MÔĐUN TỰA TỰ DO TRÊN MIỀN DEDEKIND

MỴ VINH QUANG*, PHẠM VIẾT HUY**

TÓM TẮT

Môđun phân tích được thành tổng trực tiếp các môđun cyclic được gọi là môđun tựa tự do. Lớp các môđun tựa tự do là mở rộng của lớp các môđun tự do. Bài báo này giới thiệu một số kết quả về các môđun tựa tự do trên miền Dedekind. Các kết quả này là sự mở rộng một số kết quả về nhóm Abel và môđun trên miền các ideal chính.

Từ khóa: miền Dedekind, môđun tựa tự do.

ABSTRACT

Quasi-free module over the Dedekind domain

A module decomposable into direct sum of cyclic modules is called a quasi-free module. The class of quasi-free modules is the extension of the class of free modules. This paper introduces some results about quasi-free modules over the Dedekind domain. These results are extensions of some results about Abelian groups and modules over a principal ideal domain.

Keywords: Dedekind domain, quasi-free module.

1. Mở đầu

Trong lí thuyết môđun, các môđun tự do, đặc biệt là môđun tự do trên miền các ideal chính có vai trò quan trọng. Đã có nhiều kết quả sâu sắc và thú vị về các môđun tự do trên miền các ideal chính. Chúng ta nhớ lại rằng, một môđun được gọi là môđun tự do nếu nó phân tích được thành tổng trực tiếp các môđun cyclic không xoắn. Một câu hỏi khá tự nhiên được đặt ra là: Tại sao phải là các môđun cyclic không xoắn? Nếu ta bỏ đi điều kiện không xoắn thì sao?

Chúng tôi gọi các môđun phân tích được thành tổng trực tiếp các môđun cyclic là môđun tựa tự do. Bài báo này giới thiệu một số kết quả về các môđun tựa tự do trên miền Dedekind. Chú ý rằng miền Dedekind là mở rộng khá tự nhiên về mặt số học của miền các ideal chính nhưng lại có khá nhiều tính chất khác lạ so với miền các ideal chính.

2. Một số khái niệm cơ bản

2.1. Miền Dedekind

Miền nguyên D được gọi là *miền Dedekind* nếu D là miền Noether, đóng nguyên và mọi ideal nguyên tố khác không của D đều là ideal tối đại.

Tập các ideal của miền Dedekind D với phép nhân các ideal làm thành nửa nhóm giao hoán, có đơn vị với sự phân tích duy nhất thành các phần tử nguyên tố. Nghĩa là

* PGS TS, Trường Đại học Sư phạm TPHCM
** HVCH, Trường Đại học Sư phạm TPHCM

mọi ideal khác không và khác D đều phân tích được duy nhất thành tích các ideal nguyên tố. Nếu A, B là các ideal của D thì $A|B$ khi và chỉ khi $B \subset A$, *ước chung lớn nhất của A, B* là: $(A,B) = A+B$, *bội chung nhỏ nhất của A, B* là: $[A,B] = A \cap B$. A, B gọi là *nguyên tố cùng nhau* nếu $(A,B) = D$. Nếu P là ideal nguyên tố của D thì $ord_P(A)$ là số tự nhiên lớn nhất thỏa: $P^{ord_P(A)}|A$. Các kết quả về miền Dedekind có thể tham khảo trong $[1],[2]$.

Bổ đề sau đây sẽ rất có ích khi làm việc với miền Dedekind.

2.2. Bổ đề [1, Định lí 9.3.1]

Cho D là miền Dedekind và A, B là các ideal khác không của D. Khi đó tồn tại $a \in A$ *để* $A = \langle a \rangle + AB$.

2.3. Môđun trên miền Dedekind

Cho M là môđun trên miền Dedekind D và $x \in M$. *Cấp của x*, kí hiệu $|x|$, được định nghĩa như sau: $|x| := \{a \in D, ax = 0\}$. Dễ thấy $|x|$ là một ideal của D. x được gọi là *phần tử không xoắn* nếu $|x| = 0$. Trong trường hợp ngược lại, x được gọi là *phần tử xoắn*. Tập các phần tử xoắn của M là một môđun con của M, được gọi là *môđun con xoắn* của M, và được kí hiệu là M_T. Nếu $M_T = M$ thì M được gọi là *môđun xoắn*. Nếu $M_T = 0$ thì M được gọi là *môđun không xoắn*. Hiển nhiên, M/M_T là môđun không xoắn.

Với mỗi ideal nguyên tố khác không P của D, kí hiệu $M_P = \{x \in M, |x|$ là lũy thừa của $P\}$. M_P là một môđun con của M, được gọi là *môđun con P-nguyên sơ* của M. M được gọi là *P-môđun* nếu $M_P = M$. Tập các phần tử x của M, thỏa điều kiện $Px = 0$ tạo thành một môđun con của M và được kí hiệu là $M[P]$.

Môđun M được gọi là *bị chặn* nếu cấp của các phần tử của M bị chặn, nghĩa là tồn tại ideal A khác không của D để $AM = 0$.

Cho M là P-môđun. Khi đó, số tự nhiên n được gọi là độ cao (hay P-độ cao) của $x \in M$ nếu $x \in P^n M$ nhưng $x \notin P^{n+1}M$. Trong trường hợp $x \in P^n M$ với mọi n ta nói x có độ cao vô hạn.

