VỀ ĐIỀU KIỆN ĐẲNG CẤU GIỮA CÁC TRƯỜNG CON CỦA BAO ĐÓNG ĐẠI SỐ $\Gamma(p)$

Cao Minh Nam[(1)]
(1) Phân hiệu tại Thành phố Hồ Chí Minh, Trường Đại học Giao thông vận tải
Ngày nhận bài 17/02/2025; Chấp nhận đăng 14/4/2025
Email liên hệ: namcm@utc.edu.vn

Tóm tắt

Cho N và M là hai số Steinitz. Cho p là một số nguyên tố và $GF(p)$ là một trường có p phần tử. Bao đóng đại số $\Gamma(p)$ là hợp của tất cả các trường $GF(p^{n!})$ với n là số nguyên dương. Theorem 9.8.4 của (Roman, 2005) khẳng định rằng $GF(p^N) = GF(p^M)$ khi và chỉ khi hai số Steinitz N và M bằng nhau. Trong bài báo này, chúng tôi tiếp tục phát triển kết quả trên thông qua việc chỉ ra rằng các trường con khác nhau trong bao đóng đại số $\Gamma(p)$ có cấu trúc trường khác nhau. Cụ thể, chúng tôi chứng minh rằng một đẳng cấu trường giữa $GF(p^N)$ và $GF(p^M)$ tồn tại khi và chỉ khi $N = M$. Kết quả này cung cấp một đặc trưng quan trọng về cấu trúc của các trường con trong $\Gamma(p)$.

Từ khoá: *bao đóng đại số, đẳng cấu trường, mở rộng trường, số Steinitz*

Abstract

ON THE ISOMORPHISM CONDITION AMONG SUBFIELDS OF THE ALGEBRAIC CLOSURE OF Γ(p)

Let N and M be Steinitz numbers. Let p be a prime and $GF(p)$ a field of p elements. The algebraic closure $\Gamma(p)$ is the union of all fields $GF(p^{n!})$ for positive integers n. Theorem 9.8.4 in (Roman, 2005) states that $GF(p^N) = GF(p^M)$ if and only if the two Steinitz numbers N and M are equal. In this paper, we continue to develop the above result by showing that the different subfields within $\Gamma(p)$ have distinct field structures. Specifically, it is proven that a field isomorphism between $GF(p^N)$ and $GF(p^M)$ exists if and only if $N = M$. This result provides an important characterization of the subfield structure within $\Gamma(p)$.

1. Đặt vấn đề

Cho F là một trường và A là một F-đại số với đơn vị 1. Theo (Kurosh, 1947), A là một *đại số ma trận địa phương* nếu với bất kỳ bộ hữu hạn các phần tử $a_1, a_2, \dots, a_s \in A$ nằm trong một đại số con B, $1 \in B \subseteq A$, mà đẳng cấu với một đại số ma trận $M_n(F)$ với $n \geq 1$. Vấn đề tìm hiểu cấu trúc của một số lớp đại số bằng việc tham số hóa chúng bởi tập hợp các số Steinitz đã thu hút được nhiều nhà toán học quan tâm nghiên cứu từ rất lâu. Chẳng hạn như (Glimm, 1960), (Baranov, Zhilinskii, 1999) và (Bezushchak, Oliynyk, Sushchansky, 2016) đã chỉ ra rằng: hai đại số ma trận địa phương có đơn vị với số chiều đếm được đẳng cấu với nhau khi và chỉ khi chúng có cùng số Steinitz tương ứng ((Bezushchak, Oliynyk, 2020); Theorem 1)). Một điều thú vị là tình huống này cũng đúng đối với bao đóng đại số của một trường hữu hạn có p phần tử $GF(p)$ với p là một số nguyên tố. Cụ thể, xét bao đóng đại số:

$$\Gamma(p) = \bigcup_{n\in\mathbb{N}^*} GF(p^{n!})$$

của trường hữu hạn $GF(p)$ và cho N và M là hai số Steinitz, hai trường $GF(p^N)$ và $GF(p^M)$ đẳng cấu khi và chỉ khi $N = M$ (xem Định lý 4.3). Để ý rằng theo Theorem 9.8.4 của (Roman, 2005), mỗi trường con của $\Gamma(p)$ đều có dạng $GF(p^N)$ với N là một số Steinitz nào đó. Hơn nữa, kết quả này cũng phát triển một phần của Định lý 9.8.4 trong (Roman, 2005), ở đó một số cấu trúc về các trường con của $\Gamma(p)$ được chỉ ra. Như vậy, theo kết quả trên, chúng ta thấy được rằng trong lớp các trường con của $\Gamma(p)$, các trường con phân biệt có cấu trúc trường phân biệt. Tuy nhiên, tình huống này không còn đúng đối với lớp các trường con của bao đóng đại số của trường số hữu tỉ $\mathbb{Q}$. Để chỉ ra khẳng định này, chúng ta xét lớp các trường con của *trường các số đại số* $\mathbb{A}$. Nhắc lại rằng $\mathbb{A}$ được xác định bởi

$$\mathbb{A} = \{ u \in \mathbb{C} \mid u \text{ đại số trên } \mathbb{Q} \}.$$

Theo (Nicholson, 2012), Corollary trang 296, $\mathbb{A}$ là một bao đóng đại số của $\mathbb{Q}$. Tiếp theo, nhận thấy rằng đa thức $f(x) = x^4 - 2$ bất khả quy trên $\mathbb{Q}$ và nhận các phần tử $\sqrt[4]{2}$ và $i\sqrt[4]{2}$ làm nghiệm. Ngoài ra, $\mathbb{Q}(\sqrt[4]{2})$ và $\mathbb{Q}(i\sqrt[4]{2})$ là hai trường con phân biệt của $\mathbb{A}$, và hơn nữa chúng cùng đẳng cấu với trường $\mathbb{Q}[x]/\langle x^4 - 2\rangle$ theo (Morandi, 2012), Proposition 1.15).

Nhắc lại rằng một trường E được gọi là *đóng đại số* nếu mọi đa thức khác hằng $f(x) \in E[x]$ đều có ít nhất một nghiệm trong E. *Một bao đóng đại số* của một trường F là một mở rộng đại số của F mà bản thân nó đóng đại số. Mọi trường đều có bao đóng đại số và các bao đóng đại số của một trường là duy nhất sai khác một đẳng cấu (xem (Lang, 2012), Corollary 2.6 trang 232 và Corollary 2.9 trang 234).

Các ký hiệu được sử dụng trong bài báo này là các ký hiệu thông thường. Chẳng hạn, $\mathbb{N}^*$ là tập hợp các số nguyên dương và F là một trường. Hơn nữa, p luôn được quy ước là một số nguyên tố, $GF(p)$ là một trường hữu hạn có p phần tử với bao đóng đại số $\Gamma(p)$.

2. Phương pháp nghiên cứu

Để nghiên cứu cấu trúc của các trường con trong bao đóng đại số $\Gamma(p)$ với p là một số nguyên tố chúng ta sẽ sử dụng các phương pháp sau:

Sử dụng Số Steinitz: đầu tiên, chúng ta sẽ sử dụng các số Steinitz để phân tích cấu trúc của các trường con trong bao đóng đại số $\Gamma(p)$. Các số Steinitz cung cấp một cách tham số hóa hiệu quả cho các đại số ma trận địa phương, giúp chúng ta hiểu rõ hơn về cấu trúc nội tại của các trường con.

Xác định bao đóng đại số: tiếp theo, chúng ta sẽ xác định chính xác bao đóng đại số $\Gamma(p) = \cup_{n\in\mathbb{N}^*} GF(p^{n!})$ của trường hữu hạn $GF(p)$. Việc này đòi hỏi việc hiểu rõ về cấu trúc của các trường hữu hạn và cách chúng được kết hợp lại để tạo thành bao đóng đại số.

Phân tích cấu trúc trường con: sau khi đã xác định bao đóng đại số, chúng ta sẽ tiến hành phân tích cấu trúc của các trường con trong $\Gamma(p)$. Điều này bao gồm việc tìm hiểu mối quan hệ giữa các trường con, cũng như xác định các điều kiện cần và đủ để hai trường con đẳng cấu với nhau.

Bằng cách sử dụng các phương pháp trên, chúng ta hy vọng có thể đạt được những hiểu biết sâu sắc về cấu trúc của các trường con trong bao đóng đại số $\Gamma(p)$.

