graus de* $\mathfrak{L}$ *e de* $\mathfrak{L}_o$ *relativamente a* $\mathfrak{R}$.

Seja $g' \in \mathfrak{g}$. Um elemento separável $\alpha \in \mathfrak{L}, \mathfrak{L}_o$ é transformado, por via de g', num elemento de $\mathfrak{L}$, que representaremos por $g'\alpha$. Este, como conjugado de α, é um elemento separável ($g'\alpha \in \mathfrak{L}_o$). É fácil de ver que $g'\mathfrak{L}_o = \mathfrak{L}_o$. Assim, tem-se $g' \in \mathfrak{G}$, $\mathfrak{g} \subseteq \mathfrak{G}$. Como é $\mathfrak{L}_o = \mathfrak{R}(\lambda)$, g' transforma λ num conjugado $g'\lambda$. Pondo $g'^n\lambda = g' . g'^{n-1}\lambda$, suponhamos μ a ordem de g', e, por consequência, $g'^\mu\lambda = \lambda$. Os conjugados $\lambda, g'\lambda, \ldots, g'^{\mu-1}\lambda$ são todos distintos. Se $\mathfrak{L}_1 \supseteq \mathfrak{R}$ é o corpo contido em $\mathfrak{L}_o$ que fica conservado por g', a equação $f(x) = (x-\lambda)(x-g'\lambda)\ldots(x-g'^{\mu-1}\lambda) = o$ tem coeficientes pertencentes a $\mathfrak{L}_1$. Se fosse $\lambda \in \mathfrak{L}_1$, ter-se-ia $\mathfrak{L}_1 = \mathfrak{L}_o$ e o teorema estaria demonstrado. No geral $\lambda \notin \mathfrak{L}_1$, de modo que se tem $\mathfrak{L}_o = \mathfrak{L}_1(\lambda)$. A equação irredutível em $\mathfrak{L}_1$ a que satisfaz λ é precisamente $f(x) = o$, em virtude do seguinte: se ela fosse $\Psi(x) = o$, ter-se-ia $\Psi(\lambda) = \Psi(g'\lambda) = \ldots = o$, pelo que $\Psi(x)$ seria também divisível por $f(x)$. Nestas condições é $(\mathfrak{L}_o/\mathfrak{L}_1) = \mu$, e $(\mathfrak{L}_o/\mathfrak{R}) = \mu\,(\mathfrak{L}_1/\mathfrak{R})$, o que demonstra o teorema (1).

TEOREMA 14: — *Se* $\mathfrak{M}$ *é uma ampliação separável de* $\mathfrak{R}$ *e se* $\mathfrak{L} = \mathfrak{R}\{\alpha_1, \ldots, \alpha_n\}$ *é uma ampliação pura do mesmo corpo,* $\Omega = \mathfrak{M}\{\alpha_1, \ldots, \alpha_n\}$ *é uma ampliação pura de* $\mathfrak{M}$. Os expoentes l_i, dos α_i, relativamente a $\mathfrak{R}$, são também os expoentes dos α_i relativamente a $\mathfrak{M}$. Sabe-se que é $\Omega_o = \mathfrak{M}(\alpha_1^{p^e}, \ldots, \alpha_n^{p^e})$, se e é o expoente de $\mathfrak{L}$ relativamente a $\mathfrak{R}$ (ou de Ω relativamente a $\mathfrak{M}$). Como, porém, $\alpha_i^{p^e} \in \mathfrak{R}$, é $\Omega_o = \mathfrak{M}$, como se quer.

LEMA 2: — *Se* $\mathfrak{M}$ *é uma ampliação separável de* $\mathfrak{R}$, $\Delta = \mathfrak{M}(\beta_1, \ldots, \beta_s)$ *é uma ampliação separável de* $\Omega = \mathfrak{R}(\beta_1, \ldots, \beta_s)$. Tomemos $\alpha \in \Delta$. α é um polinómio nos β_i, com coeficientes pertencentes a $\mathfrak{M}$. Ponhamos $\alpha = \Sigma m_{i_1 \ldots i_s} \beta_1^{i_1} \ldots \beta_s^{i_s}$. Vê-se que α pertence ao corpo $\phi(\beta_1, \ldots, \beta_s)$, onde $\phi = \mathfrak{R}(\ldots, m_{i_1 \ldots i_s}, \ldots)$ resulta de $\mathfrak{R}$ por adjunção das coeficientes que figuram na expressão supra dos α. Como ϕ é uma ampliação simples $\mathfrak{R}(\lambda)$, de $\mathfrak{R}$, tem-se $\alpha \in \mathfrak{R}(\lambda, \beta_1, \ldots, \beta_s) = \Omega(\lambda)$. Por ser λ separável relativamente a $\mathfrak{R}$ e a Ω, o corpo $\Omega(\lambda)$ é uma ampliação separável de Ω. Assim, qualquer elemento α de Δ é separável relativamente a Ω, pelo que Δ é ampliação separável de Ω, como se afirmou.