2.4. Bổ đề

Cho M là môđun trên miền Dedekind D. Khi đó:

i) Với mọi $x \in M, a \in D, |ax| = \dfrac{|x|}{|x| + \langle a \rangle}$, *và nếu* $|x| + \langle a \rangle = D$ *thì* $|x| = |ax|$.

ii) Nếu $x, y \in M$ *và* $|x| + |y| = D$ *thì* $|x+y| = |x||y|$.

Chứng minh:

i) Với $b \in \frac{|x|}{|x|+\langle a\rangle}$ ta có $ba \in \frac{|x|}{|x|+\langle a\rangle}\langle a\rangle \subset |x|$. Do đó, $b(ax)=(ba)x=0$. Vậy $\frac{|x|}{|x|+\langle a\rangle} \subset |ax|$. Ngược lại, nếu $b(ax)=0$ thì $ba \in |x|$. Do đó, $b\frac{\langle a\rangle}{|x|+\langle a\rangle} \subset \frac{|x|}{|x|+\langle a\rangle}$. Mặt khác, vì $\left(\frac{\langle a\rangle}{|x|+\langle a\rangle}, \frac{|x|}{|x|+\langle a\rangle}\right)=D$ nên tồn tại $u \in \frac{\langle a\rangle}{|x|+\langle a\rangle}, v \in \frac{|x|}{|x|+\langle a\rangle}$ để $u+v=1$. Khi đó, $b=b(u+v)=bu+bv \in \frac{|x|}{|x|+\langle a\rangle}$. Vậy $|ax|=\frac{|x|}{|x|+\langle a\rangle}$.

Ngoài ra, nếu $|x|+\langle a\rangle = D$ thì tồn tại $u \in |x|, v \in \langle a\rangle$ để $u+v=1$. Khi đó, $x=x(u+v)=xu+xv=xv \in \langle ax\rangle$. Do đó, $|x|=|ax|$.

ii) Với mọi $a \in |x|, b \in |y|$, ta có $ab(x+y)=abx+aby=0$ nên $c(x+y)=0$ với mọi $c \in |x||y|$. Vậy $|x||y| \subset |x+y|$. Ngược lại, vì $|x|+|y|=D$ nên tồn tại $u \in |x|, v \in |y|$ để $u+v=1$. Nếu $a \in |x+y|$ thì $a(x+y)=0$. Suy ra $au(x+y)=0$. Do đó, $auy=0$, nghĩa là $au \in |y|$. Do đó, $a=a(u+v)=au+av \in |y|$. Tương tự, $a \in |x|$. Do đó, $a \in |x| \cap |y| = [|x|,|y|] = |x||y|$, vì $|x|,|y|$ nguyên tố cùng nhau. Vậy $|x+y|=|x||y|$.

2.5. *Bổ đề*

Cho M là môđun trên miền Dedekind. Khi đó, môđun con xoắn M_T của M là tổng trực tiếp các môđun con P-nguyên sơ của M. $M_T = \bigoplus_P M_P$.

Chứng minh:

Đầu tiên, ta chứng minh $M_T = \sum_P M_P$. Giả sử $0 \neq x \in M_T$. Khi đó, $|x| = P_1^{k_1}...P_m^{k_m}$. Với mỗi $i=1,2...m$, đặt $A_i = \frac{|x|}{P_i^{k_i}}$. Khi đó, $(A_1,...,A_m)=D$ nên tồn tại $a_i \in A_i$ để $a_1+...+a_m=1$. Ta có, $x=(a_1+...+a_m)x=a_1x+...+a_mx$. Nếu $b \in P_i^{k_i}$ thì $ba_i \in |x|$ nên $ba_ix=0$. Do đó, $b \in |a_ix|$, nghĩa là, $P_i^{k_i} \subset |a_ix|$, suy ra $a_ix \in M_{P_i}$ và $x \in \sum_P M_P$. Vậy $M_T \subset \sum_P M_P$.

Tiếp theo, ta chứng minh $M_P \cap \sum_{Q\neq P} M_Q = 0$. Giả sử $0 \neq x \in M_P \cap \sum_{Q\neq P} M_Q$. Vì $x \in M_P$ nên $|x| = P^m$, với $m \geq 1$, và $x \in \sum_{Q\neq P} M_Q$ nên $(|x|, P) = D$ hay $(P^m, P) = D(!)$ Mâu thuẫn chứng tỏ $M_P \cap \sum_{Q\neq P} M_Q = 0$. Vậy $M_T = \bigoplus_P M_P$.

3. Cơ sở chính tắc của môđun tựa tự do

3.1. Môđun tựa tự do

Cho *M* là một môđun trên miền Dedekind *D*. Tập con khác rỗng *S* của *M* được gọi là *tập độc lập tuyến tính* hoặc đơn giản là *độc lập*, nếu $0 \notin S$ và với mọi $s_1,...,s_k$ đôi một khác nhau của *S*, với mọi $a_1,...,a_k \in D$ nếu $a_1s_1 + ... + a_ks_k = 0$ thì $a_is_i = 0$ với mọi *i*. Nếu *S* không độc lập, ta nói *S* là tập *phụ thuộc*. Một tập sinh của *M* mà độc lập được gọi là *cơ sở* của *M*. Môđun *M* được gọi là *môđun tựa tự do* nếu nó có thể phân tích được thành tổng trực tiếp của các môđun cyclic. Từ các định nghĩa, ta có ngay môđun là tựa tự do khi và chỉ khi nó có cơ sở. Một môđun là tự do khi và chỉ khi nó là môđun tựa tự do không xoắn. Như vậy, lớp môđun tựa tự do là mở rộng thực sự của lớp các môđun tự do.

