KŪNŲ TEORIJA

2000 metų rudens paskaitos

1. Kūnų plėtiniai

2. Galua grupės

3. Polinomų Galua grupės

4. Mažos eilės grupių klasifikacija

Pradėkime nuo grupių, kurių eilė neviršija 15, lentelės.

Eilė	Komutatyvi grupė	Nekomutatyvi grupė
2	$\mathbf{Z}_2$	
3	$\mathbf{Z}_3$	
4	$\mathbf{Z}_4, \mathbf{Z}_2 \times \mathbf{Z}_2$	
5	$\mathbf{Z}_5$	
6	$\mathbf{Z}_6$	S_3
7	$\mathbf{Z}_7$	
8	$\mathbf{Z}_8, \mathbf{Z}_4 \times \mathbf{Z}_2, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$	$\mathcal{D}_4$, Q
9	$\mathbf{Z}_9, \mathbf{Z}_3 \times \mathbf{Z}_3$	
10	$\mathbf{Z}_{10}$	$\mathcal{D}_5$
11	$\mathbf{Z}_{11}$	
12	$\mathbf{Z}_{12}, \mathbf{Z}_6 \times \mathbf{Z}_2$	$\mathcal{A}_4$, $\mathcal{D}_6$, $\mathbf{Z}_3 \bowtie \mathbf{Z}_4$
13	$\mathbf{Z}_{13}$	
14	$\mathbf{Z}_{14}$	$\mathcal{D}_7$
15	$\mathbf{Z}_{15}$	

Mums yra gerai pažįstamos Abelio grupės $\mathbf{Z}_n$. Tai ciklinės adicinės grupės generuotos elementu $1 : \mathbf{Z}_n = \langle 1 \rangle$. Kai n yra pirminis skaičius, tai egzistuoja tik viena n- osios eilės grupė - būtent $\mathbf{Z}_n$.

Parodysime, kad grupės, kurių eilė yra lygi p^2, čia $p-$ pirminis skaičius, yra Abelio grupės.

Grupės G elementas z vadinamas **centriniu**, jeigu $zg = gz$ su visais $g \in G$. Visų grupės G centrinių elementų aibė $Z(G)$ yra pogrupis, vadinamas grupės G **centru.** Viena iš svarbiausių centro savybių yra ta, kad grupės G, kurios eilė yra p^m , čia $p-$ pirminis, centras $Z(G)$ yra netrivialus, t.y. jame yra nevienetiniai elementai.

Teiginys 4.1 *Tegu $G-$ nekomutatyvioji grupė. Tada faktorgrupė $G/Z(G)$ ne ciklinė.*

Įrodymas. Sakykime priešingai, $G/Z(G) = \langle aZ(G) \rangle -$ ciklinė grupė. Tada bet kuris grupės G elementas reiškiamas $a^k z$, čia $z \in Z(G)$. Turime, kad visi tokie elementai yra perstatomi:$\left(a^k z_1\right)\left(a^l z_2\right) = a^k z_1 a^l z_2 = a^k a^l z_2 z_1 = a^l a^k z_2 z_1 = a^l z_2 a^k z_1 = \left(a^l z_2\right)\left(a^k z_1\right)$. Bet tai prieštarauja prielaidai apie grupės G nekomutatyvumą.

Įrodyta.

Teiginys 4.2 *Grupė G, turinti p^2 elementų, yra Abelio grupė.*

Įrodymas. Minėjome, kad grupės G centras $Z(G)$ yra netrivialus, todėl arba $|Z(G)| = p$, arba $|Z(G)| = p^2$. Pirmuoju atveju faktorgrupėje $G/Z(G)$ yra p elementų ir todėl ji yra ciklinė grupė, antruoju atveju faktorgrupėje $G/Z(G)$ yra vienas elementas, t.y. grupė irgi yra ciklinė. Įrodymui baigti pakanka pasinaudoti Teiginiu 4.1.

Įrodyta.

Teorema 4.3 *Tegu $p-$ pirminis skaičius.*

(1) *Egzistuoja tik dvi neizomorfinės grupės, turinčios p^2 elementų:*

$$Z_{p^2} \text{ ir } Z_p \times \mathbf{Z}_p.$$

(2) *Egzistuoja penkios grupės, turinčios p^3 elementų: trys Abelio grupės*

$$Z_{p^3} \ , \ Z_{p^2} \times \mathbf{Z}_p \text{ ir ir } Z_p \times \mathbf{Z}_p \times \mathbf{Z}_p$$

ir dvi nekomutatyvios grupės:
kai $p = 2$, tai

$$\text{diedro grupė } \mathcal{D}_4 = (a, b | a^4 = 1, b^2 = 1, bab = a^{-1}),$$
$$\text{kvaternionų grupė } Q = (a, b | a^4 = 1, b^2 = a, b^{-1}ab = a^{-1});$$

kai $p > 2$, *tai*

$$G_1 = \left(a, b | a^{p^2} = 1, b^p = 1, b^{-1}ab = a^{1+p}\right)'$$
$$G_2 = (a, b, c | a^p = 1, b^p = 1, c^p = 1, [a, b] = c, [a, c] = [b, c] = 1).$$

Dabar apsistokime ties grupėmis, turinčiomis pq, čia p ir $q-$ pirminiai, elementų. Pasinaudosime klasikine L.Silovo teorema.

