16 Dodatek A (pomembni rezultati)

Grupa. Red grupe. Red elementa.

1. V grup je enota enolično določena edinstvena.
2. V grupi je inverz elementa enolično določen.
3. Če je $(G, \cdot)$ grupa, potem je $(a^{-1})^{-1} = a \ \ \forall a \in G$.
4. Če je $(G, \cdot)$ grupa, potem je $(ab)^{-1} = b^{-1}a^{-1} \ \ \forall a, b \in G$.
5. Če je $(G, \cdot)$ grupa in $ab = ac$, potem je $b = c$.
6. Če je $(G, \cdot)$ grupa in $ba = ca$, potem je $b = c$.
7. V končni grupi je red vsakega elementa končan in ne more biti večji od reda grupe.
8. V grupi je red elementa in njegovega inverza isti.

Podgrupe.

1. Če je H podgrupa grupe G potem

   (i) Je identiteta podgrupe H in grupe G ista.

   (ii) Je inverz elementa v podgrupi H glede na grupo H in G isti.

   (iii) Je red elementa v podgrupi H glede na grupo H in G isti.
2. Naj bo G grupa z binarno operacijo množenja. Podmnožica H grupe G je podgrupa grupe G če velja eden od naslednji ekvivalentnih pogojev:

   (a) $ab \in H$, $a^{-1} \in H \ \ \forall a, b \in H$

   (b) $ab^{-1} \in H \ \ \forall a, b \in H$

   Če je H končna je H podgrupa grupe G, če je $ab \in H \ \ \forall a, b \in H$.
3. Presek dveh podgrup grupe je tudi podgrupa grupe.

Homomorfizmi. Izomorfizmi.

1. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(e) = e'$.
2. Če je ϕ homomorfizem iz grupe G v grupo G' potem $\phi(a^{-1}) = [\phi(a)]^{-1} \ \ \forall a \in G$.
3. Če je ϕ izomomorfizem iz grupe G v grupo G' potem $o(a) = o[\phi(a)] \ \ \forall a \in G$.
4. Naj bo $\phi : G \to G'$ surjektivni homomorfizem. Potem je homomorfizem ϕ izomorfizem iz grupe G v grupo G' če in samo če $\ker(\phi) = \{e\}$.

Permutacijske grupe.

1. Množica S_A vseh permutacij neprazne množice A je grupa glede na operacijo kompozicije funkcij.
2. Vsaka grupa je izomorfna neki permutacijski grupi (Cayley).
3. Vsaka permutacija se lahko napiše kot produkt transpozicij.
4. Množica vseh sodih permutacij končne množice je grupa glede na operacijo kompozicije funkcij.

Odseki in Lagrangeov izrek.

1. Če je H podgrupa grupe G, potem sta vsaka dva desna (ali leva) odseka podgrupe H v grupi G enaka ali disjunktna.
2. Če je H podgrupa grupe G, potem obstaja bijektivna korespodenca med vsakima dvema desnima (ali levima) odsekoma podgrupe H v grupi G.
3. Če je H podgrupa grupe G, potem je unija vseh desnih (ali levih) odsekov podgrupe H v grupi G enaka grupi G.
4. Če je H podgrupa grupe G, potem desni (ali levi) odseki podgrupe H v grupi G porodio particijo grupe G.
5. **Lagrangeov izrek**. Red vsake podgrupe končne grupe deli red grupe.
6. Če je G končna grupa glede na operacijo množenja potem je $a^{o(G)} = e \ \forall a \in G$.

Podgrupe edinke.

