*These are notes + solutions to herstein problems(second edition TOPICS IN ALGEBRA) on groups,subgroups and direct products.It is a cute pdf print of a MS word doc which explains er..:P

<u>Group theory</u>

Group: closure,associative,identity,inverse

a' denotes inverse of a

<u>identity is unique</u>:

Let e,e' be two identity elements
e.e'=e (e' is identity)
e.e'=e' (e is identity)
e=e'

<u>unique inverse</u>:

let a,a' be two inverses of b
a.b=e=b.a=a'.b=b.a'
(a.b).a'=e.a'=a'
a.(b.a')=a.e=a
a=a'

<u>(a')'=a</u>:

a'.(a')'=e
a'.a=e

<u>(a.b)'=b'.a'</u>:

(a.b).b'.a'=a.(b.b').a'=a.a'=e

Problems (some preliminary lemmas on grp theory): (Pg 35 Herstein)

1)See whether group axioms hold for the following:

a)G=Z a.b=a-b
associativity fails: (4-3)-1=0,4-(3-1)=2

b)G=Z+ a.b=a*b
inverse may not exist:
2' doesn't exist

c)G=$a_0,a_1,..a_6$ where $a_i.a_j=a_{i+j}$ (i+j)<7
$a_i.a_j=a_{i+j-7}$ (i+j)>=7

It is a group
Closure satisfied by definition
$(a_i.a_j).a_k$:

If i+j<7
If i+j+k>=7
$=a_{i+j+k-7}$
(if j+k<7,ai.$(a_j.a_k)=a_i.a_{j+k}$ and done)
(if j+k>=7,$a_i.(a_j.a_k)=a_i.a_{j+k-7}$ but note that \
i+j+k-7<7 as i+j<7 and so done)
If i+j+k<7 (=>j+k<7,so $a_i.(a_j.a_k)=a_{i+j+k}$)
$=a_{i+j+k}$

If i+j>=7
If i+j+k-7>=7
$=a_{i+j+k-14}$

(j+k cant be less than 7 and so done)

If i+j+k-7<7

$=a_{i+j+k-7}$

(if j+k>=7.done..If j+k<7,note as i+j>=7.done)

Indentity:a_0

Inverse:

$a_i' = a_{7-i}'$

d)G=rational numbers with odd denominators, a.b=a+b

it is a group

2)PT if G is abelian, then $(a.b)^n = a^n.b^n$

By induction assume $(a.b)^{n-1}=a^{n-1}b^{n-1}$

$(a.b)^n=a^{n-1}b^{n-1}.(a.b)=a^n.b^n$

3)PT if $(a.b)^2=a^2.b^2$ for all a,b, G is abelian

$(a.b).(a.b)=a^2b^2$

Cancelling we get b.a=a.b

4)If G is a group such that $(a.b)^i=a^i.b^i$ for 3 consecutive integers for all a,b.PT G is abelian

$(a.b)^i=a^i.b^i,(a.b)^{i+1}=a^{i+1}.b^{i+1},(a.b)^{i+2}=a^{i+2}.b^{i+2}$

$a^{i+2}.b^{i+2}=(a.b)^{i+2}=(a.b)^{i+1}(a.b)=a^{i+1}.b^{i+1}(a.b)$

$a.b^{i+1}=b^{i+1}.a$

$(a.b)^i(b.a)=a^i.b^i.(b.a)=a^i.b^{i+1}.a=a^{i+1}b^{i+1}=(a.b)^i(a.b)$

b.a=a.b

5)PT conclusion of 4 is not attained when we assume the relation for just 2 consecutive integers

…

6)In S_3 give example of 2 elements x,y such that $(x.y)^2!=x^2y^2$

$S_3=\{e,x,x^2,y,yx,yx^2\}$ x.y.x.y=e

x,y are the required elements

7)In S_3 PT there are 4 elements satisfying x^2=e and 3 elements satisfying x^3=e

e,y,yx,yx^2 and e,x,$x^{\ 2}$

8)If G is a finite group, PT there exists a positive integer N such that a^N=e for all a

