Chương 5

TRƯỜNG VÀ ĐA THỨC

§1. Định nghĩa.

Một trong những khái niệm cơ bản của đạI số và số học là các trường hữu hạn, Trong chương này, Chúng tôi sẽ trình bày những kiến thức cơ bản nhất về các trường hữu hạn, cần thiết khi tìm hiểu những ứng dụng mới của số học. Ngoài ra, chúng tôi cố gắng minh hoạ một trong những "động lực" của sự phát triển số học hiện đại: sự tương tự giữa số và đa thức. Một vài kết quả gần đây về sự tương tự đó sẽ được đề cập tới.

Để tiện lợi cho bạn đọc khi sử dụng, chúng tôi nhắc lại ở đây những khái niệm cần thiết.

Trường là một tập hợp K có quá một phần tử, được trang bị hai phép tính cộng và nhân thoả mãn các quy tắc sau đây (các chữ cái la tinh chỉ các phần tử tuỳ ý của trường)

1. (tính chất giao hoán của phép cộng): $a+b=b+a$
2. (tính chất kết hợp của phép cộng): $a+(b+c)=(a+b)+c$
3. (tồn tại phần tử 0): Tồn tại $0 \in K$ sao cho $0+a=a+0=a$
4. (tồn tại $-a$): Tồn tại $-a \in K$ sao cho $a+(-a)=0$
5. (tính chất giao hoán của phép nhân): $ab=ba$
6. (tính chất kết hợp của phép nhân): $a(bc)=(ab)c$
7. (tồn tại đơn vị): Tồn tại $1 \in K$ sao cho $1a=a$
8. (tồn tại a^{-1}): Tồn tại $a^{-1} \in K$ sao cho $aa^{-1}=1$
9. (luật phân bố của phép nhân đối với phép cộng): $a(b+c)=ab+ac$

Những ví dụ thường gặp nhất là: trường Q các số hữu tỷ, trường R các số thực, trường C các số phức. Các trường đó đều có vô hạn phần tử.

Trong nhiều vấn đề lí thuyết cũng như ứng dụng, ta thường làm việc với các trường chỉ có hữu hạn phần tử. Chẳng hạn, có thể thấy rằng, các thặng dư không âm bé nhất modulo p, lập thành một trường có p phần tử. Sau đây, ta sẽ thấy rằng, đó chính là trường cơ bản để xây dựng nên tất cả các trường hữu hạn.

Giả sử p là số nguyên tố. Kí hiệu qua F_p trường có p phần tử. Rõ ràng khi cộng p lần phần tử 1 của trường, ta được 0. Do đó, $pa=0$ với mọi phần tử $a \in F_p$. Với một trường

K tuỳ ý, số p không âm bé nhất sao cho $p1=0$ được gọi là *đặc trưng* của trường K. Chẳng hạn, Q, R, C là các trường có đặc trưng 0, F_p là trường có đặc trưng bằng p. Dễ thấy rằng, mọi trường hữu hạn đều có đặc trưng khác không, và đặc trưng của nó là một số nguyên tố.

§2. Mở rộng trường.

Giả sử $k \subset K$ là các trường, đồng thời các phép cộng và nhân trong k chính là cảm sinh bởi các phép tính tương ứng trong K. Khi đó, K được gọi là *mở rộng* của trường k.

Ví dụ. C là mở rộng của R, R là mở rộng của Q.

Nếu tồn tại các phần tử $\alpha_1, \alpha_2,..., \alpha_n \in K$ sao cho mọi phần tử của $a \in K$ đều có thể biểu diễn dưới dạng

$$a=k_1\alpha_1+k_2\alpha_2+...+k_n\alpha_n$$

trong đó $k_1,k_2,...,k_n$ là các phần tử của trường k, thì K được gọi là *mở rộng hữu hạn* của k. Trong trường hợp này, K là một *không gian vectơ hữu hạn chiều trên k*. Ta nói K là *mở rộng hữu hạn của k sinh bởi* $\alpha_1, \alpha_2,..., \alpha_n$.

Ví dụ. C là mở rộng của trường R, sinh bởi phần tử i, nói cách khác, sinh bởi nghiệm cuả phương trình $x^2+1=0$.

Ta nói C là *trường nâng của R bởi đa thức* $P(x)=x^2+1$. Sau đây, ta sẽ thấy rằng, mọi mở rộng hữu hạn của các trường đều được thực hiện bằng cách tương tự như trên.

Định nghĩa 5.1. Giả sử K là một mở rộng của k. Phần tử $a \in K$ được gọi là *đại số* trên trường k nếu nó là nghiệm của một đa thức với hệ số trên trường k.

Nếu thêm điều kiện hệ số của luỹ thừa cao nhất bằng 1 thì đa thức xác định duy nhất đối với mỗi phần tử đại số trên k. K được gọi là *trường nâng* của k bởi đa thức $P(x)$ nếu nó là mở rộng của k bởi các nghiệm của đa thức $P(x)$.