Bổ đề dưới đây mô tả một lớp các môđun tựa tự do nhưng không là môđun tự do.

3.2. Bổ đề

Cho M là môđun trên miền Dedekind D. Nếu tồn tại ideal nguyên tố khác không P của D để $PM = \{0\}$ *thì M là môđun tựa tự do.*

Chứng minh:

Vì *D* là miền Dedekind nên *P* là ideal tối đại của *D*, do đó, D/P là trường. Do $PM = \{0\}$ nên tương ứng:

$$D/P \times M \to M$$
$$(\bar{a}, m) \mapsto am$$

là phép nhân ngoài. Dễ thấy *M* với phép nhân trên trở thành một không gian véctơ trên trường D/P. Nếu S là một cơ sở của D/P-không gian vectơ *M* thì S cũng chính là một cơ sở của *D*-môđun *M*. Vậy *M* là môđun tựa tự do.

3.3. Nhận xét

Hai cơ sở bất kì của môđun tự do trên vành giao hoán, có đơn vị đều có cùng lực lượng và lực lượng đó được gọi là hạng của môđun tự do. Vấn đề được đặt ra là liệu nhận xét trên có còn đúng đối với môđun tựa tự do? Chúng ta có câu trả lời phủ định ngay cả đối với môđun tựa tự do trên miền các ideal chính bằng phản ví dụ sau: $Z/6Z$ là Z-môđun tựa tự do với 2 cơ sở có số phần tử khác nhau là $\{\bar{1}\}$ và $\{\bar{2},\bar{3}\}$.

Để khắc phục tình trạng này, chúng tôi đưa ra một khái niệm mới, gọi là cơ sở chính tắc của môđun tựa tự do như sau.

3.4. Định nghĩa

Một cơ sở S của một môđun tựa tự do được gọi là *cơ sở chính tắc* nếu mỗi phần tử $x \in S$ hoặc là không xoắn hoặc có cấp là lũy thừa của một ideal nguyên tố.

3.5. Định lí (cơ sở chính tắc của môđun tựa tự do)

Môđun tựa tự do M trên miền Dedekind D luôn có cơ sở chính tắc. Hai cơ sở chính tắc bất kì của M có cùng lực lượng, lực lượng này được gọi là hạng của môđun tựa tự do M.

Chứng minh:

Chứng minh sự tồn tại cơ sở chính tắc của *M*. Trước hết, ta có nhận xét: nếu $x \in M$ có cấp *AB* với $(A,B)=D$ thì $\langle x\rangle = \langle y\rangle + \langle z\rangle$ trong đó *y* có cấp *A*, *z* có cấp *B*. Thật vậy, theo Bổ đề 2.2, tồn tại $b \in B$ để $B = \langle b\rangle + AB$. Khi đó, theo Bổ đề 2.4, $|bx| = \dfrac{AB}{\langle b\rangle + AB} = A$. Tương tự, tồn tại $a \in A$ để $|ax| = B$. Khi đó, theo Bổ đề 2.4, $|(a+b)x| = AB$ và $\langle (a+b)x\rangle = \langle x\rangle$. Mặt khác, $\langle (a+b)x\rangle \subset \langle bx\rangle + \langle ax\rangle \subset \langle x\rangle$. Do đó, $\langle x\rangle = \langle bx\rangle + \langle ax\rangle = \langle y\rangle + \langle z\rangle$.

Bây giờ, giả sử S là một cơ sở của *M*. Khi đó, nếu $x \in S, |x| = P_1^{k_1}...P_m^{k_m}$ thì theo chứng minh trên $\langle x\rangle = \langle x_1\rangle \oplus ... \oplus \langle x_m\rangle$ với $|x_j| = P_j^{k_j}$. Như vậy, bằng cách giữ nguyên x nếu x không xoắn và thay x bằng $\{x_1,...,x_m\}$ nếu x có cấp hữu hạn. Ta nhận được cơ sở chính tắc của *M*.

Hai cơ sở chính tắc của *M* có cùng lực lượng sẽ được thấy rõ qua 2 bổ đề sau:

Bổ đề 1.

Lực lượng của các phần tử không xoắn trong hai cơ sở chính tắc của môđun M là như nhau.

Chứng minh:

Giả sử $S \cup T$ là một cơ sở chính tắc của *M* trong đó *S* là tập tất cả các phần tử không xoắn trong cơ sở chính tắc và *T* là tập tất cả các phần tử có cấp là lũy thừa ideal nguyên tố. Khi đó, $M = \bigoplus_{x\in S}\langle x\rangle \bigoplus_{y\in T}\langle y\rangle$ và mô đun con xoắn của *M* là $M_T = \bigoplus_{y\in T}\langle y\rangle$.

