ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

TRƯƠNG BÁ VẤN

P-NHÓM VÀ ỨNG DỤNG TRONG LÝ THUYẾT SỐ

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

TRƯƠNG BÁ VẤN

P-NHÓM VÀ ỨNG DỤNG TRONG LÝ THUYẾT SỐ

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số : 60460113

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. HOÀNG VĂN HÙNG

Thái Nguyên - 2016

Mục lục

LỜI NÓI ĐẦU

Lý thuyết nhóm nói chung và các p-nhóm nói riêng có nhiều áp dụng trong Lý thuyết số. Sở dĩ như vậy vì tập các số nguyên $\mathbf{Z}$ với phép cộng là một nhóm giao hoán. Thương của nhóm ($\mathbf{Z}$,+) cho các nhóm con vô hạn của nó sinh ra các nhóm xyclic hữu hạn. Trong các nhóm thương này nhóm $\mathbf{Z}_p$ (hay $\mathbf{Z}/_p\mathbf{Z}$) với p là số nguyên tố đóng một vai trò đặc biệt quan trọng trong lý thuyết số. Có thể đưa vào $\mathbf{Z}_p$ phép tính nhân giữa các lớp đồng dư theo mođun p một cách tự nhiên với phần tử đơn vị là lớp đồng dư 1(mod p) và mọi lớp đồng dư khác 0(mod p) đều có nghịch đảo trong $\mathbf{Z}_p$. Với hai phép tính cộng và nhân được định nghĩa, tập $\mathbf{Z}_p$ trở thành một trường hữu hạn với p phần tử, tập các phần tử khác 0 của nó được ký hiệu là $\mathbf{Z}_p^*$. Nhờ các đặc điểm vừa nêu, tập $\mathbf{Z}_p$ trở thành một công cụ mạnh để chứng minh nhiều sự kiện về tính chia hết trong Lý thuyết số.

Luận văn "**p-nhóm và ứng dụng trong lý thuyết số**" gồm hai chương. Chương I với tiêu đề **Lý thuyết các p-nhóm** trình bày sơ lược về Lý thuyết nhóm, khái niệm p-nhóm, tác dụng của một nhóm lên một tập và các định lý về p-nhóm con Sylow. Kết quả quan trọng nhất của chương này là công thức về các G-quỹ đạo trong một G-tập, được áp dụng nhiều ở chương II. Chương II với tiêu đề **Ứng dụng lý thuyết các p-nhóm** trong lý thuyết số trình bày chứng minh các định lý: Fermat bé, Wilson, Lucas, Định lý Fermat về tổng hai bình phương, ký hiệu Legendre và luật tương hỗ bậc hai. Định lý Fermat bé và hệ quả của nó là Định lý Wilson được sử dụng trong tất cả các chứng minh của các định lý kể trên (trừ Định lý Lucas). Tác giả trình bày chứng minh Định lý Fermat bé dựa trên Bổ đề Burnside. Khi áp dụng công thức trong bổ đề Burnside cho p-nhóm ta thu được định lý Fermat bé. Việc áp dụng được tiến hành thông qua một hệ quả của Bổ đề Burnside (Mệnh đề 2.1.4). Chứng minh Định lý Lucas dựa trên công thức $\mathrm{C}_{\mathrm{p^r}}^{\mathrm{k}} = 0(\mathrm{mod\,p})$ khi $1 \leq k \leq p^r - 1$, p là số nguyên tố, r là số nguyên dương và khai triển nhị thức Newton trong trường đặc số p. Công thức vừa nêu

được chứng minh dựa trên công thức về các quỹ đạo áp dụng cho p-nhóm có cấp p^r.

Tư liệu được sử dụng trong luận văn này được trích từ các tài liệu tham khảo [1-7].