TEOREMA 15: — *Os corpos* $\mathfrak{L}$ *e* Ω *do teorema 14 verificam a relação* $(\mathfrak{L}/\mathfrak{R}) = (\Omega/\mathfrak{M})$. Ponhamos, com efeito, $\mathfrak{L} = \mathfrak{R}(\beta_1, \ldots, \beta_s)$. Podemos supor $\beta_1, \ldots, \beta_s$ elementos inseparáveis relativamente a $\mathfrak{R}$ e a $\mathfrak{M}$, satisfazendo às mesmas equações irredutíveis nesses corpos: $x^{p^{l_i}} - \gamma_i = 0$, $(i = 1, 2, \ldots, s)$. É claro que se tem $\Omega = \mathfrak{M}(\beta_1, \ldots, \beta_s)$. Ora é $(\mathfrak{R}(\beta_1)/\mathfrak{R}) = (\mathfrak{M}(\beta_1)/\mathfrak{M})$. Fazendo $\mathfrak{R}(\beta_1, \ldots, \beta_i) = \mathfrak{L}_i$, $\mathfrak{M}(\beta_1, \ldots, \beta_i) = \Omega_i$, admitamos que tem lugar a relação $(\mathfrak{L}_{i-1}/\mathfrak{R}) = (\Omega_{i-1}/\mathfrak{M})$. Para se verificar que é também $(\mathfrak{L}_i/\mathfrak{R}) = (\Omega_i/\mathfrak{M})$, raciocina-se como segue. O elemento β_i satisfaz a uma equação irredutível em $\mathfrak{L}_{i-1}$, $x^{p^{\theta_i}} - \delta_i = 0$. Como Ω_{i-1} é ampliação separável de $\mathfrak{L}_{i-1}$, segue-se que a referida equação é irredutível em Ω_{i-1}. O teorema resulta desse facto.

COROLÁRIO 4: — *Pondo ainda, como no teorema 14,* $\mathfrak{L} = \mathfrak{R}\{\alpha_1, \ldots, \alpha_n\}$, $\Omega = \mathfrak{M}\{\alpha_1, \ldots, \alpha_n\}$, *e supondo* $\mathfrak{M}$ *ampliação finita separável de* $\mathfrak{R}$, *tem lugar a igualdade* $\Omega = \mathfrak{M} \times \mathfrak{L}$ (1).

Neste enunciado, bem-entendido, supõe-se $(\mathfrak{L}/\mathfrak{R}) = (\Omega/\mathfrak{M}) = n$. Ω, como álgebra sobre $\mathfrak{R}$, é da ordem $m = n\,(\mathfrak{M}/\mathfrak{R})$. O produto directo $\mathfrak{M} \times \mathfrak{L}$, como álgebra sobre $\mathfrak{R}$, é também da ordem m. O referido produto pode supor-se efectuado, porém, dentro da álgebra Ω (corpo), porque, supondo

$$\mathfrak{M} = \mathfrak{R}(\lambda) = \mathfrak{R}\{u, \lambda, \ldots, \lambda^q\}, \quad (u = \text{elemento um de } \mathfrak{R}),$$

(1) Esta demonstração é tirada de A. A., pág. 35.

(1) A. A., pág. 34.

os elementos $\lambda^i \alpha_j \in \Omega$ são linearmente independentes relativamente a $\mathfrak{R}$, como vamos ver. Duma relação $\sum_{i,j} \lambda^i \alpha_j k_{ij} = 0$, $(k_{ij} \in \mathfrak{R})$, deduz-se

$$\sum_j \alpha_j \left(\sum_i \lambda^i k_{ij}\right) = 0, \qquad \sum_i \lambda^i k_{ij} = 0,$$

pois, como se verificou no teorema anterior, os α_j são independentes em face de $\mathfrak{M}$. Ora a última igualdade escrita dá $k_{ij} = 0$, como se quer.