Ta có, $M/M_T \cong \underset{x\in S}{\oplus}\langle x\rangle$. Bởi vậy, M/M_T là môđun tự do có hạng bằng $|S|$. Vậy lực lượng của các phần tử không xoắn trong cơ sở chính tắc của *M* bằng hạng của môđun tự do M/M_T không phụ thuộc vào cách chọn cơ sở.

Bổ đề 2.

Với mỗi số tự nhiên m và mỗi deal nguyên tố P của D cho trước, lực lượng của các phần tử có cấp P^m trong hai cơ sở chính tắc của môđun M là như nhau.

Chứng minh:

Vì mỗi phần tử cấp lũy thừa của *P* chỉ có thể nằm trong thành phần *P*-nguyên sơ M_P nên ta có thể xem *M* là *P*-môđun. Giả sử $S\cup R\cup T$ là một cơ sở chính tắc của *M*, trong đó *S* là tập các phần tử của cơ sở có cấp là P^m, *R* là tập các phần tử của cơ sở có cấp là P^r, với $r>m$, *T* là tập các phần tử của cơ sở có cấp là P^t, với $t<m$. Đặt $H=\underset{y\in R}{\oplus}\langle y\rangle, K=\underset{z\in T}{\oplus}\langle z\rangle$. Ta có $M=\underset{x\in S}{\oplus}\langle x\rangle\oplus H\oplus K$.

Do đó $P^{m-1}M=\underset{x\in S}{\oplus}\langle P^{m-1}x\rangle\oplus P^{m-1}H$ và $(P^{m-1}M)[P]=\underset{x\in S}{\oplus}\langle P^{m-1}x\rangle\oplus H[P]$,

$P^mM=P^mH$ và $(P^mM)[P]=H[P]$.

Bởi vậy,

$(P^{m-1}M)[P]/(P^mM)[P]\cong\underset{x\in S}{\oplus}\langle P^{m-1}x\rangle$. Theo Bổ đề 3.2, $(P^{m-1}M)[P]/(P^mM)[P]$ là không gian vectơ trên trường D/P và $|S|=dim\left((P^{m-1}M)[P]/(P^mM)[P]\right)$ không phụ thuộc vào cách chọn cơ sở chính tắc.

Như vậy, Bổ đề 2 đã được chứng minh và Định lí 3.5 được chứng minh hoàn toàn.

3.6. Nhận xét

Hai môđun tự do có cùng hạng thì luôn đẳng cấu. Vậy, hai môđun tựa tự do có cùng hạng có đẳng cấu với nhau không?

Một lần nữa, chúng ta có câu trả lời phủ định thông qua ví dụ sau: *Z* là *Z*-môđun tựa tự do với cơ sở chính tắc là $\{1\}$, $Z/2Z$ cũng là *Z*-môđun tựa tự do với cơ sở chính tắc là $\{\bar{1}\}$. Cả hai môđun tựa tự do này có cùng hạng bằng 1, tuy nhiên, chúng không đẳng cấu. Để khắc phục điều này, chúng tôi đưa ra khái niệm cơ sở chính tắc cùng kiểu như sau:

3.7. Định nghĩa

Hai cơ sở chính tắc được gọi là *cùng kiểu* nếu lực lượng các phần tử không xoắn trong mỗi cơ sở là như nhau và với mỗi số tự nhiên *m*, mỗi ideal nguyên tố *P*, lực lượng của các phần tử có cấp P^m trong mỗi cơ sở là như nhau.

Như là hệ quả của Định lí 3.5, ta có kết quả sau:

3.8. Hệ quả

Hai cơ sở chính tắc của một môđun tựa tự do trên miền Dedekind có cùng kiểu. Hai môđun tựa tự do đẳng cấu với nhau khi và chỉ khi các cơ sở chính tắc của chúng có cùng kiểu.

Chứng minh:

Thật vậy, ý đầu của hệ quả suy ra ngay từ Bổ đề 1, Bổ đề 2 của Định lí 3.5. Để chứng minh ý sau, ta có nhận xét nếu $f: M \to N$ là đẳng cấu thì *x* và *f(x)* có cùng cấp. Do đó, nếu S là cơ sở chính tắc của *M* thì $\{f(x), x \in S\}$ là cơ sở chính tắc của *N* có cùng kiểu với S. Ngược lại, nếu S và T lần lượt là cơ sở chính tắc của *M* và *N* có cùng kiểu. Khi đó tồn tại song ánh $f: S \to T$ sao cho $|f(x)| = |x|, \forall x \in S$. Dễ thấy song ánh có thể mở rộng thành đẳng cấu $\overline{f}: M \to N$.

4. Điều kiện cần và đủ để môđun xoắn là môđun tựa tự do

4.1. Định lí

P-môđun M trên miền Dedekind D là môđun tựa tự do khi và chỉ khi tồn tại dây chuyền tăng các môđun con $\{M_n\}: M_1 \le M_2 \le \ldots \le M_n \le \ldots$ *và dãy các số nguyên không âm* $k(n)$ *sao cho* $\bigcup_n M_n = M$ *và độ cao của các phần tử khác không của* M_n *đều không vượt quá* $k(n)$.