1. Podgrupa N grupe G glede na operacijo množenja je edinka v grupi G če in samo če $gNg^{-1} = N$ $\forall g \in G$.
2. Podgrupa N grupe G je edinka v grupi G če in samo če je produkt dveh desnih odsek (podgrupe N v grupi G) spet desni odsek (podgrupe N v grupi G).
3. Produkt dveh edink grupe je tudi edinka grupe.
4. Presek dveh edinke grupe je tudi edinka grupe.
5. Če je ϕ homomorfizem iz grupe G v grupo G', potem je jedro homomorfizma ϕ edinka v grupi G.
6. Naj bo N edinka v grupi G glede na opearcijo množenja. Če je $\phi : G \to G/N$ definiran z $\phi(g) = Ng$, za $g \in G$, potem je ϕ surjektivni homomorfizem iz grupe G v grupo G/N. Jedro homomorfizma ϕ je N.
7. Če je ϕ surjektivni homomorfizem iz grupe G v grupo G', potem je $G/\ker(\phi) = G'$.

Ciklične grupe.

1. Vsaka ciklična grupa je abelska.
2. Če je a generator ciklične grupe G, potem je a^{-1} tudi generator grupe G.
3. Če končna grupa reda n vsebuje element reda n, potem je ta grupa ciklična.
4. Vsaka grupa praštevilskega reda je ciklična.
5. V vsaki grupi sestavljenega reda obstaja prava podgrupa.
6. Naj bo G ciklična grupa generirana z elementom $a \in G$ in naj bo $o(a) = n$. Za $m < n$, je element a^m generator grupe G če in samo če $\gcd(m, n) = 1$.
7. Vsaka podgrupa ciklične grupe je ciklična.
8. Vsaka neskončna ciklična grupa ima natanko dva generatorja.
9. Vsaka prava podgrupa neskončne ciklične grupe je neskončna.

Center. Normalizator elementa.

1. Relacija konjugiranosti na grupi je ekvivalenčna relacija na grupi G in pripadajoči ekvivalenčni razredi porode particijo grupe G v medsebojno disjunktne ekvivalenčne razrede, ki jih imenujemo razredi konjugiranosti.
2. Normalizator $N(a)$ elementa a v grupi G je podgrupa grupe G.
3. Če je G končna grupa, potem je $o(G) = \sum_a \frac{o(G)}{o(N(a))}$, kjer vsota teče po elementih a, ki so predstavniki razredov konjugiranosti.
4. Center grupe G je edinka v grupi G.
5. Število razredov konjugiranosti ne-abelskih grup reda p^3, kje je p praštevilo, je $p^2 + p - 1$.
6. Če je G končna grupa, potem je $o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$, kjer vsota teče po elementih a, ki so predstavniki razredov konjugiranosti, ki vsebujejo več kot en element.
7. Naj bo G grupa in naj bo $Z(G)$ center grupe G. Če je $G/Z(G)$ ciklična grupa, potem je G abelska.

Notranji automorfizem. Grupa automorfizmov.

1. Naj bo f automorfizem grupe G. Če je H podgrupa grupe G, potem je $f(H)$ tudi podgrupa grupe G.
2. Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.
3. Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.
4. Množica $\mathrm{Inn}(G)$ vseh notranjih automorfizmov grupe G je edinka grupe $\mathrm{Aut}(G)$ (vseh automorfizmov grupe G).
5. Za vsako grupo G je $G/Z(G)$ izomorfna z $\mathrm{Inn}(G)$ (kjer je $Z(G)$ center grupe G).

Delovanje grupe na množici.

1. Naj G deluje na množici X. Za poljuben element $x \in X$ je stabilizator G_x elementa x podgrupa grupe G.
2. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Potem je $G_{gx} = gG_xg^{-1}$. Še več, če je H neka neprazna množica, potem je $G_{gH} = gG_Hg^{-1}$.
3. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Če je $gx = y$ in $T = \{t \in G \mid tx = y\}$, potem je $T = gG_x$.
4. **(Orbita-stabilizator izrek).** Naj bo X G-množica in naj bo $x \in X$. Potem je $|Gx| = [G : G_x]$. Če je G končna, potem je $|Gx|$ deljitelj od $|G|$. Poleg tega
$$|G| = |Gx| \cdot |G_x|.$$
5. Množica orbit pri delovanju grupe G na množici X predstavlja razbitje (oz. particijo) množice X (različne orbite so disjunktne).

Izreki Sylowa.