Seja $\mathfrak{L} = \mathfrak{R}(\lambda)$ uma ampliação separável de $\mathfrak{R}$ e suponhamos $\varphi(x) = 0$ a equação irredutível, de grau r, em $\mathfrak{R}[x]$, a que satisfaz λ. O corpo de decomposição $\mathfrak{M}$, de $\varphi(x)$, é uma ampliação normal separável (1), $\mathfrak{M} = \mathfrak{R}(\alpha_1)$, de $\mathfrak{R}$. Designemos com $\alpha_1, \ldots \alpha_n$ os conjugados de α_1. Se tivermos em conta que é $\mathfrak{R}(\alpha_i) = \mathfrak{R}(\alpha_1)$, podemos afirmar que os isomorfismos relativos de $\mathfrak{M}$ com respeito a $\mathfrak{R}$ são obtidos por qualquer das correspondências

$$\mathfrak{R} \to \mathfrak{R}, \qquad \alpha_i \to \alpha_1, \ldots, \alpha_n.$$

Esta afirmação equivale a dizer que uma correspondência que conserva $\mathfrak{R}$ e muda α_i em α_j é uma correspondência que conserva $\mathfrak{R}$ e muda α_1 em α_k. Admitamos agora ser $\mathfrak{R}(\theta_1)$ um corpo intermédio entre $\mathfrak{R}$ e $\mathfrak{M}$. Se $\varphi_1(x) = 0$ for a equação irredutível em $\mathfrak{R}$ a que satisfaz θ_1, os corpos conjugados $\mathfrak{R}(\theta_1), \mathfrak{R}(\theta_2), \ldots, \mathfrak{R}(\theta_m)$, de $\mathfrak{R}(\theta_1)$, são igualmente intermediários entre $\mathfrak{R}$ e $\mathfrak{M}$. É válido o seguinte.

Teorema 16: — *O número de isomorfismos relativos* $\mathfrak{R} \to \mathfrak{R}$, $\alpha_1 \to \alpha_j$ *que conservam um corpo* $\mathfrak{Q} = \mathfrak{R}(\theta_s)$ *é um divisor do grau* $n = (\mathfrak{M}/\mathfrak{R})$, *precisamente o grau* $q = (\mathfrak{M}/\mathfrak{Q})$ (2). Efectivamente, os isomorfismos em causa são isomorfismos relativos de $\mathfrak{M}$ com respeito a $\mathfrak{Q}$. Eles constituem um subgrupo g, do grupo $\mathfrak{G}$ dos isomorfismos relativos de $\mathfrak{M}$ com respeito a $\mathfrak{R}$. O número de elementos de $\mathfrak{G}$ é n e o dos elementos de g é q, visto que $\mathfrak{M}$ é também ampliação separável de $\mathfrak{Q}$.

(1) V. W., pág. 103 (ou A. C., pág. 184).
(2) E. Steinitz, pág. 236 (ou A. C., pág. 232).

Se for $\mathfrak{Q}'$ um segundo corpo intermédio entre $\mathfrak{R}$ e $\mathfrak{M}$, ao qual corresponda o mesmo grupo g que corresponde a $\mathfrak{Q}$, então $\gamma' \in \mathfrak{Q}'$ é conservado, por hipótese, por todos os isomorfismos de g, os quais conservam $\mathfrak{Q}(\gamma')$. Como o número dos isomorfismos que conservam este último não pode exceder o número de elementos de g, deve ter-se $(\mathfrak{M}/\mathfrak{Q}(\gamma')) = (\mathfrak{M}/\mathfrak{Q})$, e, portanto, $\mathfrak{Q}(\gamma') = \mathfrak{Q}$, $\gamma' \in \mathfrak{Q}$, $\mathfrak{Q}' = \mathfrak{Q}$. Daqui se tira o

Teorema 17: — *Entre* $\mathfrak{R}$ *e* $\mathfrak{M}$ *há um número finito de corpos intermédios.*

E pode enunciar-se o

Teorema 18: — *Entre* $\mathfrak{R}$ *e uma ampliação separável finita* $\mathfrak{L}$ *de* $\mathfrak{R}$, *há um número finito de corpos intermédios.*

A questão dos corpos intermédios é resolvida por esta proposição: *é necessário e basta, para que, entre* $\mathfrak{R}$ *e a sua ampliação* Ω, *haja um número finito de corpos intermédios, que* Ω *seja uma ampliação algébrica simples de* $\mathfrak{R}$ (1).