Chứng minh:

Giả sử *M* là *P*-môđun tựa tự do với cơ sở S. Ta định nghĩa $M_n = \left\langle x \in S, |x| \,\|\, |P^n| \right\rangle$. Khi đó, mỗi phần tử khác không của M_n có độ cao không vượt quá $n-1$. Do đó $\{M_n\}$ là dây chuyền cần tìm.

Ngược lại, giả sử *M* là *P*-môđun có dây chuyền $\{M_n\}$ thỏa các điều kiện của định lí. Bằng cách bổ sung thêm hữu hạn các môđun không ở đầu dây chuyền, lặp lại M_n hữu hạn lần (nếu cần) và đánh số lại, ta có thể xem $k(n) = n-1$. Khi đó, từ các định nghĩa ta có ngay $P^n M \cap M_n = 0$ với $n = 1, 2, \ldots$

Trong tập tất cả các dây chuyền $\{K_n\}$ thỏa $M_n \subset K_n$ và $P^n M \cap K_n = 0$ với $n = 1, 2, \ldots$, ta định nghĩa quan hệ thứ tự $\{K_n\} \le \{H_n\}$ nếu và chỉ nếu $K_n \subset H_n$ với mọi *n*. Theo Bổ đề Zorn, tồn tại dây chuyền $\{H_n\}$ là phần tử tối đại của tập trên.

Theo Bổ đề 3.2, $P^{n-1}M \cap H_n[P]$ là môđun tựa tự do. Kí hiệu S_n là cơ sở của $P^{n-1}M \cap H_n[P]$. Nếu $i<j$ và $x \in S_i \cap S_j$ thì $x \in H_i[P] \subset H_{j-1}[P]$ và $x \in P^{j-1}M$ nên $x \in P^{j-1}M \cap H_{j-1}[P]=0$ nên $x=0$ (!). Do đó, các tập $S_1, S_2, \dots$ rời nhau. Hơn nữa, tập $S=\cup_n S_n$ là tập độc lập. Thật vậy, nếu $\sum_{i=1}^{n} a_i s_i = 0$ với $a_i \in D, s_i \in S_i$ thì $s_i \in H_i[P] \subset H_{n-1}[P]$ với $i=1,2,\dots,n-1$ và $s_n \in P^{n-1}M$, do đó $a_n s_n = -\sum_{i=1}^{n-1} a_i s_i \in P^{n-1}M \cap H_{n-1}[P]=0$. Suy ra $a_n s_n = \sum_{i=1}^{n-1} a_i s_i = 0$. Bằng quy nạp, ta có $a_i s_i = 0$ với mọi i và S là tập độc lập.

Tiếp theo, với mỗi $s \in S$, giả sử *h(s)* là độ cao của *s*. Ta sẽ chứng minh *s* viết được dưới dạng $s = p(s)^{h(s)} x(s)$, trong đó $p(s) \in P, x(s) \in M$ và $|x(s)| = P^{h(s)+1}$.

Thật vậy, vì $s \in P^{h(s)}M$ nên $s = \sum_{hh} p_i x_i$ với $p_i \in P^{h(s)}, x_i \in M, |x_i| = P^{n_i}$. Đặt $k = max\{h(s), n_i\}$, theo Bổ đề 2.2 tồn tại $p(s) \in P$ thỏa $P = \langle p(s) \rangle + P^k$. Do đó, $P^{h(s)} \subset \langle p(s)^{h(s)} \rangle + P^{k+1}$. Vì $p_i \in P^{h(s)}$ nên $p_i = a_i p(s)^{h(s)} + u_i$ với $a_i \in D, u_i \in P^{k+1}$. Ta có $s = \sum \left(a_i p(s)^{h(s)} + u_i\right) s_i = p(s)^{h(s)} x(s)$ trong đó $x(s) = \sum a_i s_i \in M$. Mặt khác, ta có $1 = ord_P P = min\{ord_P \langle p(s) \rangle, k\}$ và $k>1$ nên $ord_P \langle p(s) \rangle = 1$, nghĩa là $\langle p(s) \rangle = PI$ với I là ideal của D và $(P, I) = D$. Đặt $|x(s)| = P^l$, theo Bổ đề 2.4, ta có

$$P = |s| = \left|p(s)^{h(s)} x(s)\right| = \frac{|x(s)|}{\left(|x(s)|, \langle p(s)^{h(s)} \rangle\right)} = \frac{P^l}{\left(P^l, P^{h(s)} I^{h(s)}\right)} = \frac{P^l}{P^{min\{l, h(s)\}}}.$$

Do đó, $min\{l, h(s)\} = l-1$ nên $h(s) = l-1$ và $l = h(s)+1$ hay $|x(s)| = P^{h(s)+1}$.

Ngoài ra, chú ý rằng nếu $a(s) \in P^{h(s)}$ thì $a(s).x(s) = b(s).s$ với $b(s) \in D$.

Thật vậy,

vì $P^{h(s)} \subset \langle p(s)^{h(s)} \rangle + P^{k+1}$ nên $a(s) = p(s)^{h(s)} b(s) + u(s)$ với $b(s) \in D, u(s) \in P^{k+1}$.

Do đó $a(s)x(s) = \left(p(s)^{h(s)} b(s) + u(s)\right) x(s) = p(s)^{h(s)} b(s) x(s) = b(s).s$.