3. Chuẩn bị

Trong mục này chúng tôi nhắc lại một số khái niệm và kết quả được dùng cho Mục 4. Cụ thể, cho mở rộng trường E/F. Dễ thấy E là một không gian vectơ trên F. Ký hiệu $[E:F]$ được dùng để chỉ số chiều của E trên F, nói cách khác

$$[E:F] = \dim_F E.$$

Nếu $[E:F] = n$, trong đó $n \in \mathbb{N}^*$, thì ta nói E là một *mở rộng bậc* n của F. Mệnh đề dưới đây chỉ ra một cách xác định bậc của một mở rộng hữu hạn của $GF(p)$.

Mệnh đề 3.1. $[GF(p^d): GF(p)] = d$ *với mọi* $d \in \mathbb{N}^*$.

Chứng minh. Xem (Roman, 2005), Theorem 9.6.1).

Cho K và L là hai trường con của một trường E. Ký hiệu KL là trường con nhỏ nhất của E chứa cả K và L. Tiếp theo, cho trước hai số nguyên dương n và m, các ký hiệu $\text{lcm}(n,m)$ và $\gcd(n,m)$ lần lượt chỉ bội chung nhỏ nhất và ước chung lớn nhất của n và m. Gọi F_p là tập hợp tất cả các lớp đẳng cấu của các trường hữu hạn chứa $GF(p)$. Cấu trúc của tập hợp F_p có thể được xác định thông qua tập hợp các số nguyên dương $\mathbb{N}^*$ bằng định lý dưới đây.

Định lý 3.2. *Ánh xạ* $\phi: \mathbb{N}^* \to F_p$ *xác định bởi*

$$\phi(n) = GF(p^n), \forall\, n \in \mathbb{N}^*$$

là một song ánh. Hơn nữa, cho trước $n, m \in \mathbb{N}^*$*, các khẳng định dưới đây là đúng:*

a) $n|m$ *khi và chỉ khi* $GF(p^n) \le GF(p^m)$.

b) $GF(p^n) \cap GF(p^m) = GF\left(p^{gcd(n,m)}\right)$.

c) $GF(p^n)GF(p^m) = GF\left(p^{lcm(n,m)}\right)$.

Chứng minh. Xem ((Roman, 2005), Theorem 9.8.2).

Tóm lại, định lý vừa rồi cho chúng ta thấy rằng ánh xạ ϕ tạo ra một cấu trúc dàn giữa các trường hữu hạn $GF(p^n)$ tương ứng với các số nguyên dương n và các tính chất của dàn này được xác định bởi quan hệ chia hết, bội chung nhỏ nhất và ước chung lớn nhất.

Ở nội dung kế tiếp, chúng tôi trình bày sơ lược về một cách để xác định bao đóng đại số của trường hữu hạn $GF(p)$. Đặt

$$\Gamma(p) := \bigcup_{n=1}^{\infty} GF(p^{n!}).$$

Dễ dàng chứng minh được rằng $\Gamma(p)$ là một trường. Hơn nữa, $\Gamma(p)$ là một bao đóng đại số của $GF(p)$ (xem (Roman, 2005), Theorem 9.8.1). Để mô tả các trường con của $\Gamma(p)$, trong bài báo này, khái niệm về *số siêu tự nhiên* hay *số Steinitz* (xem (Steinitz, 1910) hoặc (Roman, 2005)) sẽ được sử dụng. Cụ thể, gọi $\mathbb{P}$ là tập hợp của tất cả các số nguyên tố. Một tích hình thức vô hạn có dạng

$$\prod_{p\in\mathbb{P}} p^{r_p}, \text{ trong đó các số mũ } r_p \in \mathbb{N} \cup \{\infty\} \text{ với mọi } p \in \mathbb{P},$$

được gọi là một *số Steinitz*. Gọi $\mathbb{SN}$ là tập hợp của tất cả các số Steinitz. Dễ thấy tập hợp các số nguyên dương $\mathbb{N}^*$ là tập con của $\mathbb{SN}$ vì mỗi số nguyên dương đều có dạng của một số Steinitz với hầu hết các thành phần mũ bằng 0 chỉ trừ một số hữu hạn. Cho hai số Steinitz $N = \prod_{p\in\mathbb{P}} p^{r_p}$ và $M = \prod_{p\in\mathbb{P}} p^{k_p}$. Ta nói hai số Steinitz N và M *bằng nhau* khi và chỉ khi $r_p = k_p$ với mọi $p \in \mathbb{P}$. Lúc này, ta ký hiệu $N = M$. Hơn nữa,