1. **(Cauchijev izrek za abelske grupe).** Naj bo G končna abelska grupa in naj p deli $o(G)$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$.
2. **(Cauchijev izrek).** Naj bo G končna grupa in naj p deli $o(G)$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$ (obstaja element reda p).
3. **(Prvi izrek Sylowa).** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem za vsak i $(1 \leq i \leq k)$, G vsebuje najmanj eno podgrupo reda p^i.
4. Končna grupa G je p-grupa če in samo če je $o(G)$ enak potenci števila p.
5. Relacija konjugiranosti na množici vseh nepraznih podmnožic grupe je ekvivalenčna relacija.
6. Relacija konjugiranosti na množici vseh podgrup grupe je tudi ekvivalenčna relacija.
7. Naj bo G grupa. Za poljubno neprazno podmnožico S grupe G, je normalizator $N(S)$ množice S podgrupa grupe G.
8. Če je G končna grupa in $S \subseteq G$ $(S \neq \emptyset)$ potem je $o(C(S)) = \dfrac{o(G)}{o(N(S))}$.
9. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x, y \in G$ sta dvojna odseka HxK in HyK bodisi enaka, bodisi disjunktna.
10. Naj bosta H in K dve (ne nujno različni) podgrupi končne grupe G. Za $x \in G$ je $o(HxK) = \dfrac{o(H)\, o(K)}{o((x^{-1}Hx) \cap K)}$.
11. **(Frobenius).** Če sta H in K dve (ne nujno različni) podgrupi končne grupe G, potem je $o(G) = \sum \dfrac{o(H)o(K)}{o((x^{-1}Hx) \cap K)}$ kjer vsota (na desni strani) teče po elementih x, ki so predstavniki dvojnih odsekov HyK.
12. **(Drugi izrek Sylowa).** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem sta vsaki dve podgrupi reda p^k konjugirani.
13. **(Tretji izrek Sylowa).** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem je število podgrup reda p^k oblike $1 + mp$, kjer je m neko ne-negativno celo število. Velja tudi $1 + mp$ deli $o(G)$.

Direktni produkt grup.

1. **(Direktni produkt grup).** Naj bodo $G_1, G_2, ..., G_n$ grupe. Za $(a_1, a_2, ..., a_n)$ in $(b_1, b_2, ..., b_n)$ v $\prod_{i=1}^{n} G_i$ definirajmo operacijo množenja po komponentah $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$. Potem je $\prod_{i=1}^{n} G_i$ skupaj s to operacijo grupa, ki jo imenujemo direktni produkt grup G_i.
2. **(Red elementa v direktnem produktu).** $|(g_1, g_2, ..., g_n)| = \operatorname{lcd}(|g_1|, |g_2|, ..., |g_n|)$
3. **(Kriterij, da je $G \times H$ ciklična).** Naj bosta G in H končni ciklični grupi. Potem je $G \times H$ ciklična, če in samo če sta $|G|$ in $|H|$ tuji števili.
4. **(Fundamentalni izrek o končno generiranih abelskih grupah)** Vsaka končna abelska grupa G je izomorfna direktnemu produktu cikličnih grup v obliki $\mathbb{Z}_{{p_1}^{\alpha_1}} \times \mathbb{Z}_{{p_2}^{\alpha_2}} \times ... \times \mathbb{Z}_{{p_k}^{\alpha_k}}$ kjer so p_i praštevila (ki niso nujno različna) in $\alpha_i \in \mathbb{N}$.

1

Preliminaries

1. INTRODUCTION

This appendix contains some of the very important definitions and results. These results would be used very frequently in our present course. The readers are strongly advised to remember the contents of this chapter.

2. BINARY OPERATION

Let S be a non-empty set. A function from S × S into S is called a **binary operation** on S. Thus, if '*' is a binary operation on S, then it means that '*' is a function from S × S into S.

If $(a, b) \in S \times S$, then the image $*(a, b)$ of (a, b) under the binary operation '*' is written as $a * b$.