Bây giờ, ta chứng minh $\{x(s), s \in S\}$ là tập độc lập. Giả sử ngược lại, khi đó tồn tại $a(s) \in D$ để $\sum_{s \in S} a(s)x(s) = 0$ và có ít nhất $a(s)x(s) \neq 0$. Gọi *d* là số tự nhiên bé nhất để $P^d a(s)x(s) = 0$ với mọi $s \in S$. Nếu *d=1* thì $Pa(s)x(s) = 0$ với mọi $s \in S$. Vì $|x(s)| = P^{h(s)+1}$ nên $Pa(s) \subset P^{h(s)+1}$ hay $a(s) \in P^{h(s)}$. Do đó, theo chú ý trên,

$a(s).x(s) = b(s).s$. Bởi vậy, $\sum b(s).s = \sum a(s).x(s) = 0$ nên $b(s).s = 0$ do đó $a(s).x(s) = 0$ với mọi $s \in S$ (!).

Nếu *d>1*, do $P^d a(s)x(s) = 0$ và $|x(s)| = P^{h(s)+1}$ nên $P^d a(s) \subset P^{h(s)+1}$ hay $P^{d-1}a(s) \subset P^{h(s)}$, theo chú ý trên với mọi $p \in P^{d-1}$ ta có $pa(s)x(s) = b(s).s$. Bởi vậy, $\sum b(s).s = p\sum a(s)x(s) = 0$ nên $b(s).s = 0$ với mọi $s \in S$ nghĩa là $pa(s)x(s) = 0$ với mọi $s \in S$ (vì *S* độc lập). Suy ra $P^{d-1}a(s)x(s) = 0$ (!), trái với cách chọn *d*. Vậy $\{x(s), \ s \in S\}$ là tập độc lập.

Cuối cùng ta chứng minh $\{x(s), \ s \in S\}$ là cở sở của *M*. Đặt $T = \langle x(s), \ s \in S \rangle$. ta chứng minh $M = T$.

Đầu tiên, ta chứng minh $M[P] \subset T$. Thật vậy, nếu $s \in S_1$ thì $h(s) = 0$ do đó $s = x(s) \in T$ bởi vậy $H_1[P] = P^0 M \cap H_1[P] = \langle S_1 \rangle \subset T$. Bây giờ, giả sử ngược lại $M[P]$ không là môđun con của *T*. Vì $M[P] = \cup H_n[P]$ nên tồn tại số tự nhiên *r* bé nhất để $H_r[P]$ không nằm trong *T* và tất nhiên $r > 1$ vì $H_1[P] \subset T$. Lấy $x \in H_r[P] \backslash T$, khi đó $x \notin H_{r-1}$ do tính bé nhất của *r*. Khi đó, ta có $P^{r-1}M \cap \langle x, H_{r-1} \rangle \neq 0$ vì nếu ngược lại, ta có thể thay thế H_{r-1} bởi $\langle x, H_{r-1} \rangle$ ta được dây chuyền mới lớn hơn dây chuyền $\{H_n\}$, mâu thuẫn với tính tối đại của $\{H_n\}$.

Lấy $0 \neq y \in P^{r-1}M \cap \langle x, H_{r-1} \rangle$, ta có $y = ax + h_{r-1}$ với $a \in D, h_{r-1} \in H_{r-1}$. Do $P^{r-1}M \cap H_{r-1} = 0$ nên $ax \neq 0$ và $ax = y - h_{r-1} \in \langle x \rangle \cap \left(P^{r-1}M + H_{r-1}\right)$. Mặt khác, $|x| = P$ nên $a \notin P$ do đó $(\langle a \rangle, P) = D$, nghĩa là tồn tại $b \in D, p \in P$ để $ab + p = 1$. Do đó $x = (ab+p)x = b(ax) \in P^{r-1}M + H_{r-1}$, nghĩa là $x = x_1 + h$ với $x_1 \in P^{r-1}M, h \in H_{r-1}$. Suy ra $x_1 = x - h \in P^{r-1}M \cap H_r$. Bởi vậy, với mọi $p \in P$ ta có $px_1 \in P^r M \cap H_r = \{0\}$ hay $x_1 \in H_r[P]$. Do đó, $x_1 \in P^{r-1}M \cap H_r[P] = \langle S_r \rangle \subset T$. Mặt khác, với mọi $p \in P$, $ph = px - px_1 = 0$ nên $h \in H_{r-1}[P] \subset T$ (do cách chọn *r*). Bởi vậy, ta lại có $x = x_1 + h \in T$ (!). Mâu thuẫn này chứng tỏ $M[P] \subset T$.

Tiếp theo, *S* là tập sinh, do đó *S* là cơ sở của $T[P]$. Thật vậy, nếu $x \in T[P]$ thì $x = \sum_{s \in S} a(s)x(s)$. Vì $Px = 0$ nên với mọi $p \in P$ ta có $\sum_{s \in S} pa(s)x(s) = 0$ suy ra $pa(s)x(s) = 0$ do tính độc lập của $\{x(s), s \in S\}$. Do đó, $pa(s) \subset |x(s)| = P^{h(s)+1}$. Suy ra $a(s) \in P^{h(s)}$ nên theo chú ý trên $a(s).x(s) = b(s).s$, bởi vậy $x = \sum_{s \in S} a(s)x(s) = \sum_{s \in S} b(s).s$ và *S* là tập sinh của $T[P]$.