Tác giả xin chân thành cám ơn các thầy cô thuộc Khoa Toán-Tin - Đại học Khoa học-Đại học Thái Nguyên, vì sự tận tụy của các thầy cô đối với khóa cao học mà tác giả là một trong các học viên. Tác giả cũng bày tỏ lòng cảm ơn sâu sắc đến thầy hướng dẫn, T.S Hoàng Văn Hùng-giảng viên Đại học Hàng Hải Việt Nam, vì sự quan tâm của thầy đến công việc của tác giả trong suốt quá trình chuẩn bị luận văn.

Ngày, 29 tháng 05 năm 2016.

Tác giả

.

Trương Bá Vấn

Chương 1

Lý thuyết các p-nhóm

1.1 Nhóm, đồng cấu và đẳng cấu nhóm

Định nghĩa 1.1.1: Một tập hợp khác rỗng G với một luật hợp thành trong viết theo lối nhân được gọi là một nhóm nếu các tính chất sau được thỏa mãn:
i) $(ab)c = a(bc)$ với mọi $a, b, c \in$ G ;
ii) $\exists e \in$ G có tính chất: $ae = ea = a$ với mọi $a \in$ G;
iii) Với mỗi $a \in G$, tồn tại phần tử $a' \in$ G có tính chất: $aa' = a'a = e$.
Tính chất i) gọi là tính chất kết hợp. Phần tử e trong tính chất ii) được gọi là phần tử trung hòa của G (khi luật hợp thành được viết theo lối nhân ta cũng gọi e là phần tử đơn vị của G, phần tử trung hòa của nhóm với luật hợp thành viết theo lối cộng thường được ký hiệu là 0). Phần tử a' trong tính chất iii) được gọi là phần tử nghịch đảo của a khi luật hợp thành trong trên G được viết theo lối nhân và gọi là phần tử đối của a khi luật hợp thành trong trên G được viết theo lối cộng. Thêm nữa, với mỗi $a \in$ G phần tử nghịch đảo (tương ứng, phần tử đối) của nó là duy nhất và được ký hiệu bởi a^{-1} (tương ứng,$-a$).

Các nhóm có số phần tử hữu hạn được gọi là các nhóm hữu hạn. Số phần tử của một nhóm G được gọi là cấp của G, ký hiệu bởi |G|.

Ví dụ về nhóm: Các tập sau đây cùng với các luật hợp thành trong được chỉ ra là các nhóm:

- Tập hợp các số thực dương $\mathbf{R}^+$ với luật hợp thành trong là phép nhân thông thường. Phần tử đơn vị là 1, nghịch đảo của số dương x là $x^{-1} = \frac{1}{x}$. Ta ký hiệu nhóm này bởi $(\mathbf{R}^+, .)$

- Tập hợp các số nguyên $\mathbf{Z}$ với luật hợp thành trong là phép cộng thông thường. Phần tử trung hòa là số 0. Phần tử đối của số nguyên n là số nguyên -n. Ta ký hiệu nhóm này bởi ký hiệu ($\mathbf{Z}$,+).

- Tập hợp các ma trận vuông thực cấp n có định thức khác 0 với luật hợp thành trong là phép nhân ma trận. Phần tử đơn vị là ma trận đơn vị cấp n. Nghịch đảo của ma trận vuông A là ma trận nghịch đảo A^{-1}. Ta ký hiệu nhóm này bởi $GL(n, R)$.

-Tập hợp các song ánh từ một tập S khác rỗng tùy ý lên chính nó với luật hợp thành trong là phép hợp các ánh xạ là một nhóm gọi là nhóm các phép thế của S, ký hiệu là P(S). Phần tử đơn vị là ánh xạ đồng nhất. Nghịch đảo của song ánh f là ánh xạ ngược của nó f^{-1}. Mỗi song ánh từ S lên chính nó gọi là một phép thế của S.

Định nghĩa 1.1.2: Cho G và G' là hai nhóm với luật hợp thành trong được viết theo lối nhân. Một ánh xạ h từ G vào G' thỏa mãn tính chất: $h(ab) = h(a)h(b)$với mọi $a, b \in$G được gọi là một đồng cấu nhóm từ G vào G'.