3. GROUP

A non-empty set G with a binary operation, denoted by '.', is called a **group** if :

(*i*) $x \,.\, (y \,.\, z) = (x \,.\, y) \,.\, z \quad \forall\, x, y, z \in G$

(*ii*) There exists $e \in G : x \,.\, e = x = e \,.\, x \quad \forall\, x \in G$

e is called the **identity** of G.

(*iii*) For $x \in G$, there exists $y \in G : x \,.\, y = e = y \,.\, x$

y is called the **inverse** of x. The inverse of x is written as x^{-1}.

If in addition, we have

(*iv*) $x \,.\, y = y \,.\, x \quad \forall\, x, y \in G$,

then G is called a **commutative group.** A commutative group is also called an **abelian group** after the famous Norwegian mathematician **N.H. Abel.** A group is called **non-commutative** or **non-abelian** if it is not commutative.

If the binary operation of a group is written as '+', then we write

(*i*) $x + (y + z) = (x + y) + z \quad \forall\, x, y, z \in G$

(*ii*) $\exists\, e \in G : x + e = x = e + x \quad \forall\, x \in G$

(*iii*) For $x \in G$, $\exists\, y \in G : x + y = e = y + x$

And for commutativity, $x + y = y + x \quad \forall\, x, y \in G$.

Remark 1. The binary operation '+' used above has got nothing to do with the ordinary addition of numbers. In fact *, +, . are just symbols representing binary operations.

Remark 2. In order to show a non-empty set G with a given binary operation to be a group, we should verify all the three conditions given above.

4. ORDER OF A GROUP

If the number of elements in a group is finite, the group is said to be a **finite group,** otherwise an **infinite group.** The number of elements in a finite group is called the **order of the group.**

If a group G is finite and has n elements, then we write $o(G) = n$.

5. ORDER OF AN ELEMENT

Let (G, .) be a group with identity element e. For $a \in G$, if there exists a smallest natural number m such that $a^m = e$, then m is called the **order** of a and write $o(a) = m$.

If no such natural number exists then we say that a is of **infinite order.**

IMPORTANT RESULTS

1. *In a group, identity element is unique.*
2. *In a group, every element has unique inverse.*
3. *If (G, .) is a group, then* $(a^{-1})^{-1} = a \quad \forall\, a \in G$.
4. *If (G, .) is a group, then* $(a \,.\, b)^{-1} = b^{-1} \,.\, a^{-1} \quad \forall\, a, b \in G$.
5. *If (G, .) is a group and* $a \,.\, b = a \,.\, c$, *then* $b = c$.
6. *If (G, .) is a group and* $b \,.\, a = c \,.\, a$, *then* $b = c$.
7. *For a finite group, the order of every element is finite and cannot exceed the order of the group.*
8. *In a group, the order of an element and its inverse are same.*

6. HOMOMORPHISM

A mapping ϕ from a group G into a group G′ is called a **homomorphism** of G into G′ if $\phi(ab) = \phi(a)\,\phi(b) \quad \forall\, a, b \in G$.

If binary operation in G is $*$ then ab stands for $a * b$ and if the binary operation in G′ is $*'$, then $\phi(a) *' \phi(b)$ is written briefly $\phi(a)\,\phi(b)$.

7. KERNEL OF A HOMOMORPHISM

If ϕ is a homomorphism of group G into group G′, then the set

$$\{a \in G : \phi(a) = \text{identity element of } G'\}$$

is called the **kernel of the homomorphism** ϕ and write **ker** ϕ.

Since $\phi(e) = e'$, so $e \in \ker \phi$.

$\therefore$ ker ϕ is always a non-empty set.

8. ISOMORPHISM

A mapping ϕ from a group G into a group G′ is called an **isomorphism** of G into G′ if

(*i*) ϕ is a homomorphism *i.e.*, $\phi(ab) = \phi(a)\,\phi(b) \quad \forall\, a, b \in G$

(*ii*) ϕ is one-one.