As G is finite, for all x in G,there exists n(x) where $x^{n(x)}$=e

N=LCM of {n(x) for all x in G}

9)If order of G is 3 , 4 or 5 PT G is abelian

a) $G=\{e,x_1,x_2\}$

$x_1.x_2$=e (as else one of x_1,x_2 will be e)

hence cyclic-done

b)$G = \{e,x_1,x_2,x_3,x_4\}$

if $x_1.x_1$=e then $x_1.x_2=x_3$ (it cant be e,x_1,x_2) so $x_1.x_1.x_2=x_1.x_3$ so $x_2=x_1.x_3$

$x_1.x_2=x_1.x_1.x_3=x_3$ So $x_1.x_2=x_3$..then $x_1.x_4$ poses a problem

so $x_1.x_1=x_2$

$x_1.x_1=x_2$ and so $x_2.x_2=x_3$ (it cant be e by above reasoning and if $x_2.x_2=x_1$ then x_1^3=e and as $x_1.x_3$ cant be x_1^2, so $x_1.x_3=x_4$.$x_1^2x_3$ poses problem)

$x_3.x_3$ can only be x_4 or x_1.It cant be x_1 as then x_1^7=e $x_1.x_3=x_1^5=x_4$

($x_1^5=x_1^2$ will lead to $x_1=x_3$) so $x_1.x_4$ will pose a problem.

So group is $\{e,x,x_2,x_3,x_4\}$ which is cyclic

c)$G=\{e,x_1,x_2,x_3\}$

x1.x1=x2 or x1.x1=e

1) $x_1.x_1=e$
   then $x_1.x_2=x_3$ (it cant be x_1,x_2 or e)
   similarly $x_2.x_1=x_3$
   likewise $x_1.x_3=x_3.x_1=x_2$
   so $x_2.x_3=x_1.x_3.x_3$ $x_3.x_2=(x_3.x_1).x_3=x_1.x_3.x_3$
   so abelian
2) $x_1.x_1=x_2$
   then $x_1.x_2=x_3$
   so group is cyclic $\{e,x,x^2,x^3\}$

10)PT if every element of G is its own inverse,then G is abelian

a=a' b=b'

x=ab

x=x' so (ab)'=b'a'=ba = ab

11) If G is a group of even order PT it has an element a!=e such that a^2=e

If there exists an element of even order, a!=e say a^{2x}=e then b=a^x satisfies condition.

If all elements except e have odd order,then list down group as the following

G={e}U{a…a2x}U{b…b2y}……

So G has odd order which is a contradiction

12)Let G be a nonempty set closed under associative product which also satisfies

a)e such that a.e=a for all a

b)given a , y(a) exists in G such that a.y(a)=e

PT G is a group

Its closed,associative

PT a.e=e.a for all a

If e.a=x

e.a.y(a)=x.y(a)

e.a.y(a)=e.e=e

x.y(a)=e=a.y(a)

x.y(a).y(y(a))=a.y(a).y(y(a))

x.e=a.e

x=a

PT y(a).a=e for all a

Let y(a).a=x

x.y(a)=y(a).a.y(a)=y(a).e=y(a)=e.y(a)

(Cancellation law: a.b=c.b a.b.y(b)=c.b.y(b) so a.e=c.e so a=c)

So x=e

13)Prove by example that if a.e=a for all a and there exists y(a).a=e that G neednt be a group

….

14)Suppose a finite set G is closed under associative product and both cancellation laws hold. PT G is a group

Since G is finite let G={x_1,x_2..x_n}

Look at S(x_1)= {x_1.x_1, x_1.x_2, x_1.x_3,…..x_1.x_n}

All these are distinct because of left cancellation law

So S (x_1) in some order is G

Let x_i be the element such that x_1.x_i=x_1

Claim:For all y in G y.x_i=y

Proof:

Any y can be written as y_1.x_1 (because look at Z(x_1)={x_1.x_1, x_2.x_1…x_n.x_1}.By similar reasoning Z=G (right cancellation law). So y.x_i=y_1.x_1.x_i=y_1.x_1=y.

Also by looking at S(y),we know that given any y,there exists y' such that y.y'=x_1 .