Đối với các đa thức, ta cũng có các tính chất hoàn toàn tương tự như đối với các số nguyên.

Đối với một trường k tuỳ ý, ta kí hiệu qua $k[x]$ vành các đa thức với hệ số trong k. Đa thức P được gọi là *chia hết* cho đa thức Q nếu tồn tại đa thức R sao cho $P=QR$. Một đa thức không chia hết cho đa thức nào bậc nhỏ hơn, khác hằng số được gọi là *đa thức bất khả quy*. Hai đa thức không có ước chung nào khác hằng được gọi là *nguyên tố cùng nhau*. Một đa thức trong $k[x]$ luôn luôn phân tích được thành tích của các đa thức bất khả quy. Phân tích đó là duy nhất, nếu đòi hỏi các đa thức ban đầu cũng như đa thức trong khai triển đều có hệ số của luỹ thừa cao nhất bằng 1.

Đối với mỗi đa thức $P(x)$ trên trường k, bao giờ cũng tồn tại một trường K mở rộng của k sao cho $P(x)$ phân tích được thành các đa thức bậc nhất trên K. Như vậy, nếu hệ số của luỹ thừa cao nhất trong $P(x)$ là 1 thì $P(x)$ được phân tích dưới dạng:

$$P(x)=(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n), \quad \text{với } \alpha_i \in K,\ i=1,...,n.$$

Nếu đối với đa thức hệ số trong k, phân tích trên đây có được với $\alpha_i \in k$, trường k được gọi là *đóng đại số*. Nói cách khác, trường đóng đại số là trường chứa mọi nghiệm của các đa thức với hệ số trong trường đó. Như vậy, trong trường đóng đại số, các đa thức bất khả quy chỉ có thể là đa thức bậc nhất. Chẳng hạn trường số phức C là trường đóng đại số, trường các số thực R không đóng đại số. Thương của hai đa thức với hệ số trong k được gọi là *hàm hữu tỷ* trên k.

§3. Trường hữu hạn.

Như đã nói, trường gồm hữu hạn phần tử có đặc trưng khác không, và đặc trưng đó là một số nguyên tố p.

Giả sử F_q là một trường hữu hạn gồm q phần tử, đặc trưng p. Vì F_q chứa phần tử 1 nên nó sẽ chứa trường F_p như một trường con. Do F_q là trường hữu hạn nên nó là mở rộng hữu hạn của F_p, nghĩa là một không gian vectơ r chiều trên F_p. Từ đó suy ra rằng F_q gồm p^r phần tử, tức là $q=p^r$.

Ngược lại, ta sẽ chứng tỏ rằng, với p, r cho trước (p là số nguyên tố và r là số nguyên dương), tồn tại trường với p^r phần tử. Hơn nữa, các trường hữu hạn với số phần tử như nhau sẽ đẳng cấu với nhau, nghĩa là có tương ứng 1-1 giữa chúng, và tương ứng này bảo toàn các phép tính cộng và nhân, phần tử 0 và phần tử nghịch đảo của trường.

Ta có định lí sau.

Định lí 5.2. *Giả sử F_q là trường hữu hạn với $q=p^r$ phần tử. Khi đó, mọi phần tử của F_q đều thoả mãn phương trình*

$$X^q-X=0,$$

và F_q chính là tập hợp các nghiệm của phương trình đó. Ngược lại, trường nâng của F_p bởi đa thức X^q-X là trường hữu hạn có q phần tử.

Chứng minh định lí này hoàn toàn tương tự như chứng minh định lí 3.27 Chương 3, và được dành cho độc giả .

Giả sử F_q là trường có q phần tử. Ta kí hiệu qua F_q^* tập hợp các phần tử khác không của trường F_q. Khi đó, mọi phần tử của F_q^* đều có nghịch đảo, và F_q^* lập thành một nhóm Aben. Vì F_q^* có hữu hạn phần tử, nên đối với một phần tử tuỳ ý $a \in F_q^*$, tồn tại số nguyên không âm k sao cho $a^k=1$. Số k bé nhất thoả mãn tính chất đó được gọi là bậc của phần tử a.

Đối với mọi phần tử a tuỳ ý, bậc của a luôn là một ước của $q-1$. Chứng minh điều này cũng hoàn toàn tương tự như khi chứng minh bậc của một số modulo n là ước của $\phi(n)$ (xem hệ quả 3.20 Chương 3).

Giả sử g là một phần tử của F_q^*, và bậc của g đúng bằng $q-1$. Khi đó, tập hợp $\{g,g^2,...,g^{q-1}\}$ chính là tất cả các phần tử của F_q^*. Ta nói g là phần tử sinh của nhóm F_q^*.

Định lí sau đây là một tương tự của định lí 3.26 trong chương 3.