Teorema 19: — *É condição necessária e suficiente, para que uma ampliação inseparável finita* $\mathfrak{L}$ *de* $\mathfrak{R}$, *seja simples, que se tenha* $(\mathfrak{L}/\mathfrak{L}^{(p)}) = p$.

Já sabemos que a condição é necessária. Para se ver que é suficiente, ponhamos

$$\mathfrak{L} = \mathfrak{R}(a_1, \ldots, a_r), \qquad \mathfrak{L}^{(p)} = \mathfrak{R}(a_1^p, \ldots, a_r^p).$$

Um dos elementos a_i, a_1, por ex., não pertence a $\mathfrak{L}^{(p)}$. Por isso, tem-se

$$\mathfrak{L} = \mathfrak{L}^{(p)}(a_1) = \mathfrak{R}(a_1, a_2^p, \ldots, a_r^p),$$

$$\mathfrak{L}^{(p)} = \mathfrak{R}(a_1^p, \ldots, a_r^{p^2}).$$

Daqui tira-se agora

$$\mathfrak{L} = \mathfrak{R}(a_1, a_2 p^2, \ldots, a_r p^2) = \ldots = \mathfrak{R}(a_1, a_2^{p^e}, \ldots, a_r^{p^e}),$$

(1) E. Steinitz, pág. 244 (ou A. C., pág. 238).

ou seja, se $\mathfrak{L}_o = \mathfrak{R}(\theta)$,

$$\mathfrak{L} = \mathfrak{L}_o(a_1) = \mathfrak{R}(\theta, a_1) = \mathfrak{R}(\mu).$$

Corolário 5: — *A condição* $(\mathfrak{L}/\mathfrak{L}^{(p)}) = p$ *arrasta* $(\mathfrak{L}(p^i)/\mathfrak{L}(p^{i+1})) = p$.

Seja $\mathfrak{L}$ uma ampliação pura de $\mathfrak{R}$. Se o grau de $\mathfrak{L}$ é p, tem-se $\mathfrak{L} \supset \mathfrak{L}^{(p)} = \mathfrak{L}_o = \mathfrak{R}$. $\mathfrak{L}$ é ampliação simples de $\mathfrak{R}$ e não há, efectivamente, corpo intermédio entre um e outro. No caso da ampliação pura $\mathfrak{L}$ ser de grau $p^r (r \geq 1)$, suponhamos $\alpha^p \in \mathfrak{R}$, para cada $\alpha \in \mathfrak{L}$. A cadeia $\mathfrak{L} \supset \mathfrak{L}^{(p)} = \mathfrak{L}_o = \mathfrak{R}$ diz nos que $\mathfrak{L}$ não pode ser ampliação simples de $\mathfrak{R}$. Dum modo preciso, é fácil encontrar r elementos tais que $\mathfrak{L} = \mathfrak{R}(a_1, \ldots, a_r)$, e verificar que um número de elementos inferior a r não pode gerar $\mathfrak{L}$, a partir de $\mathfrak{R}$. Este resultado fixa-se no seguinte

Teorema 20: — *Se* $\mathfrak{L}$ *é ampliação pura de* $\mathfrak{R}$, *de grau* p^r, *e se, para cada* $\alpha \in \mathfrak{L}$, *se tem* $\alpha^p \in \mathfrak{R}$, *o número mínimo de elementos a adjuntar a* $\mathfrak{R}$ *para obter* $\mathfrak{L}$ *é igual a* r.