$$NM := \prod_{p\in\mathbb{P}} p^{r_p+k_p},$$

trong đó phép cộng số mũ được hiểu theo nghĩa thông thường với quy ước $n + \infty = \infty$ cho mọi $n \in \mathbb{N}$, được gọi là *tích* của N và M. Ngoài ra, nếu $r_p \le k_p$ với mọi $p \in \mathbb{P}$, ta nói N *chia hết* M hay N là *ước* của M, ký hiệu $N|M$, và

$$\frac{M}{N} := \prod_{p\in\mathbb{P}} p^{r_p-k_p}$$

được gọi là *thương* của phép chia M cho N, ở đây phép trừ các số mũ cũng được hiểu theo nghĩa thông thường cùng các quy ước $\infty - \infty = 0$ và $\infty - n = \infty$ với mọi $n \in \mathbb{N}$. Nếu $r_p > k_p$ với một vài $p \in \mathbb{P}$ thì ta nói N *không chia hết* M hay N *không là ước* của M. Dễ thấy, quan hệ chia hết được định nghĩa như trên biến $\mathbb{SN}$ thành một tập hợp được sắp, trong đó $I := \prod_{p\in\mathbb{P}} p^{\infty}$ là phần tử lớn nhất và 1 là phần tử nhỏ nhất.

Bổ đề 3.3. *Cho $N \in \mathbb{SN}$ và cho $a, b \in \mathbb{N}^*$. Nếu a và b đều là ước của N thì bội chung nhỏ nhất $lcm(a, b)$ cũng là ước của N.*

Chứng minh. Đặt $N = \prod_{p\in\mathbb{P}} p^{r_p}$. Không mất tính tổng quát, ta có thể giả sử

$$a = p_1^{n_1}p_2^{n_2}\dots p_k^{n_k} \text{ và } b = p_1^{m_1}p_2^{m_2}\dots p_k^{m_k},$$

trong đó các p_i là các số nguyên tố và các n_i, m_i là các số nguyên không âm. Vì $a|N$ và $b|N$ nên $n_i \le r_{p_i}$ và $m_i \le r_{p_i}$ với mọi $1 \le i \le k$. Từ đây,

$$\max\{n_i, m_i\} \le r_{p_i} \text{ với mọi } 1 \le i \le k.$$

Vì vậy, $\text{lcm}(a, b) = p_1^{\max\{n_1,m_1\}}p_2^{\max\{n_2,m_2\}}\dots p_k^{\max\{n_k,m_k\}}$ là ước của N và ta có điều phải chứng minh.

Cho N là một số Steinitz. Đặt $GF(p^N) = \bigcup_{d|N} GF(p^d)$, trong đó d chạy khắp các ước nguyên dương của N. Mệnh đề dưới đây cho thấy rằng tập hợp $GF(p^N)$ có cấu trúc của một trường.

Mệnh đề 3.4. *Với mọi $N \in \mathbb{SN}$, $GF(p^N)$ là một mở rộng đại số của $GF(p)$.*

Chứng minh. Lấy $a, b \in GF(p^N)$. Khi đó, $a \in GF(p^{d_1})$ với $d_1|N$ và $b \in GF(p^{d_2})$ với $d_2|N$. Gọi d là bội chung nhỏ nhất của $d_1$và d_2. Dễ thấy a và b đều thuộc $GF(p^d)$ theo Định lý 3.2. Hơn nữa, vì d_1 và d_2 là các ước của N nên theo Bổ đề 3.3, d cũng là ước của N. Từ đây, $GF(p^N)$ là trường. Ngoài ra, theo Mệnh đề 3.1, $[GF(p^d): GF(p)] = d < \infty$. Vì mọi mở rộng hữu hạn đều là mở rộng đại số nên phần tử a đại số trên $GF(p)$. Vì vậy, $GF(p^N)$ là mở rộng đại số của $GF(p)$.