Định lí 5.3. *Mọi trường hữu hạn đều có phần tử sinh. Nếu g là một phần tử sinh của F_q^* thì g^s là phần tử sinh của F_q^* khi và chỉ khi $(s,q-1)=1$. Như vậy, tồn tại tất cả $\phi(q-1)$ phần tử sinh của F_q^*.*

Bây giờ ta sẽ mô tả cụ thể cách xây dựng trường F_q từ trường F_p.

Để dễ hình dung, trước tiên ta xét việc xây dựng trường số phức C như là một trường nâng của số thực R bởi đa thức $P(x)=x^2+1$. Như ta đã biết, có thể xem mỗi số phức như một cặp số thực (a,b), và do đó, có thể đồng nhất mỗi số phức với một đa thức $ax+b$ hệ số thực. Với cách tương ứng như vậy, khi nhân hai số phức (biểu diễn bởi hai đa thức), ta chỉ việc nhân theo quy tắc nhân các đa thức, và thay x^2 bởi (-1). Nói cách khác, tập hợp các số phức chính là tập hợp các đa thức với hệ số thực, trong đó hai đa thức được đồng nhất khi và chỉ khi hiệu của chúng bằng đa thức $P(x)=x^2+1$. Ta viết $C=R[x]/P(x)$.

Trường F_q, $q=p^r$, được xây dựng từ trường F_p theo cách hoàn toàn tương tự. Ta xuất phát từ một đa thức bất khả quy $P(x)$ bậc r với hệ số trong F_p, trong đó hệ số của x^r bằng 1. Khi đó ta có:

$$F_q=F_p[x]/P(x).$$

Như vậy, các phần tử của F_q là các đa thức với hệ số trong F_p, bậc bé hơn r (vì giả sử $P(x)=x^r+a_{r-1}x^{r-1}+...+a_0$, khi đó x^r sẽ được thay bởi $-(a_{r-1}x^{r-1}+...+a_0)$).

Ta có thể xuất phát từ đa thức bất khả quy tuỳ ý. Các trường nhận được có số phần tử như nhau , và đẳng cấu với nhau.

Ta minh hoạ những điều nói trên qua ví dụ cụ thể.

Ví dụ. Xây dựng trường F_{16} từ trường F_2 bởi đa thức

$$P(x)=x^4+x^3+x^2+x+1.$$

Đa thức đang xét là một đa thức bất khả quy trên trường F_2. Thật vậy, nếu nó có ước khác hằng số thì phải có ước là đa thức bậc 1 hoặc bậc 2. Nếu ước là đa thức bậc 1, $P(x)$ có nghiệm trong F_2: điều này không xảy ra vì $P(0)=P(1)=1$. Có bốn đa thức bậc 2 trên F_2 đó là các đa thức x^2, x^2+1, x^2+x, x^2+x+1. Thử trực tiếp cho thấy rằng không có cặp đa thức nào có tích bằng $P(x)$.

Các phần tử của F_{16} là các đa thức bậc bé hơn hoặc bằng 3, với hệ số 0 hoặc 1:

-Bậc 0: $0,1$.

-Bậc 1: $x, x+1$.

-Bậc 2: $x^2, x^2+1, x^2+x, x^2+x+1$.

-Bậc 3: $x^3, x^3+1, x^3+x, x^3+x^2, x^3+x+1, x^3+x_2+x+1, x_3+x^2+x, x^3+x^2+x+1$.

Quy tắc cộng và nhân là quy tắc cộng và nhân thông thường của các đa thức, với chú ý $1+1=0$ và $x^4=-(x^3+x^2+x+1)$.

Trong nhiều ứng dụng, chẳng hạn trong lí thuyết thông tin, người ta thường viết các phần tử của trường F_q theo các hệ số của chúng. Như trong ví dụ trên đây, các phần tử của trường sẽ là: 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1100, 1001, 1101, 1110, 1111, cùng với một bảng để cho quy tắc cộng và nhân của chúng. Chú ý rằng, các quy tắc này khác với các quy tắc số học đồng dư modulo q.

Khi biết một phần tử sinh của trường F_q, ta có thể tìm các phần tử khác bằng cách nâng lên luỹ thừa. Sau đây, ta sẽ tìm hiểu một thuật toán thời gian đa thức để làm việc đó. Thuật toán này sẽ được áp dụng trong những chương sau.

Trước khi đi vào mô tả thuật toán, để dễ hình dung, ta xét ví dụ sau đây. Giả sử ta cần tính $(1994)^{23}(\text{mod } 4611)$. Nếu dùng cách thông thường (tính lần lượt các luỹ thừa của 1994), ta phải làm 22 phép nhân và 22 phép chia. Để giảm bớt số phép tính phải làm, ta dùng phương pháp bình phương liên tiếp như sau. Ta có:

$$(1994)^{23}=(1994)^{16+4+2+1}$$

Như vậy, ta chỉ cần tính modulo của các luỹ thừa 1,2,4,8,16 của 1994. Nói cách khác, ta chỉ cần làm phép bình phương liên tiếp 4 lần, sau đó nhân các kết quả ở những luỹ thừa nào tương ứng với số 1 trong biểu diễn số 23 dưới dạng cơ số 2. Ta có $23=(10111)_2$, nên ta nhân kết quả của những luỹ thừa 16,4,2,1.