Một đồng cấu nhóm từ G vào G' đồng thời là một đơn ánh được gọi là một đơn cấu; một đồng cấu nhóm từ G vào G' đồng thời là một toàn ánh gọi là một toàn cấu; một đồng cấu nhóm từ G vào G' đồng thời là một song ánh gọi là

một đẳng cấu. Nếu có một đẳng cấu nhóm từ G vào G' thì nhóm G gọi là đẳng cấu với nhóm G', hay G và G' đẳng cấu với nhau, ký hiệu G≈G'. Nếu j là một đẳng cấu nhóm từ G lên G' thì ánh xạ ngược j^{-1} là một đẳng cấu nhóm từ G' lên G. Nếu G là một nhóm hữu hạn và G≈G' thì G' cũng là nhóm hữu hạn và |G|=|G'| .

1.2 Nhóm giao hoán và nhóm xyclic

Định nghĩa 1.2.1: Nhóm (G, $*$) được gọi là nhóm giao hoán (hay nhóm Abel) nếu a$*$b=b$*$a với mọi a,b∈G.

Các nhóm ($\mathbf{R}^+$,.), ($\mathbf{Z}$,+), ($\mathbf{R}$,+), là các nhóm giao hoán. Nhóm $GL(n, R)$ là nhóm không giao hoán. Nhóm P(S) không giao hoán nếu S có từ 3 phần tử trở lên.

Định nghĩa 1.2.2: Nhóm (G,.) được gọi là nhóm xyclic nếu tồn tại phần tử a thuộc G sao cho nếu b thuộc G thì tồn tại số nguyên k sao cho $b = a^k$. Phần tử a khi đó được gọi là phần tử sinh của nhóm xyclic G.

- Nhóm ($\mathbf{Z}$,+) là nhóm xyclic với phần tử sinh là 1.

- Đặt S= $\{1, -1\}$. Luật hợp thành trong S là phép nhân thông thường. Khi đó (S,.) là một nhóm xyclic với phần tử đơn vị là 1, phần tử sinh là -1.

- Giả sử d là một số nguyên dương > 1 . Với mọi số nguyên r thỏa mãn $0 \leq$ r $\leq$ d-1 ta ký hiệu $n = r(\mathrm{mod} d)$ nếu có số nguyên k sao cho n = kd+r. Như vậy, với số nguyên n bất kỳ ta sẽ có $n = r(\mathrm{mod}\, d)$ với một số nguyên r nào đó thỏa mãn $0 \leq$ r $\leq$ d-1.Với hai số nguyên m, n đã cho, nếu $m - n = 0(\mathrm{mod} d)$ ta viết $m = n(\mathrm{mod} d)$ và nói m, n thuộc vào cùng một lớp đồng dư theo modun d. Với mỗi số nguyên n

ta ký hiệu $\overline{n}$ là tập tất cả các số nguyên m thỏa mãn $m = n(\mathrm{mod}\, d)$ và gọi $\overline{n}$ là một lớp đồng dư theo modun d. Tập các số nguyên $\mathbf{Z}$ được phân hoạch thành d lớp đồng dư theo modun d là $\overline{0}, \overline{1}, ..., \overline{\mathrm{d}-1}$. Một phần tử của lớp đồng dư $\overline{r}$ được gọi là một đại diện của nó. Ta có các tính chất sau:

i) $m = n(\mathrm{mod}\, d) \& m' = n'(\mathrm{mod}\, d) \Rightarrow m + m' = n + n'(\mathrm{mod}\, d)$;

ii) $m = n(\mathrm{mod}\, d) \& m' = n'(\mathrm{mod}\, d) \Rightarrow mm' = nn'(\mathrm{mod}\, d)$

Ký hiệu $\mathbf{Z}_d = \left\{\overline{0}, \overline{1}, ..., \overline{d-1}\right\}$ là tập các lớp đồng dư theo modun d. Trên $\mathbf{Z}_d$ ta có thể định nghĩa hai phép tính cộng và nhân theo quy tắc sau:

$$\overline{r} + \overline{s} = \overline{r+s}; \quad \overline{r}.\overline{s} = \overline{rs}$$