Tiếp theo, cho trước hai số Steinitz $N = \prod_{p\in\mathbb{P}} p^{r_p}$ và $M = \prod_{p\in\mathbb{P}} p^{k_p}$. Các số Steinitz

$$\gcd(N, M) := \prod_{p\in\mathbb{P}} p^{\min\{r_p,k_p\}} \text{ và } \text{lcm}(N, M) := \prod_{p\in\mathbb{P}} p^{\max\{r_p,k_p\}}$$

lần lượt được gọi là *ước chung lớn nhất* và *bội chung nhỏ nhất* của N và M. Tập hợp các số Steinitz $\mathbb{SN}$ cũng đóng vai trò tương tự tập hợp các số nguyên dương $\mathbb{N}^*$ trong Định lý 3.2. Cụ thể, tập $\mathbb{SN}$ giúp chúng ta xác định được cấu trúc của tập hợp tất cả các trường con của $\Gamma(p)$. Khẳng định này là nội dung chính của định lý dưới đây.

Định lý 3.5. *Ánh xạ f từ $\mathbb{SN}$ vào tập tất cả các trường con của $\Gamma(p)$ xác định bởi*

$$f(N) = GF(p^N), \forall N \in \mathbb{SN}.$$

Khi đó, f là một song ánh. Hơn nữa, nếu N và M là hai số Steinitz thì các khẳng định sau đây đúng:

a) $GF(p^N)$ *hữu hạn khi và chỉ khi* N *hữu hạn.*
b) $GF(p^N) \leq GF(p^M)$ *khi và chỉ khi* $N|M$.
c) $GF(p^N) \cap GF(p^M) = GF\left(p^{\gcd(N,M)}\right)$.
d) $GF(p^N)\, GF(p^M) = GF\left(p^{\text{lcm }(N,M)}\right)$.

Chứng minh. Xem ((Roman, 2005), Theorem 9.8.4).

Như vậy, theo kết quả trên, ta thấy rằng mỗi trường con của $\Gamma(p)$ đều có dạng $GF(p^M)$ với M là một số Steinitz nào đó.

4. Kết quả chính

Với mỗi số Steinitz N, ta đặt $I(N) = \{d \in \mathbb{N}^* \mid d \text{ là ước của } N\}$. Để đi đến kết quả chính của bài báo, chúng ta sẽ thiết lập một điều kiện cần và đủ để hai trường con của $\Gamma(p)$ bằng nhau dựa vào mối quan hệ giữa tập hợp các ước nguyên dương của các số Steinitz tương ứng.

Bổ đề 4.1. *Cho N và M là hai số Steinitz. Khi đó, $GF(p^N) \leq GF(p^M)$ khi và chỉ khi $I(N) \subseteq I(M)$.*

Chứng minh. Trước tiên, giả sử rằng $GF(p^N) \leq GF(p^M)$. Gọi d là một ước nguyên dương của N. Khi đó, theo Định lý 3.5, $GF(p^d) \leq GF(p^N) \leq GF(p^M)$. Tiếp tục theo Định lý 3.5, ta có khẳng định $d|M$. Điều này có nghĩa là $I(N) \subseteq I(M)$.

Tiếp theo, giả sử rằng $I(N) \subseteq I(M)$. Vì $GF(p^N) = \bigcup_{d|N} GF(p^d)$ với d chạy khắp các ước nguyên dương của số Steinitz N nên $GF(p^N) = \bigcup_{d\in I(N)} GF(p^d)$. Một cách tương tự, ta cũng có khẳng định $GF(p^M) = \bigcup_{\ell\in I(M)} GF\left(p^\ell\right)$. Mặt khác, vì $I(N)$ là tập con của $I(M)$ nên $\bigcup_{d\in I(N)} GF(p^d) \leq \bigcup_{\ell\in I(M)} GF\left(p^\ell\right)$. Từ đây, $GF(p^N)$ nằm trong $GF(p^M)$ và vì vậy ta có điều phải chứng minh.

Hệ quả 4.2 dưới đây được suy ra trực tiếp từ Bổ đề 4.1.

Hệ quả 4.2. *Cho N và M là hai số Steinitz. Khi đó, $GF(p^N) = GF(p^M)$ khi và chi khi $I(N) = I(N)$.*

Chứng minh. Trước tiên, giả sử rằng $GF(p^N) = GF(p^M)$. Khi đó,

$$GF(p^N) \leq GF(p^M) \text{ và } GF(p^N \geq GF(p^M).$$

Theo Bổ đề 4.1, $I(N) \subseteq I(M)$ và $I(N) \supseteq I(M)$. Do đó, $I(N) = I(M)$. Tiếp theo, giả sử rằng $I(N) = I(M)$. Từ đây, $I(N) \subseteq I(M)$ và $I(N) \supseteq I(M)$. Tiếp tục áp dụng Bổ đề 4.1, ta thu được $GF(p^N) = GF(p^M)$ như mong muốn.