Bây giờ, ta chứng minh $M = T$. Giả sử ngược lại, $T < M$. Khi đó, tồn tại $x_0 \in M \setminus T$ sao cho $|x_0|$ chia hết $|x|$ với mọi $x \in M \setminus T$. Lại vì $M[P] \subset T$ nên $|x_0| \neq P$, do đó $|x_0| = P^{n+1}$ với $n \geq 1$. Mặt khác, theo Bổ đề 2.2 tồn tại $p \in P$ sao cho $P = \langle p \rangle + P^2$. Khi đó, với mọi số tự nhiên *h* ta có $P^h \subset \langle p^h \rangle + P^{h+1}$.

Vì $p^n x_0 \in M[P] = T[P]$ nên theo chứng minh trên $p^n x_0 = a_1 s_1 + a_2 s_2 + ... + a_k s_k$ với $s_i \in S$. Bằng cách đánh số lại, nếu cần, ta có thể xem $s_1, s_2 ..., s_j \in S_{n+1} \cup S_{n+2} \cup ...$ và $s_{j+1}, ..., s_k \in S_1 \cup ... \cup S_n$ trong đó $0 \leq j \leq k$.

Ta có:

Nếu $i = j+1, ..., k$ thì $s_i \in H_n[P]$ vì $S_1, ..., S_n$ nằm trong $H_n[P]$.

Nếu $i = 1, 2..., j$ thì $s_i \in P^n M$ nên $h(s_i) \geq n$.

Lại vì $p(s_i)^{h(s_i)} \in P^{h(s_i)} \subset \langle p^{h(s_i)} \rangle + P^{h(s_i)+1}$ nên với $i = 1, 2..., j$, ta có

$a_i s_i = a_i p(s_i)^{h(s_i)} x(s_i) = a_i p^{h(s_i)} b(s_i) x(s_i) = p^n x_i$ với

$x_i = a_i b(s_i) p^{h(s_i)-n} x(s_i) \in \langle x(s_i) \rangle \subset T$. Do đó

$p^n (x_0 - x_1 - ... - x_j) = a_{j+1} s_{j+1} + ... + a_k s_k \in P^n M \cap H_n[P] = 0$.

Mặt khác, với mọi $u \in P^{n+1}$, ta có $u x_i = a_i b(s_i) \left(u p^{h(s_i)-n} x(s_i) \right) = 0$ với $i = 1, 2..., j$ do đó $u(x_0 - x_1 - ... - x_j) = 0$.

Bây giờ, với mọi $a \in P^n \subset \langle p^n \rangle + P^{n+1}$ ta có $a = p^n b + u$ với $b \in D, u \in P^{n+1}$, khi đó, $a(x_0 - x_1 - ... - x_j) = b p^n (x_0 - x_1 - ... - x_j) + u(x_0 - x_1 - ... - x_j) = 0$ nên $x_0 - x_1 - ... - x_j \in T$, do cách chọn x_0. Vì $x_1, ..., x_j \in T$ nên $x_0 \in T$ (!).

Vậy $M = T$ và *M* là môđun tựa tự do. Định lí 4.1 được chứng minh hoàn toàn.

Từ Định lí 4.1, ta thu được một số hệ quả thú vị sau đây.

4.2. *Hệ quả* (*Điều kiện cần và đủ để một môđun xoắn là môđun tựa tự do*)

Môđun xoắn M trên miền Dedekind D là môđun tựa tự do khi và chỉ khi với mọi ideal nguyên tố khác không P của D, môđun con P-nguyên sơ M_P của nó thỏa các điều kiện của Định lí 4.1.

Chứng minh:

Giả sử *M* là môđun xoắn, tựa tự do và $S \cup T$ là cơ sở chính tắc của *M* trong đó *S* là tập tất cả các phần tử có cấp là lũy thừa của *P* trong cơ sở chính tắc. Khi đó, $M_P = \bigoplus_{s \in S} \langle s \rangle$. Vậy M_P là môđun tựa tự do, do đó, M_P thỏa các điều kiện của Định lí

4.1. Ngược lại, nếu M_P thỏa các điều kiện của Định lí 4.1 thì M_P là môđun tựa tự do, do đó $M = \bigoplus_P M_P$ cũng tựa tự do.

Kết quả dưới đây có thể xem như là một mở rộng của định lí nổi tiếng về cấu trúc của nhóm Abel hữu hạn.

4.3. Hệ quả

Mọi môđun bị chặn trên miền Dedekind đều là môđun tựa tự do. Nói riêng, môđun xoắn, hữu hạn sinh trên miền Dedekind là môđun tựa tự do.

Chứng minh:

Dựa vào Hệ quả 4.2, ta chỉ cần chứng minh khi *M* là *P*-môđun là đủ. Do *M* bị chặn nên tồn tại số tự nhiên *k* để $P^k M = 0$. Khi đó, mọi phần tử khác không của *M* đều có độ cao không vượt quá *k*. Đặt $M_n = M$ và $k(n) = k$ với mọi $n = 1, 2, ...$ Dây chuyền M_n và dãy $k(n)$ thỏa các điều kiện của Định lí 4.1 nên *M* là môđun tựa tự do.