Teorema 4.4 (Silov) *Tegu* $G-$ *baigtinė grupė, kurios eilė* $|G|$ *dalijasi iš* p^n *ir nesidalija iš* p^{n+1}, *čia* $p-$ *pirminis.*

(1) *Su kiekvienu* $r \leq n$ *egzistuoja grupės* G *pogrupis, kurio eilė yra* p^r.

(2) *Pogrupių, kurių eilė yra* p^n *(šie pogrupiai vadinami Silovo* $p-$ *pogrupiais), skaičius lygsta* $1(\mathrm{mod}\, p)$ *ir dalija* $|G|$.

Nagrinėkime grupę G, kurios eilė $|G| = pq$, čia p ir $q-$ pirminiai ir $p < q$. Silovo $p-$ ir $q-$ grupės G pogrupiai, t.y pogrupiai, kurių eilės yra p ir q, yra cikliniai. Tegu (a) ir (b) yra šie Silovo pogrupiai: $|(a)| = p$ ir $|(b)| = q$. Iš Silovo teoremos matome, kad Silovo $q-$ pogrupių skaičius yra lygus $1 + kq$ ir yra pq daliklis. Taigi, Silovo $q-$ pogrupis yra vienintėlis $-$ tai pogrupis (b). Tai normalusis pogrupis. Iš Silovo teoremos taip pat matome, kad Silovo $p-$ pogrupių skaičius yra lygus $1 + kp$ ir yra q daliklis. Šiuo atveju galimi du variantai:

1. (i) Silovo $p-$ pogrupis (a) yra vienintėlis. Tada jis yra normalusis ir $G = (ab)$, t.y. $G \approx Z_{pq}$.

(ii) Yra q Silovo $p-$ pogrupių. Tai teisinga tik tada, kada $q \equiv 1\, (\mathrm{mod}\, p)$. Kadangi (b) normalusis pogrupis, tai $a^{-1}ba \in (b)$, t.y. $a^{-1}ba = b^r$:

$\alpha)$ jeigu $r = 1$, tai $G = (ab)$ ir $G \approx Z_{pq}$.

$\beta)$ jeigu $r \neq 1$, tai $r^p \equiv 1\, (\mathrm{mod}\, q)$, $r \not\equiv 1\, (\mathrm{mod}\, q)$ ir sandaugos formulė $a^x b^y \cdot a^z b^t = a^{x+z} b^{yr^z + t}$ apibrėžia nekomutatyvią pq eilės grupę G.

Gavome, kad yra galimi tik du pq eilės grupių tipai: tai komutatyvi grupė Z_{pq} ir nekomutatyvi grupė, kai $q \equiv 1\, (\mathrm{mod}\, p)$.

Pavyzdys. Tegu $p = 2$, $q = 3$. Turime $3 \equiv 1\, (\mathrm{mod}\, 2)$. Gerai mums žinomos 6-os eilės grupės: komutatyvi Z_6 ir nekomutatyvi S_3, ir sudaro visą grupių, kurių eilė lygi 6, sąrašą.

Dabar aptarkime grupes, turinčias p^2q elementų, čia $p, q-$ pirminiai skaičiai. Pradėsime apibrėžimu.

Apibrėžimas 4.5 *Tegu $G-$ grupė, o A ir B – tokie jos pogrupiai, kad*
(i) *A ir B yra normalieji G pogrupiai;*
(ii) $A \cap B = \langle e \rangle$;
(iii) $A \cdot B = G$.
Tada grupę G vadina pogrupių A ir B vidine tiesiogine sandauga: $G = A \bowtie B$

Pavyzdys. Simetrinė grupė S_3 yra savo normaliųjų pogrupių $B = \{\mathrm{id},\ (12)\}$ ir $A = \{\mathrm{id},\ (123), (132)\}$ vidinė tiesioginė sandauga : $G = A \bowtie B$.

Teorema 4.6 *Tegu $G-$ grupė, turinti p^2q elementų, čia p ir $q-$ pirminiai. Tada G yra savo Silovo pogrupių vidinė tiesioginė sandauga.*

Teorema 4.7 $12-$ *osios eilės nekomutatyvioji grupė yra izomorfinė arba $\mathcal{A}_4$, arba $\mathcal{D}_6$, arba $Z_3 \bowtie Z_4$.*

Įrodymas. Tegu $G-$ grupė ir $|G| = 12$. Silovo $2-$ pogrupis yra izomofinis arba $\mathbf{Z}_4$, arba $\mathbf{Z}_2 \times \mathbf{Z}_2$, o Silovo $3-$ pogrupis yra izomorfinis $\mathbf{Z}_3$. Išnagrinėkime visas galimas vidines tisiogines šių pogrupių sandaugas.
(i) $\mathbf{Z}_4 \bowtie \mathbf{Z}_3$ yra izomorfinė $\mathbf{Z}_4 \times \mathbf{Z}_3 \approx \mathbf{Z}_{12}$.
(ii) $(\mathbf{Z}_2 \times \mathbf{Z}_2) \bowtie \mathbf{Z}_3$ yra izomorfinė $\mathcal{A}_4$.
(iii) $\mathbf{Z}_3 \bowtie (\mathbf{Z}_2 \times \mathbf{Z}_2)$ yra izomorfinė $\mathcal{D}_6$.
(iv) $\mathbf{Z}_3 \bowtie \mathbf{Z}_4$ yra taip vadinama "T" grupė.
Įrodyta.