Remark. If $\phi : G \to G'$ is a mapping and we write $\phi(ab) = \phi(a)\,\phi(b)$, then it should be clearly understood that :

(*i*) ab is that element of the group G which is obtained by applying the binary operation of G on the ordered pair $(a, b) \in G \times G$.

(*ii*) $\phi(a)\,\phi(b)$ is that element of the group G′ which is obtained by applying the binary operation of G′ on the ordered pair $(\phi(a), \phi(b)) \in G' \times G'$.

9. ISOMORPHIC GROUPS

Two groups G and G′ are called **isomorphic groups** if there exists an isomorphism of G onto G′. If groups G and G′ are isomorphic groups then we write $G \simeq G'$.

Remark. If groups G and G′ are isomorphic then there may exist one or more than one isomorphism from G onto G′.

IMPORTANT RESULTS

1. *If ϕ is a homomorphism of group G into group G′, then $\phi(e) = e'$.*
2. *If ϕ is a homomorphism of group G into group G′, then*
$$\phi(a^{-1}) = [\phi(a)]^{-1} \quad \forall\, a \in G.$$
3. *If ϕ is an isomorphism of a group G into group G′, then*
$$o(a) = o[\phi(a)] \quad \forall\, a \in G.$$
4. *Let $\phi : G \to G'$ be a homomorphism. The homomorphism ϕ is an isomorphism of G into G′ if and only if ker $\phi = \{e\}$.*

10. COMPLEX

Let (G, .) be a group. A non-empty subset H of G is called a **complex** of the group (G, .).

11. SUBGROUP

Let (G, .) be a group. A non-empty subset H of G is called a **subgroup** of the group (G, .), if under the binary operation '.' of G, the set H itself forms a group.

$\therefore$ By definition, every subgroup of G is a complex of G but a complex of G may not be a subgroup of G.

Since every set is a subset of itself, so if (G, .) is a group, then G is a subgroup of (G, .).

If 'e' is identity element of group G, then the set $\{e\}$ is also a subgroup of G.

The subgroups $\{e\}$ and G are called **trivial subgroups** of the group G.

$\therefore$ Every group has at least one subgroup.

Remark 1. In practice we generally write $a \,.\, b$ as ab. In other words, ab denotes the element of the group G when the binary operation '.' of G is applied on the ordered pair (a, b). If binary operation on G is $*$, then ab represents $a * b$.

Remark 2. If a non-empty subset H of group G is a group under some other binary operation on H and not with the binary operation of G, then H cannot be said a subgroup of G.

IMPORTANT RESULTS

1. *If H is a subgroup of a group G, then*
   (*i*) *the identity element of H and G are same.*
   (*ii*) *the inverse of an element of H w.r.t. H and G are same.*
   (*iii*) *the order of an element of H w.r.t. H and G are same.*
2. *Let G be a group with binary operation denoted multiplicatively. A complex H of G is a subgroup of G if*
   either $ab \in H, a^{-1} \in H \quad \forall\, a, b \in H$
   or $ab^{-1} \in H \quad \forall\, a, b \in H$
   or $ab \in H \quad \forall\, a, b \in H$, *provided H is finite.*
3. *Intersection of two subgroups of a group is also a subgroup of the group.*

12. COSETS

Let G be a group with binary operation denoted multiplicatively. Let H be a subgroup of G.

For $a \in G$, we define $Ha = \{ha : h \in H\}$.

Ha is called a **right coset** of H in G generated by a.

Similarly, $aH = \{ah : h \in H\}$ is called a **left coset** of H in G generated by a.

$Ha \neq \phi$ because $a = ea \in Ha$. Also $ha \in Ha$ implies $ha \in G$.

$\therefore$ Ha is a complex of G. Similarly, aH is a complex of G.

If G is an abelian group, then we have $Ha = aH$, because $ha = ah \quad \forall\, h \in H$.

H itself is also a right (and left) coset of G because $He = H = eH$.

Remark. If the binary operation of G is denoted additively, then right coset of H in G generated by a is given by $H + a = \{h + a : h \in H\}$.