Neste caso expresso pelo teorema, façamos $\mathfrak{R}(a_1, \ldots, a_s) = \Psi_s$. Se considerarmos a cadeia

$$\mathfrak{L} = \Psi_r \supset \Psi_{r-1} \supset \ldots \supset \Psi_1 \supset \mathfrak{R} = \mathfrak{L}^{(p)},$$

sabemos que não é possível encontrar corpo intermédio entre dois corpos consecutivos. Mas, entre dois não consecutivos, há uma infinidade de corpos intermédios. Tomemos por ex., Ψ_3 e Ψ_1. Sejam $\rho, \rho', \ldots$ elementos de Ψ_1 (em número infinito) e consideremos

$$\beta = \alpha_2 + \rho\alpha_3, \quad \beta = \alpha_2 + \rho'\alpha_3, \ldots.$$

Os corpos $\Psi_1(\beta)$, $\Psi_1(\beta') \ldots$. não estão contidos em Ψ_2, mas estão contidos em Ψ_3. Eles são diferentes, se for $\rho \neq \rho'$. Na verdade, se pudesse ser $\beta' \in \Psi_1(\beta)$, como se tem $\beta' - \beta = (\rho' - \rho)\alpha_3$, ter-se-ia $\alpha_3 \in \Psi_1(\beta)$. Então, α_2 pertenceria a $\Psi_1(\beta)$, seria $\Psi_1(\beta) = \Psi_3$, o que não pode ter lugar, pelo facto de ser $(\Psi_1(\beta)/\Psi_1) = p$. Passando a uma ampliação finita qualquer Ω, de $\mathfrak{R}$, os raciocínios feitos permitem enunciar, de facto, o seguinte

Teorema 21: — *Se a ampliação finita* Ω, *de* $\mathfrak{R}$ *(este suposto com uma infinidade de elementos), não é simples, há entre* $\mathfrak{R}$ *e* Ω *uma infinidade de corpos intermédios.*

Dada a ampliação finita Ω, de $\mathfrak{R}$, consideremos a cadeia

$$\Omega \supset \Omega^{(p)} \supset \ldots \supset \Omega_o \supset \mathfrak{R} \qquad (2)$$

e suponhamos $(\Omega/\Omega^{(p)}) = p^r$. Pondo

$$\Omega = \mathfrak{R}(a_1, \ldots, a_\lambda), \qquad \Omega^{(p)} = \mathfrak{R}(a_1^p, \ldots, a_\lambda^p),$$

concluímos imediatamente que não pode ser $\lambda < r$. Admitindo, pois, que é $\lambda \geq r$, designemos por $a_1, \ldots, a_r$ elementos a_i, em número de r, não pertencentes a $\Omega^{(p)}$, os quais existem certamente. Tem-se

$$\Omega = \Omega^{(p)}(a_1, \ldots, a_r) =$$

$$= \mathfrak{R}(a_1, \ldots, a_r, a_{r+1}^p, \ldots, a_\lambda^p).$$

Como no teorema 19, chega-se a estabelecer

$$\Omega = \mathfrak{R}(a_1, \ldots, a_r, a_{r+1}^{p^e}, \ldots, a_\lambda^{p^e}) = \Omega_o(a_1, \ldots, a_r) =$$

$$= \mathfrak{R}(\theta, a_1, \ldots, a_r) = \mathfrak{R}(b_1, \ldots, b_r).$$

Tem lugar este

Teorema 22: — *Se na cadeia (2) se tiver* $(\Omega/\Omega^{(p)}) = p^r$, Ω *resulta de* $\mathfrak{R}$ *por adjunção de* r *elementos e nunca por menos do que* r *elementos.*

Na cadeia (2), o grau de $\Omega^{(p)}$ relativamente a $\Omega^{(p^2)}$ não pode exceder p^r. Se excedesse, $\Omega^{(p)}$ só poderia resultar de $\mathfrak{R}$ por adjunção de mais do que r elementos e não seria $\Omega^{(p)} = \mathfrak{R}(b_1^p, \ldots, b_r^p)$. Dum modo geral, na referida cadeia, o grau de cada corpo relativamente ao seguinte nunca pode aumentar. Se todos os graus são iguais a p, salvo $(\Omega/\Omega^{(p)}) = p^r$ [bem entendido que $(\Omega_o/\mathfrak{R})$ não está em causa], $\Omega^{(p)}$ é uma ampliação simples de $\mathfrak{R}$, o mesmo podendo dizer-se de $\Omega^{(p)}(b_1)$, se b_1 é de expoente e (um

dos elementos b_i é necessàriamente de expoente e). Efectivamente, tem-se

$$(\Omega^{(p)}(b_1)/\Re) = (\Omega^{(p)}(b_1)/\Omega^{(p)})(\Omega^{(p)}/\Re) = \\ = p \cdot N_o p^{e-1} = N_o p^e .$$