Kai kurių baigtinių grupių veiksmų lentelės.

$\mathcal{D}_4$:

·	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	e	f	g
c	c	d	a	b	g	h	e	f
d	d	a	b	c	f	g	h	e
e	e	f	g	h	a	b	c	d
f	f	g	h	e	d	a	b	c
g	g	d	e	f	c	d	a	b
h	h	e	f	g	b	c	d	a

Q:

·	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	e	f	g
c	c	d	a	b	g	h	e	f
d	d	a	b	c	f	g	h	e
e	e	f	g	h	c	d	a	b
f	f	g	h	e	b	c	d	a
g	g	h	e	f	a	b	c	d
h	h	e	f	g	d	a	b	c

$\mathcal{D}_5$:

·	a	b	c	d	e	f	g	h	i	j
a	a	b	c	d	e	f	g	h	i	j
b	b	c	d	e	a	j	f	g	h	i
c	c	d	e	a	b	i	j	f	g	h
d	d	e	a	b	c	h	i	j	f	g
e	e	a	b	c	d	g	h	i	j	k
f	f	g	h	i	j	a	b	c	d	e
g	g	h	i	j	f	e	a	b	c	d
h	h	i	j	f	g	d	e	a	b	c
i	i	j	f	g	h	c	d	e	a	b
j	j	f	g	h	i	b	c	d	e	a

$\mathcal{D}_6$:

·	a	b	c	d	e	f	g	h	i	j	k	l
a	a	b	c	d	e	f	g	h	i	j	k	l
b	b	c	d	e	f	a	l	g	h	i	j	k
c	c	d	e	f	a	b	k	l	g	h	i	j
d	d	e	f	a	b	c	j	k	l	g	h	i
e	e	f	a	b	c	d	i	j	k	l	g	h
f	f	a	b	c	d	e	h	i	j	k	l	g
g	g	h	i	j	k	l	a	b	c	d	e	f
h	h	i	j	k	l	g	f	a	b	c	d	e
i	i	j	k	l	g	h	e	f	a	b	c	d
j	j	k	l	g	h	i	d	e	f	a	b	c
k	k	l	g	h	i	j	c	d	e	f	a	b
l	l	g	h	i	j	k	b	c	d	e	f	a

$\mathbf{Z}_3 \bowtie \mathbf{Z}_4$:

·	a	b	c	d	e	f	g	h	i	j	k	l
a	a	b	c	d	e	f	g	h	i	j	k	l
b	b	c	d	e	f	a	l	g	h	i	j	k
c	c	d	e	f	a	b	k	l	g	h	i	j
d	d	e	f	a	b	c	j	k	l	g	h	i
e	e	f	a	b	c	d	i	j	k	l	g	h
f	f	a	b	c	d	e	h	i	j	k	l	g
g	g	h	i	j	k	l	d	e	f	a	b	c
h	h	i	j	k	l	g	c	d	e	f	a	b
i	i	j	k	l	g	h	b	c	d	e	f	a
j	j	k	l	g	h	i	a	b	c	d	e	f
k	k	l	g	h	i	j	f	a	b	c	d	e
l	l	g	h	i	j	k	e	f	a	b	c	d

$\mathcal{D}_7$:

·	a	b	c	d	e	f	g	h	i	j	k	l	m	n
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n
b	b	c	d	e	f	g	a	n	h	i	j	k	l	m
c	c	d	e	f	g	a	b	m	n	h	i	j	k	l
d	d	e	f	g	a	b	c	l	m	n	h	i	j	k
e	e	f	g	a	b	c	d	k	l	m	n	h	i	j
f	f	g	a	b	c	d	e	j	k	l	m	n	h	i
g	g	a	b	c	d	e	f	i	j	k	l	m	n	h
h	h	i	j	k	l	m	n	a	b	c	d	e	f	g
i	i	j	k	l	m	n	h	g	a	b	c	d	e	f
j	j	k	l	m	n	h	i	f	g	a	b	c	d	e
k	k	l	m	n	h	i	j	e	f	g	a	b	c	d
l	l	m	n	h	i	j	k	d	e	f	g	a	b	c
m	m	n	h	i	j	k	l	c	d	e	f	g	a	b
n	n	h	i	j	k	l	m	b	c	d	e	f	g	a

Visų grupių, kurių eilė neviršija 15, veiksmo lenteles galima rasti tinklo adresu: http://math.ucsd.edu/˜ jwavrik/Groups15/Groups15.html