Cuối cùng, ta đi đến kết quả chính của bài báo.

Định lý 4.3. *Cho N và M là hai số Steinitz. Cho p là một số nguyên tố. Nếu tồn tại đẳng cấu trường từ $GF(p^N)$ vào $GF(p^M)$ thì $N = M$.*

Chứng minh. Trước tiên, ta có nhận xét rằng cả $GF(p^N)$ và $GF(p^M)$ đều chứa trường $GF(p)$. Giả sử φ là một đẳng cấu trường từ $GF(p^N)$ vào $GF(p^M)$. Vì $\varphi(1) = 1$ nên $\varphi(a) = a$ với mọi $a \in GF(p)$. Do đó, φ cũng là một đồng cấu $GF(p)$-tuyến tính. Tiếp theo, lấy d là một ước thuần nguyên dương của N. Khi đó, dễ thấy rằng $\varphi\left(GF(p^d)\right)$ là một trường con của $GF(p^M)$. Theo Định lý 3.5, $\varphi\left(GF(p^d)\right) = GF(p^S)$ với S là một số Steinitz nào đó thỏa mãn S là ước của M. Hơn nữa, vì $[GF(p^d): GF(p)] = d$ nên với $\{u_1, u_2, \dots, u_d\}$ là một cơ sở của $GF(p^d)$ trên $GF(p)$, tập hợp $\{\varphi(u_1), \varphi(u_2), \dots, \varphi\ (u_d)\}$ là một cơ sở của $GF(p^S)$ trên $GF(p)$. Do đó, $[GF(p^S): GF(p)] = d < \infty$. Nhận thấy rằng $GF(p^S)$ hữu hạn vì $GF(p)$ hữu hạn. Theo Định lý 3.5, S hữu hạn và do đó $[GF(p^S): GF(p)] = S$ theo Mệnh đề 3.1. Vì vậy, $S = d$ và theo Định lý 3.5, $d|M$. Điều này có nghĩa là số nguyên $d \in I(M)$ và từ đây $I(N) \subseteq I(M)$. Chứng minh tương tự, ta cũng thu được $I(M) \subseteq I(N)$. Theo Hệ quả 4.2, $GF(p^N) = GF(p^M)$ và theo Định lý 3.5 ta kết luận được $N = M$.

5. Kết luận

Cấu trúc của lớp các trường con của bao đóng đại số $\Gamma(p)$ với p là một số nguyên tố có thể được phân tích thông qua việc sử dụng các số Steinitz. Kết quả nghiên cứu cho thấy rằng mỗi số Steiniz tương ứng với duy nhất một cấu trúc trường con trong $\Gamma(p)$.

TÀI LIỆU THAM KHẢO

[1] Baranov, A. A., Zhilinskii, A. G. (1999). Diagonal direct limits of simple lie algebras. *Communications in Algebra*, 2749-2766.

[2] Glimm, J. G. (1960). On a Certain Class of Operator Algebras. *Transactions of the American Mathematical Society*, 318-340.

[3] Kurosh, A. (1947). Direct decompositions of simple rings. *Recueil Mathématique (Nouvelle série)*, 245-264.

[4] Lang, S. (2012). *Algebra.* Springer Science & Business Media.

[5] Morandi, P. (2012). *Field and Galois theory.* Springer Science & Business Media.

[6] Nicholson, W. K. (2012). *Introduction to abstract algebra.* John Wiley & Sons.

[7] Bezushchak, O., Oliynyk, B. (2020). Unital locally matrix algebras and Steinitz numbers. *Journal of Algebra and Its Applications*.

[8] Bezushchak, O., Oliynyk B., Sushchansky, V. (2016). Representation of Steinitz's lattice in lattices of substructures of relational structures. *Algebra and Discrete Mathematics*, 184-201.

[9] Roman, S. (2005). *Field Theory.* Springer Science & Business Media.

[10] Steinitz, E. (1910). Algebraische Theorie der Korper. *J. reine angew. Math., 137*, 167-309.