Hence done by prev problems

15) So look at nonzero integers relatively prime to n.PT they form a group under multiplication mod n

Multiplication is associative.And a,b relatively prime to n =>ab is also relatively prime to n.There are only finite residues mod n.And cancellation laws hold (because of "relative primeness")Hence by 14 done

18)Construct a non abelian group of order 2n (n>2)

D(n)={e,x,..x^{n-1},y,yx,yx^2..yx^{n-1}} xyxy=e

*26)Done in vector spaces chapter

*PT e=e'

e.e=e

hence done

Examples of some groups:

* $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ (gen by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$)

* {n|n in Z , x^n=1}

Subgroup:Nonempty subset H of G forms a group under the same operation

⇨ (G,*) is a group.H is a subset of G is a subgrp iff it is closed under * and for all a, a' belongs to H

If H is a subgrp then by def true

Reverse way:

Associativity holds as it holds for operation in G

a,a' is in H

=>a.a' = e is in H

=> if H is a finite subset of G closed under *,it is a subgrp

Some problems done in class:

1) PT every subgroup of (Z,+) consists of only multiples of some integers
   If a is in S(subgrp),then a' is in S.if S!={0}
   So assume a>0 which is the smallest +ve number in S
   a+a'=0
   qa in S for all q in Z
   If possible let b=qa + r be in Z
   ⇨ r is in Z but 0<=r<a
   ⇨ r=0
2) If (a,b)=c PT c= na +mb
   Wlog assume a>b
   $a=q_1b + r_1$
   $b=r_1q_2 + r_2$
   $r_1=r_2q_3 + r_3$
   ..
   $r_{n-1}=r_nq_{n+1}$
   $= >r_n/r_{n-1} \ldots =>r_n/a \quad r_n/b => r_n/d$
   Where d=(a,b)
   $d/a \; d/b =>d/r_1..d/r_n$
   $=>d=r_n$

Equivalence relations,partitions:

Partitions:

S = union of nonempty disjoint subsets.the set of these subsets forms a partition of S

Relation:

Relation on S is a subset of S X S

Equivalence relation:

a~a(reflexive)

a~b => b~a (symmetric)

a~b , b~c => c~a (transitive)

An eq relation on a set S defines a partition of S:

Eqclass(a) = { x in S | x~a}

Note that a is in Eqclass(a)

And if x belongs to Eqclass(a) and Eqclass(b)

=> x~b ,x~a

=>a~b

=>Eqclass(a) = Eqclass(b)

So Eqclasses form a partition of S

A partition of S defines an Eq relation

a~b iff a and b belong to the same partition

Cosets:

H is a subgrp of G

aH={ah|h in H} is a left coset of H. Similarly right cosets can be defined

Properties:

1)eH = H

2)hH=H

3)aH = bH iff b'a is in H

If aH = bH

- a = bh
- b'a = h

if b'a = h

- a = bh
- $ah_1 = bhh_1 = bh_2$
- aH is a subset of bH

$bh_1 = bhh'h_1 = ah'h_1 = ah_2$

- bH is a subset of aH

4)every coset of a subgrp has the same number of elements

X:aH → bH

ah →bh.

This map is one one onto

5)G is union of left(right)cosets of H

Claim:cosets form equivalence classes (verify)

6) |aH| =|Ha| (ah → ha)

Index: No of left(right) cosets of a subgrp in a grp is called index of the subgrp in the grp

Index of H in G = [G:H]

Lagrange's theorem:

|G|=|H|[G:H]

Proof:

G = U (left cosets of H)

|aH|=|H|

So G = (no of cosets)|H|

Problems done in class:

1) If G has p (prime) no. of elements ,PT it is cyclic
   |G|!=1
   So let a!= e belong to G.
   H= subgrp generated by a
   |H| /|G|
   And |H| >1 => |H| =|G|
2) Write down the multiplication table for groups of order 2,3,4

*	e	A
e	e	A
a	a	E

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

*	e	a	B	c
e	e	a	B	c
a	a	e	C	b
b	b	c	A	e
c	c	b	E	a

From Lagrange's theorem

1) If G is finite, a in G then o(a)/o(G)
2) $a^{o(G)}$=e ($a^{o(a)}$ = e. and o(G) = k.o(a))
   so euler's theorem follows (a $^{phi(n)}$ = 1 mod n (a,n)=1)
   fermat's little theorem is a corollary (n = p (prime))

Some "flavour" of group theory:

HK=KH ←→ HK is a subgroup

HK=KH

Closure:$h_1k_1.h_2k_2 = h_1k_1(k^2h^2) = h_1k_xh_2= h_1h_xk^x= h_yk^x$

Associativity – as * in G is associative

Identity : e.e = e

Inverse: $(h_1k_1)' = k_1'h_1' = h_2k_2$

HK is a subgrp:

kh = (h'k')' which belongs to HK . So KH is contained in HK let x be in HK ,x' is in HK, x' = hk so x'' = x = k'h' in KH .so HK contained in KH

☺ *the one theorem I keep on using*

O(HK) = o(H)o(K)/o(H∩K)

Supposing (H∩K) = {e}

Now if $h_1k_1= h_2k_2$

⇨ $h_2'h_1=k_2k_1'$

⇨ $h_1 =h_2$, $k_1=k_2$

so o(HK) = o(H)o(K)

Claim: an element hk appears as many times as o(H∩K) times

hk = $(hh_1)(h_1'k)$ which belongs to HK if h_1 belongs to H∩K

so hk duplicated at least o(H∩K) times

if hk = h_1k_1

⇨ $h_1'h = k_1k' = u$

⇨ u is in H∩K

⇨ h_1 = hu'

⇨ k_1 = uk

⇨

Corollary:

If sqrt o(G)<o(H),o(K)=> H∩K is non empty

o(HK) <o(G)

o(HK) = o(H)o(K)/o (H∩K) < o(G)/o(H∩K)

So o(G) > o(G)/o(H∩K)

O(G)= pq (p>q are primes) then there is atmax one subgrp of order p

If H,K are different order p subgrps

Then they are cyclic

So H∩K is {e}

So o(HK) = p^2 > pq = o(G) -><-

Herstein (subgrps) Pg 46:

Problems

1) If H,K are subgroups,PT H∩K is a subgroup

   Closure: h is in H∩K, k is in H∩K

   ⇨ h, k is in H

   ⇨ h.k is in H

   ⇨ similarly h.k is in K

   ⇨ h.k is in H∩K

   associativity - * in G is associative

   identity: e is in H,e is in K

   inverse : h is in H∩K

   ⇨ h is in H,h is in K

   ⇨ h' is in H, h' is in K (this can be extended to any number of groups)

2) Let G be a group such that intersection of all non {e} subgrps is non {e}.PT every element in G has a finite order
If x is an element with infinite order,{ ….x’,e,x,x^2,x^3…} is a subgrp
So intersection of all subgrps contain x^k.
Now consider subgrp generated by x^{k+1}
x^k belongs to the above subgrp
$x^{(k+1)m} = x^k$
so x has finite order -><-
3) If G has no nontrivial subgrps,PT G must be cyclic of prime order
G!={e}
Let a !=e belong to G
H= subgrp generated by a
H !={e}
So H=G
G is cyclic
Now if G is finite, let d/o(G)
Look at subgrp generated by a^d -><-
If G is infinite look at subgrp generated by a^2 -><-
4) If H is a subgrp of G and a is in G,let aHa’ = {aha’ |h in H}.PT aHa’ is a subgrp,what is order of o(aHa’)
Proving it is a subgrp is left as an exercise (yawn!)
o(aHa’) = o(H)
aha’ → h
it is one one ,onto
5) PT there is a one one corr bet left cosets and right cosets
aH → Ha
6,7,8 – enumeration , boring
9) If H is a subgrp of G such that whenever Ha!=Hb , then aH!= bH.
PT gHg’ is contained in H for all g
Ha!=Hb => aH!=bH
⇨ aH=bH => Ha=Hb
⇨ a’b is in H => ab’ is in H
⇨ a = g b =gh’
⇨ So ghg’ is in H
10) H(n) = { kn | k in Z}.index of H(n)? right cosets of H(n)
Index H(n) = n
Cosets = 0+H, 1+H, 2+H, ..n-1+H
11) what is H(n)∩H(k)?
l=[k,n]
{ml|m in Z}
12) If G is a grp, H,K are finite index subgrps.PT H∩K is of finite index in G.can you find an upper bound
a_1H U a_2H…U a_hH = G
b_1K U b_2K…U b_kK = G
⇨ (a_1H U a_2H…U a_hH) ∩ (b_1K U b_2K…U b_kK) = G
⇨ U (a_iH ∩ b_jK) = G