Cách làm như trên áp dụng được cho mọi nhóm nhân. Giả sử $g \in G$ là phần tử của nhóm nhân G nào đó, ta cần tính g^n, với n là số tự nhiên. Ta viết n dưới dạng cơ số 2: $n=\sum \varepsilon_i 2^i$, trong đó $\varepsilon = \pm 1$. Khi đó ta tính

$$g^n=\prod_{\varepsilon_i=1}(g^i).$$

Thuật toán.

S1. (Xuất phát) đặt $y \leftarrow 1$. Nếu $n=0$, thuật toán kết thúc. Nếu ngược lại, đặt $N \leftarrow n$, $z \leftarrow g$.

S2. (Nhân). Nếu N lẻ, đặt $y \leftarrow z.y$.

S3. (Chia đôi N). Đặt $N \leftarrow [N/2]$. Nếu $N=0$, in ra y và kết thúc thuật toán. Ngược lại, đặt $z \leftarrow z.z$ và quay về S2.

Có thể chứng minh tính đúng đắn của thuật toán với nhận xét rằng, từ bước thứ hai trở đi, ta luôn luôn có $g^n=y.z^N$.

Ta sẽ đánh giá độ phức tạp của thuật toán nói trên.

Số phép nhân phải làm bằng số chữ số của n, cộng thêm số chữ số 1 trong cách viết nhị phân của n, và trừ đi 1. Như vậy, số phép nhân không vượt quá $2[\log n]+1$, tức là $O(\log n)$. Nếu ta tính trong lớp đồng dư modulo m nào đó, mỗi phép nhân đòi hỏi $O(\log^2 m)$ phép tính bit, và toàn bộ số phép tính bit cần thiết sẽ là $O(\log n \log^2 m)$.

Như ta đã thấy ở trên, để thực hiện các phép tính trên trường F_q, ta phải làm các phép tính đối với các đa thức. Sau đây là vài thuật toán để thực hiện các phép tính đó.

Thuật toán chia

Xét các đa thức với hệ số trong trường K tuỳ ý. Với mỗi đa thức P, kí hiệu qua $l(P)$ hệ số của luỹ thừa cao nhất. Ta có thuật toán để, với đa thức đã cho A, B, $B \neq 0$, tìm các đa thức Q, R sao cho $A=BQ+R$, và $\deg R<\deg B$:

C1. (Xuất phát). Đặt $R \leftarrow A$, $Q \leftarrow 0$.

C2. (Kết thúc?). Nếu $\deg R<\deg B$, kết thúc thuật toán.

C3.(Tìm hệ số). Đặt $S \leftarrow \frac{l(R)}{l(B)} x^{\deg R-\deg B}$. Sau đó, đặt $Q \leftarrow Q+S$, $R \leftarrow R-S.B$, và chuyển sang bước C2.

Ta cần lưu ý ngay một điều. Về mặt lí thuyết, sau bước S3, bậc của R phải giảm (vì hệ số của $x^{\deg R}$ sẽ bằng 0 do định nghĩa của S). Tuy nhiên, khi làm việc trên máy, thực tế là ta chỉ có các số gần đúng, nên có thể xảy ra trường hợp hệ số của $x^{\deg R}$ tuy rất nhỏ, nhưng khác không, nghĩa là bậc không giảm, và do đó không bảo đảm là thuật toán kết thúc! Vì thế, khi viết chương trình, nhất thiết phải để hệ số đó bằng 0 sau phép tính $R \leftarrow R-S.B$.

Để tìm ước chung lớn nhất của các đa thức, ta có thuật toán Euclid sau đây.

Thuật toán

Cho các đa thức A,B, tìm ƯCLN của A,B.

EP1. (Kết thúc?) Nếu $B=0$, in ra A và kết thúc thuật toán.

EP2. (Bước Euclid). Giả sử $A=BQ+R$, với $\deg R<\deg B$ (tính bằng thuật toán C trình bày ở trên). Đặt $A \leftarrow B$, $B \leftarrow R$, và quay về bước EP1.