Also $a + H = \{a + h : h \in H\}$.

IMPORTANT RESULTS

1. *If H is any subgroup of a group G, then any two right (or left) cosets of H in G are either equal or disjoint.*
2. *If H is any subgroup of a group G, then there is one-one correspondence between any two right (or left) cosets of H in G.*
3. *If H is any subgroup of a group G, then the union of all right (or left) cosets of H in G is equal to G.*
4. *If H is any subgroup of a group G, then the right (or left) cosets of H in G partitions the group G.*
5. **Lagrange's theorem.** *The order of each subgroup of a finite group divides the order of the group.*
6. *If G is a finite group with binary operation denoted multiplicatively, then* $a^{o(G)} = e \quad \forall\, a \in G$.

13. NORMAL SUBGROUP

Let G be a group with binary operation denoted multiplicatively. A subgroup N of the group G is called a **normal subgroup** of G if

$$gng^{-1} \in N \quad \forall\, n \in N \text{ and } g \in G.$$

Examples 1. Every subgroup of an abelian group G is a normal subgroup of the group G.

2. If G is any group, then the subgroups $\{e\}$ and G of G are normal subgroups of G. A group not having any normal subgroup except for $\{e\}$ and itself is called a **simple group.**

IMPORTANT RESULTS

1. *A subgroup N of a group G, with binary, operation denoted multiplicatively, is normal if and only if* $gNg^{-1} = N \quad \forall\, g \in G$.
2. *A subgroup N of a group G is a normal subgroup of G if and only if the product of any two right cosets of N in G is again a right coset of N in G.*

3. *The product of two normal subgroups of a group is also a normal subgroup of the group.*
4. *The intersection of two normal subgroups of a group is also a normal subgroup of the group.*
5. *If ϕ is a homomorphism of a group G into group G' then the kernel of ϕ is a normal subgroup of G.*
6. *Let N be a normal subgroup of a group G with binary operation denoted multiplicatively. If $\phi : G \to G/N$ be defined by $\phi(g) = Ng$, for $g \in G$ then ϕ is a homomorphism of G onto G/N and with kernel equal to N.*
7. *If ϕ is a homomorphism of a group G onto a group G', then $G/\ker \phi \simeq G'$.*

14. CYCLIC GROUP

A group G is called a **cyclic group** if there exists an element a in G such that every element of G is of the form a^n, where n is an integer. The element a is called a **generator** of G and we write $G = (a)$.

If the cyclic group G is generated by a ($\in$ G) then the elements of G are of the form :

$$....., a^{-3}, a^{-2}, a^{-1}, a^0(= e), a^1, a^2, a^3, ...$$

Some of these elements may be equal of each other.

A cyclic group may also have more than one generator *i.e.*, a generator of a cyclic group is not unique.

Also, a cyclic group may have any number of elements.

IMPORTANT RESULTS

1. *Every cyclic group is abelian.*
2. *If a is a generator of a cyclic group G then a^{-1} is also a generator of G.*
3. *If a finite group of order n contains an element of order n, then the group must be cyclic.*
4. *Every group of prime order is cyclic.*
5. *Every group of composite order has proper subgroups.*
6. *Let G be a cyclic group generated by an element a of G and $o(a) = n$. For $m < n$, the element a^m is a generator of G if and only if $(m, n) = 1$.*
7. *Every subgroup of a cyclic group is cyclic.*
8. *Every infinite cyclic group has exactly two generators.*
9. *Every proper subgroup of an infinite cyclic group is infinite.*

15. PERMUTATION

Let S be any non-empty set. A one-one mapping of S onto itself is called a **permutation** of S.

The set of all permutations of set S is denoted by A(S).

IMPORTANT RESULTS

1. *The set A(S) of all permutations of a non-empty set S is a group with composition of mappings as the binary operation.*
2. *Every group is isomorphic to a permutation group (Cayley).*
3. *Every permutation can be expressed as a product of transpositions.*
4. *The set of even permutations on a finite set is a group with composition of mappings as the binary operation.*