Vamos fazer mais duas observações. Primeiramente, quando Ω, nas condições do teorema 22, resulta de $\Re$ por adjunção dum certo número de elementos $(s \geqq r)$, r dos referidos elementos não pertencem a $\Omega^{(p)}$, e entre os elementos não pertencentes a $\Omega^{(p)}$ há $r-1$ que podem fazer-se figurar nos r elementos que levam de $\Re$ a Ω. A segunda observação vem a seguir. Ponhamos, em (2), $\Omega^{(p^i)} = \Delta$, $\Omega^{(p^k)} = \phi$, $(i<k)$. Considerando $\Delta = \phi(\alpha_1, \ldots, \alpha_t)$ como ampliação finita de ϕ, a cadeia $\Delta \supset \Delta^{(p)} \supset \ldots \supset \Delta_o = \phi$ é precisamente a parte de (2) intermediária entre ϕ e Δ. Na verdade, tendo-se

$$\Delta \supset \Omega^{(p^{i+1})} \geqq \phi \geqq \Re,$$

pode escrever-se

$$\Delta = \Re(x_1, \ldots, x_m) = \phi(x_1, \ldots, x_m),$$

e, em seguida,

$$\Omega^{(p^{i+1})} = \Re(x_1^p, \ldots, x_m^p) = \phi(x_1^p, \ldots, x_m^p) = \Delta^{(p)},$$

como se deseja.

Consideremos a ampliação algébrica $\mathfrak{L} = \Re(\alpha_1, \ldots, \alpha_r)$, de $\Re$, e tomemos um corpo $\mathfrak{M} = \Re(x_1, \ldots, x_t)$, intermediário entre $\Re$ e $\mathfrak{L}$. Pondo

$$\mathfrak{L} = \mathfrak{M}(\beta_1, \ldots, \beta_s) = \Re(x_1, \ldots, x_t, \beta_1, \ldots, \beta_s),$$

tem-se imediatamente

$$\mathfrak{L}^{(p^r)} = \Re(x_1^{p^r}, \ldots, \beta_s^{p^r}) = \mathfrak{M}^{(p^r)}(\beta_1^{p^r}, \ldots, \beta_s^{p^r}),$$

a que podemos dar ainda a forma

$$\mathfrak{M}(\beta_1, \ldots, \beta_s)^{(p^r)} = \mathfrak{M}^{(p^r)}(\beta_1^{p^r}, \ldots, \beta_s^{p^r}).$$

Em particular será

$$\mathfrak{L}^{(p)} = \mathfrak{M}(\beta_1, \ldots, \beta_s)^{(p)} = \mathfrak{M}^{(p)}(\beta_1^p, \ldots, \beta_s^p).$$

Suponhamos $\beta_1, \ldots, \beta_s$ elementos em número mínimo a adjuntar a $\mathfrak{M}$ para obter $\mathfrak{L}$. Se β_1 verifica a equação irredutível em $\mathfrak{M}$,

$$\varphi_1(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0, \quad (2')$$

o elemento β_1^p verifica a equação seguinte, com coeficientes de $\mathfrak{M}^{(p)}$:

$$\phi_1(x) = x^n + a_1^p x^{n-1} + \ldots + a_n^p = 0. \quad (2'')$$

Por isso, será

$$(\mathfrak{M}^{(p)}(\beta_1^p)/\mathfrak{M}^{(p)}) \leqq (\mathfrak{M}(\beta_1)/\mathfrak{M}). \quad (3)$$

Anàlogamente, β_2 satisfaz à equação irredutível em $\mathfrak{M}(\beta_1)$,

$$\varphi_2(x) = x^m + a'_1 x^{m-1} + \ldots + a'_m = 0,$$

e β_2^p à equação

$$\phi_2(x) = x^m + a'^p_1 x^{m-1} + \ldots + a'^p_m = 0.$$

Os coeficientes desta última equação pertencem a $\mathfrak{M}(\beta_1)^{(p)} = \mathfrak{M}^{(p)}(\beta_1^p)$, de sorte que se tem

$$\left(\mathfrak{M}^{(p)}(\beta_1^p, \beta_2^p)/\mathfrak{M}^{(p)}(\beta_1^p)\right) \leqq \\ \leqq \left(\mathfrak{M}(\beta_1, \beta_2)/\mathfrak{M}(\beta_1)\right). \quad (4)$$