Định lí 5.4. *Có thể nhân hoặc chia hai phần tử của trường F_q với $O(\log^3 q)$ phép tính bit. Nếu k là số nguyên dương thì một phần tử của F_q có thể nâng lên luỹ thừa k với $O(\log k \log^3 q)$ phép tính bit.*

Chứng minh. Giả sử F_q được xây dựng bằng cách nâng trường F_p bởi đa thức bất khả quy $P(x)$ bậc r. Khi đó, các phần tử của trường F_q chính là các đa thức với hệ số trong trường F_p modulo đa thức $P(x)$. Để nhân hai phần tử của trường F_q, ta phải nhân hai đa thức như vậy. Để làm việc đó, ta phải thực hiện $O(r^2)$ phép nhân modulo p (vì các đa thức có bậc nhỏ hơn r), cùng với một số phép tính cộng. Các phép này đòi hỏi thời gian ít hơn. Sau khi có kết quả của phép nhân, ta lại phải tính "modulo đa thức P(x)", nghĩa là làm phép chia cho đa thức $P(x)$ để biết được phần dư. Phép chia đa thức này đòi hỏi $O(r)$ phép chia các số nguyên modulo p và $O(r^2)$ phép nhân các số nguyên modulo p Như ta đã biết, mỗi phép nhân số nguyên modulo p có thể thực hiện bằng $O(\log^2 p)$ phép tính bit , còn mỗi phép chia modulo p có thể làm (chẳng hạn, dùng thuật toán Euclid) với $O(\log^3 p)$ phép tính bit. Như vậy, toàn bộ số

phép tính bit được thực hiện khi nhân hai phần tử của trường F_q là: $O(r^2\log^2 p+r\log^3 p)=O((r\log p)^3)=O(\log^3 q)$. Khẳng định của định lí được chứng minh đối với phép nhân.

Xét phép chia các phần tử của F_q. Để chứng minh rằng có thể hiện phép chia sau $O(\log^3 q)$ phép tính bit, ta chỉ cần chứng tỏ rằng, nghịch đảo của một phần tử tìm được bởi $O(\log^3 q)$ phép tính bit, rồi áp dụng kết quả đã chứng minh đối với phép nhân.

Giả sử ta cần tìm nghịch đảo của phần tử $Q \in F_q$ (là một đa thức bậc nhỏ hơn r, hệ số trong F_p). Dùng thuật chia Euclid cho các đa thức trên trường F_q, ta cần biểu diễn 1 như là tổ hợp tuyến tính của đa thức $P(x)$ và $Q(x)$. Điều này làm được bởi $O(r)$ phép chia các đa thức bậc nhỏ hơn r. Mỗi phép chia như vậy cần $O(r^2\log^2 p+r\log^3 p)=O(r^2\log^3 p)$ phép tính bit. Như vậy, ta cần tất cả là $O(r^3\log^3 p)=O(\log^3 q)$ phép tính bit, điều phải chứng minh.

Còn phải xét phép tính nâng lên luỹ thừa bậc k. Ta có thể dùng phương pháp bình phương liên tiếp, và như vậy, số phép nhân và bình phương cần thực hiện là $O(\log k)$. Số phép tính bit cần thiết trong trường hợp này là $O(\log k\log^3 q)$. Định lí được chứng minh.

§4. Sự tương tự giữa số nguyên và đa thức.

Sự phát triển của số học, đặc biệt là trong những thập kỉ gần đây, chịu ảnh hưởng rất lớn của sự tương tự giữa số nguyên và đa thức. Nói cách khác, khi có giả thuyết nào đó chưa chứng minh được đối với các số nguyên, người ta cố gắng chứng minh sự kiện tương tự cho các đa thức. Điều đó thường dễ làm hơn, có lẽ nguyên nhân chủ yếu là vì, đối với các đa thức, ta có phép tính đạo hàm, trong khi một khái niệm tương tự chưa có đối với các số nguyên.

Trong tiết này, chúng tôi cố gắng thông qua một vài ví dụ đơn giản, minh họa vai trò quan trọng của sự tương tự nói trên trong các nghiên cứu về số học.

Trước hết, chúng ta thấy rõ, giữa tập hợp các số nguyên và tập hợp các đa thức có những tính chất rất giống nhau sau đây:

1) Các qui tắc cộng, trừ, nhân, chia hoàn toàn như nhau cho cả hai tập hợp.

2) Nếu đối với các số nguyên, ta có các số nguyên tố, thì với các đa thức, ta có các đa thức bất khả quy.

3) Đối với hai số nguyên, cũng như đối với hai đa thức, có thể định nghĩa ước chung lớn nhất. Hơn nữa, trong cả hai trường hợp, ước chung lớn nhất này tìm được bằng thuật toán Euclid.

4) Mỗi số nguyên có phân tích thành các thừa số nguyên tố, mỗi đa thức có phân tích thành các đa thức bất khả quy.

5) Các số hữu tỷ tương ứng với các hàm hữu tỷ.

Chúng tôi dành cho độc giả việc kéo dài bảng danh sách này. Ở đây, chúng tôi sẽ đi vào một vài tương tự khó nhìn thấy hơn.

Ta để ý đến sự tương tự giữa phân tích ra thừa số nguyên tố và phân tích bất khả quy. Nếu giả thiết rằng trường k là đóng đại số, thì mỗi đa thức $Q(x) \in k[x]$ có thể phân tích được dưới dạng sau:

$$Q(x)= P_1^{a_1} P_2^{a_2} \dots P_n^{a_n},$$

trong đó $P_i(x)=(x-\alpha i)$, $\alpha i \in k$.