Khi đó nhóm ($\mathbf{Z}_d$,+)là nhóm xyclic với phần tử sinh là $\overline{1}$, phần tử trung hòa là $\overline{0}$. Cấp của nhóm ($\mathbf{Z}_d$,+) là d. Ký hiệu $\mathbf{Z}_d^* = \left\{\overline{1}, ..., \overline{d-1}\right\}$, nếu d là số nguyên tố thì luật nhân định nghĩa ở trên là một luật hợp thành trong của $\mathbf{Z}_d^*$, với luật hợp thành nhân này $\mathbf{Z}_d^*$ là một nhóm xyclic với phần tử đơn vị là $\overline{1}$. Chứng minh khẳng định này (sẽ được trình bày ở chương sau) là một trong các ứng dụng của lý thuyết các p-nhóm.

1.3 Nhóm con và nhóm con chuẩn tắc

Định nghĩa 1.3.1: Cho (G,$*$) là một nhóm và H là một tập con khác rỗng của G. Nếu luật hợp thành trong $*$ thu hẹp trên H biến H thành một nhóm thì H được gọi là một nhóm con của G.

Mệnh đề 1.3.1: i) Để tập con khác rỗng H của nhóm (G,$*$) là một nhóm con của G điều kiện cần và đủ là với mọi phần tử a, b thuộc H ta có a $*$b thuộc H và a^{-1}

thuộc H;
ii) Giao của một họ tùy ý các nhóm con của G là một nhóm con của G.

Ví dụ:- Nhóm ($\mathbf{Z}$,+) là nhóm con của nhóm ($\mathbf{R}$,+). Nhóm ($\mathbf{R}^+$,.) là nhóm con của nhóm ($\mathbf{R}^*$,.), trong đó R^* là tập các số thực khác 0.

Giả sử H là một nhóm con của nhóm G với luật hợp thành trong viết theo lối nhân, x là một phần tử của G. Tập tất cả các phần tử của G có dạng xy với y là một phần tử của H được ký hiệu là xH và được gọi là một lớp ghép trái theo H trong G. Hai lớp ghép trái theo H trong G hoặc là trùng nhau hoặc là có giao bằng rỗng. Thực vậy, trước hết ta nhận xét rằng nếu u là phần tử của H thì uH=H. Nếu xH và x'H có phần tử chung là z thì có các phần tử y và y' thuộc H sao cho z = xy = x'y'. Suy ra $x' = xyy'^{-1} = xu$ với $u = yy'^{-1}$ thuộc H và x'H=(xu)H=x(uH)=xH. Vậy G được phân hoạch thành các lớp ghép trái theo H trong G. Dễ thấy ánh xạ xu $\rightarrow$ yu là một song ánh từ lớp ghép trái xH lên lớp ghép trái yH. Do đó, nếu G là nhóm hữu hạn thì cấp của G chia hết cho cấp của nhóm con H bất kỳ của nó, nghĩa là |G|:|H| là một số nguyên dương, hay |H| là một ước số của |G|. Lực lượng của tập các lớp ghép trái theo H trong G gọi là chỉ số của nhóm H trong G và ký hiệu bởi |G:H|. Nếu |G| hữu hạn thì |G:H|=|G|:|H| hay |G|=|H| |G:H|. Các lớp ghép phải theo H trong G được định nghĩa tương tự và G cũng được phân hoạch bởi các lớp ghép phải trong G. Nếu H là nhóm con của nhóm không giao hoán G thì xH và Hx có thể khác nhau, nhưng có một song ánh từ tập các lớp ghép trái theo H lên tập các lớp ghép phải theo H cho bởi tương ứng xH $\rightarrow$ Hx.

Định nghĩa 1.3.2: Nhóm con H của nhóm G với luật hợp thành trong viết theo lối nhân được gọi là nhóm con chuẩn tắc của G nếu xH=Hx với mọi x thuộc G.

Đẳng thức xH=Hx tương đương với $xHx^{-1} = H$. Dùng mệnh đề 1.3.1 dễ chứng