Continuando o processo, chega-se por combinação de (3), (4), etc., à relação

$$(\mathfrak{L}^{(p)}/\mathfrak{M}^{(p)}) \leqq (\mathfrak{L}/\mathfrak{M}),$$

e em seguida, das igualdades

$$(\mathfrak{L}/\mathfrak{M}^{(p)}) = (\mathfrak{L}/\mathfrak{M})(\mathfrak{M}/\mathfrak{M}^{(p)}) = \\ = (\mathfrak{L}/\mathfrak{L}^{(p)})(\mathfrak{L}^{(p)}/\mathfrak{M}^{(p)}),$$

tira-se a relação

$$(\mathfrak{M}/\mathfrak{M}^{(p)}) \leqq (\mathfrak{L}/\mathfrak{L}^{(p)}).$$

Podemos enunciar, assim, o seguinte

TEOREMA 23: — *Se* $\mathfrak{L}$ *é uma ampliação algébrica finita de* $\mathfrak{R}$, *que resulta deste pela adjunção dum número mínimo de elementos* $= r$, *um corpo* $\mathfrak{M}$, *intermediário entre* $\mathfrak{R}$ *e* $\mathfrak{L}$, *pode fazer-se resultar de* $\mathfrak{R}$ *pela adjunção dum número de elementos* $\leqq r$.

Tira-se daqui o

COROLÁRIO 6: — *Se* $\mathfrak{L}$ *é uma ampliação algébrica simples de* $\mathfrak{R}$, *um corpo* $\mathfrak{M}$, *intermediário entre* $\mathfrak{R}$ *e* $\mathfrak{L}$, *é também ampliação simples de* $\mathfrak{R}$ (1).

Um caso em que, em (3), vale a igualdade, é aquele em que $\mathfrak{L}$ é ampliação simples de $\mathfrak{R}$. Se for $\mathfrak{L} = \mathfrak{R}(\alpha) \supset \supset \mathfrak{M} \supset \mathfrak{R}$, e $\mathfrak{L} = \mathfrak{M}(\beta)$, a equação $(2'')$, a que satisfaz β^p, é irredutível em $\mathfrak{M}^{(p)}$, tal como $(2')$ é irredutível em $\mathfrak{M}$. Efectivamente, dum modo geral, o elemento β^{p^k} satisfaz à equação

$$\Phi_k(x) = x^n + \alpha_1{}^{p^k} x^{n-1} + \ldots + \alpha_n{}^{p^k} = 0,$$

com coeficientes pertencentes a $\mathfrak{M}^{(p^k)}$. Ora, tendo-se

$$(\mathfrak{L}/\mathfrak{M}^{(p^k)}) = (\mathfrak{L}/\mathfrak{M})\,(\mathfrak{M}/\mathfrak{M}^{(p)}) \ldots (\mathfrak{M}^{(p^{k-1})}/\mathfrak{M}^{(p^k)}) =$$

$$= n.p^k = (\mathfrak{L}/\mathfrak{L}^{(p)}) \ldots (\mathfrak{L}^{(p^{k-1})}/\mathfrak{L}^{(p^k)}).(\mathfrak{L}^{(p^k)}/\mathfrak{M}^{(p^k)}) =$$

$$= p^k \,.\, (\mathfrak{L}^{(p^k)}/\mathfrak{M}^{(p^k)}),$$

conclui-se imediatamente a afirmação supra. Podemos fixar o seguinte

TEOREMA 24: — *Se* $\varphi(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n = 0$ *é uma equação irredutível em* $\mathfrak{M}$, *e se* β *é uma raiz desta equação tal que* $\mathfrak{M}(\beta) = \mathfrak{R}(\alpha)$ *é ampliação simples de* $\mathfrak{R}$, *a equação* $\Phi_k(x) = x^n + \alpha_1{}^{p^k} x^{n-1} + \ldots + \alpha_n{}^{p^k} = 0$ *é irredutível em* $\mathfrak{M}^{(p^k)}$.

(1) E. STEINITZ, pág. 243 (ou A. C., pág. 236).