Như vậy, có thể thấy rằng, trong sự tương tự giữa phân tích bất khả quy và phân tích ra thừa số nguyên tố *các nghiệm của đa thức tương ứng với các ước nguyên tố của số nguyên*. Do đó, số các nghiệm phân biệt của một đa thức có vai trò tương tự như số các ước nguyên tố của một số nguyên. Từ nhận xét đó, ta đi đến định nghĩa sau đây.

Định nghĩa 5.5. Cho a là một số nguyên. Ta định nghĩa *căn của a*, kí hiệu qua $N_0(a)$, là tích các ước nguyên tố của a:

$$N_0(a)=\prod_{p|a} p.$$

Ta sẽ thấy rằng, sự tương tự trên đây cùng với các tính chất của đa thức gợi mở một con đường nhiều hy vọng để đi đến chứng minh định lí Fermat.

Năm 1983, R. C. Mason chứng minh định lí rất đẹp sau đây về các đa thức.

Định lí 5.6. *Giả sử a(t), b(t), c(t) là các đa thức với hệ số phức, nguyên tố cùng nhau từng cặp và thoả mãn hệ thức*

$$a(t)+ b(t)= c(t)$$

Khi đó, nếu kí hiệu qua $n_0(f)$ số nghiệm phân biệt của một đa thức f, thì ta có

$$max\{ deg\ a, deg\ b, deg\ c\} \le n_0(abc)-1.$$

Trước khi đi vào chứng minh định lí, ta chứng minh hệ quả sau đây của định lí Mason.

Hệ quả 5.7. *Không tồn tại các đa thức a, b, c, khác hằng số, nguyên tố cùng nhau, thoả mãn phương trình*

$$a^n + b^n = c^n$$

với $n \ge 3$.

Chứng minh. Gỉa sử các đa thức a, b, c thoả mãn phương trình nói trên. Rõ ràng số nghiệm phân biệt của đa thức $a^n b^n c^n$ không vượt quá $deg\ a + deg\ b + deg\ c$. Áp dụng định lí Mason ta có

$$n\ deg\ a \le deg\ a + deg\ b + deg\ c - 1$$

Viết đẳng thức trên với b, c, rồi cộng từng vế ba bất đẳng thức ta được :

$$n(deg\ a + deg\ b + deg\ c) \le 3\ (deg\ a + deg\ b + deg\ c) - 3$$

Ta có mâu thuẫn nếu $n \geq 3$.

Như vậy, định lí Mason cho ta một chứng minh đơn giản của định lí Fermat cho các đa thức. Sau đây, ta chứng minh định lí Mason.

Chứng minh định lí Mason. Đặt $f = a/b$, $g = a/c$, ta có: $f+g=1$. Lấy đạo hàm hai vế của phương trình này, ta được: $f'+g'=0$. Nhằm mục đích xét số các nghiệm của đa thức, ta xét các thương của đạo hàm và hàm số. Ta có:

$$(f'/f)f+(g'/g)g=0, \ \frac{b}{a}=-\frac{f'/f}{g'/g}.$$

Mặt khác, giả sử $R(t)$ là một hàm hữu tỷ có phân tích sau đây

$$R(t)=\prod (t-\vartheta_i)^{q_i}, \quad q_i \in Z.$$

Tính toán đơn giản cho ta:

$$R'/R=\sum \frac{q_i}{t-\vartheta_i}.$$

Bây giờ giả sử a, b, c tương ứng có các nghiệm phân biệt là $\alpha_i, \beta_j, \gamma_k$. Ta có:

$$a(t)=\prod (t-\alpha_i)^{m_i}, \ b(t)=\prod (t-\beta_j)^{n_j}, \ c(t)=\prod (t-\gamma_k)^{r_k}.$$

Như vậy,

$$\frac{b}{a}=-\frac{f'/f}{g'/g}=-\frac{\sum \frac{m_i}{t-\alpha_i}-\sum \frac{r_k}{t-\gamma_k}}{\sum \frac{n_j}{t-\beta_j}-\sum \frac{r_k}{t-\gamma_k}}$$

Mẫu số chung của các phân số trong phần tử số và mẫu số của thương sau cùng là

$$N_0=\prod (t-\alpha_i)\prod (t-\beta_j)\prod (t-\gamma_k).$$

Đó là một đa thức có bậc là $n_0(abc)$. Như vậy, N_0f'/f và N_0g'/g là các đa thức có bậc không quá $n_0(abc)-1$. Mặt khác ta có:

$$\frac{b}{a}=-\frac{N_0f'/f}{N_0g'/g}$$

Vì a, b nguyên tố cùng nhau nên từ đẳng thức này suy ra bậc của a và bậc của b đều không vượt quá $n_0(abc)-1$. Điều tương tự cũng đúng đối với c do vai trò đối xứng của a, b, c trong phương trình xuất phát. Định lí được chứng minh.