Nếu *M* là môđun xoắn, hữu hạn sinh thì *M* bị chặn, do đó *M* là môđun tựa tự do.

4.4. Hệ quả

Môđun con của môđun tựa tự do, xoắn trên miền Dedekind là môđun tựa tự do

Chứng minh.

Giả sử *M* là *P*-môđun tựa tự do và *H* là môđun con của *M*. Theo Định lí 4.1, *M* có dây chuyền $\{M_n\}$ và dãy $k(n)$ thỏa các điều kiện của Định lí 4.1. Đặt $H_n = H \cap M_n$. Khi đó,*H* có dây chuyền $\{H_n\}$ và dãy $k(n)$ thỏa các điều kiện của Định lí 4.1, do đó *H* là tựa tự do.

Nếu *M* là môđun tựa tự do, xoắn thì $M = \bigoplus_P M_P$ trong đó M_P cũng là các môđun tựa tự do (theo Hệ quả 4.2). Giả sử *H* là môđun con của *M*. Khi đó H_P là môđun con của M_P nên theo chứng minh trên H_P là môđun tựa tự do. Do đó $H = \bigoplus_P H_P$ là môđun tựa tự do.

4.5. Nhận xét

Hệ quả 4.3 và 4.4 sẽ không còn đúng nữa nếu ta bỏ đi điều kiện "xoắn". Thậm chí, môđun con của môđun tự do trên miền Dedekind có thể không là môđun tựa tự do. Ví dụ dưới đây chứng tỏ điều đó.

Xét vành $D = \left\{a + b\sqrt{-5},\ \ a, b \in Z\right\}$, *D* chính là vành các số nguyên đại số của mở rộng $Q\left(\sqrt{-5}\right)$ trên *Q* nên *D* là miền Dedekind.

Trong *D* xét ideal $I = \left\langle 2, 1 + \sqrt{-5} \right\rangle$. Không khó để chứng minh *I* không là ideal chính của *D*. Mặt khác, nếu xét *I* như *D*-môđun thì hai phần tử bất kì của *I* đều phụ thuộc. Do đó, nếu *I* là môđun tựa tự do thì cơ sở của *I* có thể gồm một phần tử, suy ra *I* là ideal chính của *D* (!). Vậy *I* không là môđun tựa tự do. Như vậy *I* là môđun con của môđun tự do *D* nhưng *I* không là môđun tựa tự do. Hơn thế nữa, ta có kết quả sau:

4.6. Hệ quả

Cho D là miền nguyên. Khi đó, D là miền các ideal chính khi và chỉ khi mọi môđun con của D-môđun tựa tự do là môđun tựa tự do.

Chứng minh:

Giả sử *D* là miền các ideal chính, *M* là một *D*-môđun tựa tự do và $S \cup T$ là một cơ sở chính tắc của *M* trong đó *S* là tập tất cả các phần tử không xoắn trong cơ sở chính tắc. Khi đó $M = \bigoplus_{x\in S} \langle x \rangle \bigoplus_{y\in T} \langle y \rangle$. Ta có môđun con xoắn của M, $M_T = \bigoplus_{y\in T} \langle y \rangle$, là môđun tựa tự do và $M/M_T = \bigoplus_{x\in S} \langle x \rangle$ là môđun tự do.

Bây giờ, giả sử *H* là môđun con của *M*. Khi đó, môđun con xoắn của *H* là $H_T = H \cap M_T$. Vì M_T là môđun tựa tự do nên H_T là môđun tựa tự do (Hệ quả 4.4). Mặt khác, ta có $H/H_T = H/H \cap M_T \cong (H + M_T)/M_T \subset M/M_T$

Vì *D* là miền các ideal chính và M/M_T là môđun tự do nên H/H_T là môđun tự do. Khi đó *H* là tổng trực tiếp của H_T và một môđun con tự do (đẳng cấu với H/H_T) nên *H* là môđun tựa tự do.

Ngược lại, giả sử mọi môđun con của *D*-môđun tựa tự do là môđun tựa tự do và *I* là một ideal khác không của *D*. Khi đó, xem *I* như là một môđun con của *D*-môđun tựa tự do *D*. Theo giả thiết, *I* là môđun tựa tự do. Tuy nhiên, hai phần tử bất kì của *I* đều phụ thuộc. Do đó, cơ sở của *I* chỉ có thể có một phần tử. Bởi vậy, *I* là ideal chính của *D* và *D* là miền các ideal chính.

TÀI LIỆU THAM KHẢO

1. Alaca, S. and Williams, K.S. (2004), *Introductory Algebraic Number Theory*, Cambridge University Press.
2. Atiyah, M.F. and Macdonald, I.G. (1969), *Introduction to Commutative Algebra*, Addison-Wesley publishing company.
3. Cartan, H. and Eilenberg, S. (1956), *Homological Algebra*, Princeton University Press
4. Robinson, J.S. (1996), *A Course in the Theory of Groups*, Springer

(Ngày Tòa soạn nhận được bài: 25-4-2013; ngày phản biện đánh giá: 09-5-2013; ngày chấp nhận đăng: 21-6-2013)