Claim : ($a_iH \cap b_jK$), ($a_mH \cap b_nK$) are disjoint

If x is in intersection

⇨ $x=a_ih= b_jk = a_mh_1 = b_nk_1$

⇨ $a_m'a_i$ is in H, $b_n'b_j$ is in K

⇨ $a_iH=a_mH$ and $b_jK=b_nK$

Claim: if ($a_iH \cap b_jK$)!={} , it is contained in a coset of ($H \cap K$)

a is in ($a_iH \cap b_jK$)

=> $a_iH = aH$

=> $b_jK = aK$

So ($a_iH \cap b_jK$)= ($aH \cap aK$)

Claim: ($aH \cap aK$) is contained $a(H \cap K)$

Let b be in ($aH \cap aK$)

=> b = ah = ak

=> h =k and belongs to ($H \cap K$)

=> b is in $a(H \cap K)$

So as the former is finite in no. so will the latter be

some trivial stuff – so just convert to definitions

Following are some subgroups

Normalizer of a : N(a) = { x | x in G, xa=ax}

Centralizer of H = { x | x in G , xh = hx for all h in H}

Center of G = Z = centralizer of G

N(H) = { a | aHa' = H}

H is contained in N(H)

C(H) is contained in N(H)

In D_3, C({1,x,x^2}) != N({1,x,x^2})

18) If H is a subgrp of G, let N = $\cap_{x \text{ in } G}$ xHx'.PT N is a subgrp and aNa'=N for all a

Proving it is a subgrp is boring

Now aNa' = a ($\cap_{x \text{ in } G}$ xHx') a' = $\cap_{x \text{ in } G}$ axHx'a' = $\cap_{x \text{ in } G}$ (ax)H(ax)'

= $\cap_{ax \text{ in } G}$ (ax)H(ax)' = N

19)If H is a subgrp of finite index in G,PT there is only a finite no. of distinct subgrps in G of form aHa'

aH = bH

←→ a'b is in H

←→a'b = k

←→ (aha' = akk'hkk'a' = (ak) (k'hk) (ak)'

←→aHa' is contained in bHb'

20) If H is of finite index, PT there is a subgrp N of H and of finite index in G such that aNa' = N for all a in G. Upper bound for [G:N]?

Let N = $\cap_{x \text{ in } G}$ xHx'

N is contained in xHx' for all x (put x =e, so N is in H)

H is of finite index, then only finite subgrps of form aHa'

If we PT xHx' is of finite index in G, then by prob 12, and above we are done

TPT xHx' is of finite index if H is of finite index:

*(involves quotienting ☹ though)

Phi : G/H -> G/aHa'

gH → ga' (aHa')

this map is well defined!!

Why?

If bH = cH

⇨ b'c is in H

PT ba'(aHa') = ca'(aHa')

PT (ba')'(ca') is in aHa'

PT ab'ca' is in aHa' (but b'c is in H ☺)

Phi is onto : k(aHa') = kaa'(aHa') = phi(kaH)

Hence done

21-23 again boring enumerative stuff

24) Let G be a finite group whose order is not divisible by 3.If $(ab)^3 = a^3b^3$ for all a,b. PT G is abelian

$(aba'b')^3 = (ab)^3(a'b')^3 = a^3b^3a'^3b'^3 = a^3(bab')^3$

⇨ $b^2a'^3 = a'^3b^2$

⇨ so $x^2y^3 = y^3x^2$ for any x,y

⇨ so $a^6b^6 = b^6a^6$

⇨ $(a^2b^2)^3 = (b^2a^2)^3$

if $x^3 = y^3$ =>$x^3y'^3 = e$ => $(xy')^3 = e$

⇨ xy'=e as order not div by 3

⇨ x =y

so $a^2b^2 = b^2a^2$

proved bfr $a^2b^3 = b^3a^2$

$(a^2b^2)(b'^3a'^2) = (b^2a^2)(a'^2b'^3)$

⇨ $a^2b'a'^2 = b'$

⇨ $x^2y = yx^2$ for any x,y

⇨ $xy = x'yx^2$

Now $(yx)^3 = y^3x^3$

⇨ $yxyxyx = y^3x^3$

⇨ $xyxy = y^2x^2 = yyxx = y(xx')yxx = (yx)(x'yx^2) = yx(xy)$ (as $xy = x'yx^2$)