Từ định lí Mason, ta có thể suy ra nhiều hệ thức giữa các đa thức. Chẳng hạn, một trong những hệ quả là định lí sau đây:

Định lí Davenport. *Giả sử $f(t), g(t)$ là các đa thức, sao cho $f^3 \neq g^2$. Khi đó ta có $\deg(f^3-g^2) \geq 1/2 \deg f+1$*

Chúng tôi dành chứng minh định lí này cho độc giả. Khẳng định tương tự đối với các số nguyên vẫn còn chưa được chứng minh. Ta có:

Giả thuyết Hall. Giả sử *x, y* là các số nguyên dương sao cho $x^3 \neq y^2$. Khi đó, với mọi $\varepsilon>0$, tồn tại $C>0$ chỉ phụ thuộc ε sao cho

$$| y^2-x^3|>Cx^{1/2-\varepsilon}$$

Có thể nói thêm rằng, bất đẳng thức trong định lí Davenport là tốt nhất có thể: đối với các đa thức $f(t)=t^6+4t^4+10t^2+6$, $g(t)=t^9+6t^7+21t^5+35t^3+63/2t$ ta có: $deg(f^3-g^2)=1/2degf+1$. Năm 1982, L. V. Danilov cũng đã chứng minh rằng, số mũ 1/2 trong giả thuyết Hall là tốt nhất có thể.

Định lí Mason và tương tự giữa các số nguyên và đa thức đã gợi ý cho giả thuyết sau đây:

Giả thuyết abc (Oesterlé, 1986). Giả sử *a, b, c* là các số nguyên, nguyên tố cùng nhau và thoả mãn hệ thức $a+b=c$. Khi đó, với mọi $\varepsilon>0$, tồn tại số *C* sao cho

$$\max(|a|, |b|, |c|)<CN^{1+\varepsilon},$$

trong đó $N=\prod_{p|abc} p$ là căn của *abc*.

Hoàn toàn tương tự như trên, từ giả thuyết "*abc*" có thể suy ra *Định lí Fermat tiệm cận*: với *n* đủ lớn, phương trình Fermat không có nghiệm nguyên.

Nhận xét. Giả sử *p* là một ước nguyên tố nào đó của một trong các số *a, b, c,* chẳng hạn $p|a$. Khi đó, nếu *p* lớn thì trong phân tích của *a* ra thừa số nguyên tố, *p* phải có số mũ tương đối nhỏ (để $|a|$ không vượt quá xa căn của *abc* theo giả thuyết). Điều này cũng giải thích tại sao phương trình Fermat không có nghiệm với bậc đủ lớn: khi đó, mọi ước nguyên tố của a^n, b^n, c^n sẽ tham gia với bậc quá lớn.

Trên đây là một ví dụ về sự tương tự giữa các giả thuyết đối với các số và các đa thức. Khi nghiên cứu một vấn đề nào đó đặt ra đối với các số, người ta thường nghiên cứu đồng thời tương tự của nó trên trường hàm. Phần lớn các giả thuyết của số học được chứng minh trước hết trên trường hàm. Như ta đã thấy trong chứng minh định lí Mason, điều quan trọng ở đây là có phép tính đạo hàm.

Gần đây, Manin (1992) đặt ra vấn đề: nếu như các số nguyên tương ứng với các đa thức một biến, thì các đa thức nhiều biến tương ứng với đối tượng nào? Câu hỏi đó dẫn đến việc xây dựng những "tích" mới của các "lược đồ" Spec Z. Đây là một hướng nghiên cứu đang phát triển mạnh, và nội dung của nó vượt ngoài khuôn khổ của cuốn sách này.

Bài tập và tính toán thực hành chương 5

I. Bài tập

5.1. Giả sử K là trường đặc trưng p. Chứng minh rằng, đối với các phần tử của trường K, ta có:

$$(a+b)^p=a^p+b^p.$$

5.2. Xây dựng trường F_9 từ trường F_3 bởi các đa thức sau:

1) x^2+1

2)x^2-x-1.

5.3. Dùng thuật toán EP để tìm ƯCLN của các đa thức P,Q trong trường F_p, và biểu diễn dạng $d=uP+vQ$:

1) $P=x^3+x+1$, $Q=x^2+x+1$, $p=2$.

2) $P=x^6+x^5+x^4+x^3+x^2+x+1$, $Q=x^4+x^2+x+1$, $p=2$.

3) $P=x^3-x+1$, $Q=x^2+1$, $p=3$.

4) $x^5+x^4+x^3-x^2-x+1$, $Q=x^3+x^2+x+1$, $p=3$.

5) $x^5+88x^4+73x^3+83x^2+51x+67$, $Q=x^3+97x^2+40x+38$, $p=101$.

5.4. Với mỗi $d \le 6$, tìm tất cả các đa thức bất khả quy bậc d trên trường F_2.

5.5. Những đa thức nào trong $F_p[x]$ có đạo hàm đồng nhất bằng 0?

5.6. Chứng minh rằng từ giả thuyết "*abc*" suy ra định lí Fermat tiệm cận.

5.7. Chứng minh định lí Davenport.

5.8. Cho f, g là các đa thức với hệ số nguyên, sao cho f^3-g^4 không đồng nhất bằng 0. Chứng minh rằng

$$\deg(f^3-g^4) \ge 5/3\deg g+1.$$

Phát biểu kết luận tương tự cho các số nguyên.

5.9. Dựa vào định lí Mason, tìm những hệ thức mới liên quan đến bậc của các đa thức hệ số nguyên (tương tự bài tập trên đây). Thử phát biểu và chứng minh kết luận tương tự dối với các số nguyên.

5.10. Thử đưa ra một định nghĩa về đạo hàm của một số nguyên.

II. Thực hành trên máy tính

II. 1. Thực hành tính số đa thức bất khả quy bậc *d* trên trường hữu hạn

Để tính số đa thức bất khả quy bậc n trên trường hữu hạn có đặc số *p* ta thực hiện dòng lệnh như sau;

```
[>mipolys(n, p);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện số đa thức cần tìm.

Thí dụ: Tính số các đa thức bất khả quy bậc 6 trên trường có đặc số 2.

Ta thực hiện lệnh sau:

```
[>mipolys(6, 2);
                                9
```

Như vậy có 9 đa thức bất khả quy trên trường F_2.

II. 2. Thực hành tìm ước chung lớn nhất của các đa thức trên trường hữu hạn

Cho *P, Q* là các đa thức biến *x* với hệ số trên trường hữu hạn có đặc số *p*. Để tìm ước chung lớn nhất *D* của *P* và *Q* và biểu diễn dưới dạng D=sP+tQ ta thực hiện dòng lệnh sau:

```
[> Gcdex(P,Q,x,'s','t') mod p;
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện một đa thức, đó chính là ước chung lớn nhất của *P, Q*. Tiếp tục thực hiện lệnh:

```
[>s,t;
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện hai đa thức *s, t* cần tìm.

Chú ý lệnh "Gcdex" chữ "G" là chữ viết hoa.

Thí dụ1: Tìm ước chung lớn nhất *D* của các đa thức *P, Q* trên trường F_2 và biểu diễn dưới dạng D=sP+tQ, trong đó $P=x^3+x+1$, $Q=x^2+x+1$.

Ta thực hiện dòng lệnh:

```
[> Gcdex(x^3+x+1,x^2+x+1,x,'s','t') mod 2;
                                1
[>s,t;
                             1+x,x^2
```

Vậy $1=(1+x)P+x^2Q$.

Thí dụ2: Tìm ước chung lớn nhất *D* của các đa thức *P, Q* trên trường F_{101} và biểu diễn dưới dạng D = sP + tQ, trong đó $x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67$, $Q=x^3+97x^2+40x+38$

Ta thực hiện dòng lệnh:

```
[>Gcdex(x^5+88*x^4+73*x^3+83*x^2+51*x+67,x^3+97*x^2+40*x
+38,x,'s','t') mod 101;
```

```
                                    x + 78
```

```
[> s,t;
```

```
                          50x + 20, 51x^3 + 26x^2 + 27x + 4
```

Vậy $x+78=(50x+20)P+(51x^3+26x^2+27x+4)Q$.

II. 3. Thực hành tìm ước chung lớn nhất, bội chung nhỏ nhất của các đa thức trên trường hữu tỷ

Cho *P, Q* là các đa thức biến *x* với hệ số trên trường hữu tỷ.

1. Để tìm ước chung lớn nhất *D* của *P* và *Q* ta thực hiện dòng lệnh sau:

```
[> gcd(P,Q);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện kết quả, đó chính là ước chung lớn nhất của *P, Q*.

Thí dụ1: Tìm ước chung lớn nhất *D* của các đa thức *P, Q* trên trường hữu tỷ trong đó $P=x^2-y^2$, $Q=x^3-y^3$.

Ta thực hiện dòng lệnh:

```
[> gcd(x^2-y^2,x^3-y^3);
```

```
                                    -y+x
```

Vậy ước chug lớn nhất của *P* và *Q* là -y+x

2. Để tìm bội chung nhỏ nhất của *P, Q* ta thực hiện dòng lệnh như sau:

```
[> lcm(P,Q);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện kết quả, đó chính là bội chung nhỏ nhất của *P,Q*.

Thí dụ 2: Tìm bội chung nhỏ nhất của các đa thức *P, Q* trên trường hữu tỷ trong đó $P=x^2-y^2$, $Q=x^3-y^3$.

Ta thực hiện dòng lệnh:

```
[> lcm(x^2-y^2,x^3-y^3);
```

```
                                -yx^3+y^4-x^4+xy^3
```

Vậy bội chung nhỏ nhất của *P* và *Q* là $-yx^3+y^4-x^4+xy^3$