⇨ xyxy = (yx)(xy)

⇨ xy = yx

(25,26 → I got discouraged inspite of what herstein had to say :P (see exercises on finite abelian groups for this)

27)PT subgrp of a cyclic grp is cyclic

let G = cyclic grp generated by a , H be a subgrp

let H' = { x| a^x is in H}

and d = HCF of elements in H'

claim : H = $<a^d>$

if we PT a^d belongs to H, then we are done as H is a subgrp and any element of H = $a^x = (a^d)^{x'}$

Note that if a^x , a^y belongs to H, then $a^{HCF(x,y)}$ belongs to H

Hence done

28) How many generators does a cyclic grp of order n have?

U(n) = { x |x<=n, (x,n)=1}

|U(n)| is the answer

let G = <a> and o(a) = n

if G = <ax> then a is in G, so (ax)y = e

⇨ xy = 1 mod n

⇨ (x,n) = 1

and once a is in G, then rest are in G

35)Hazard a guess at what all n such that U_n is cyclic

chk no. theory book as herstein suggests :P

36)If a is in G, a^m = e.PT o(a) | m.

o(a) is the smallest integer such that $a^{o(a)}$ = e

let m = qo(a) + r

⇨ a^r=e

⇨ r=0

37) If in group G, a^5 = e, aba' = b^2 . for some a,b.Find o(b)

aba' = b^2

⇨ ab^2a' = b^4

⇨ a(aba')a' = b^4

⇨ $a^2ba'^2$ = b^4

⇨ $a^2b^2a'^2$ = b^8

⇨ a^2(aba')a'^2 = b^8

⇨ $a^3ba'^3$ = b^8

⇨ $a^3b^2a'^3$ = b^{16}

⇨ $a^4ba'^4$ = b^{16}

⇨ $a^4b^2a'^4$ = b^{32}

⇨ $a^5ba'^5$ = b^{32}

⇨ b = b^{32}

⇨ b^{31} = e

⇨ as 31 is a prime,o(b) = 31

38) Let G be a finite abelian grp in which the number of solutions in G for x^n=e is at most n for all n. PT G is cyclic

now let o(a) =m , o(b)=n and b is not in <a>

there exists an element x such that o(x) = lcm(m,n) (see exercise on finite abelian grp)

so for lcm(m,n) there are solutions e,x,x^2…$x^{[m.n]-1}$

but a, b are also solutions

so a is in <x>,b is in <x>

39) Double coset AxB.

{axb| a in A, b in B}

40)If G is finite,PT no. of elements in AxB is o(A)o(B)/o(A ∩ xBx')

imitating proof for o(AB)

if y in A ∩ xBx', say y = xbx'

axb* = ayxb’b*

so each axb* repeated A ∩ xBx’ times

also if axb = a*xb*

=> a*’a = xb*b’x’ which is in A ∩ xBx’

41)If G is finite and A is a subgrp such that all AxA have same number number of elements,PT gAg’ = A for all g

|AxA| = o(A)o(A)/0(A ∩ xAx’)

so o(A ∩ xAx’) = o(A ∩ x*Ax*’)

⇨ putting x = e , o(A ∩ x*Ax*’) = o(A)

⇨ x*Ax*’ contains A

but |xAx’| = |A|

map xax’ → a

so xAx’ = A

Direct product

External direct product:

G = A **X** B.

A,B are groups => under pointwise multiplication G is also a group

(can be extended to any finite number of groups)

e,f are identity elements in A,B respectively

A’={(a,f)|a in A}

A’ is normal in G:

$(a,b).(a_1,f).(a',b')=(aa_1a',f)$ and aa_1a' belongs to A

A’ is isomorphic to A:

$(a_1,f) \rightarrow a_1$

Internal direct product

G is internal direct product of N_i s when:

$G=N_1N_2N_3..N_n$ where N_i is normal in G for all i

Any g in G can be written in a unique way as $n_1n_2..n_n$ where n_i is in N_i

Lemma: $N_i \cap N_j = \{e\}$ and if a is in N_i ,b in N_j => ab=ba

If x belongs to $N_i \cap N_j$, then x = e.e….(x)…e…e = ee….e…x.…e

⇨ x = e

look at aba'b' . ba'b' is in N_i as it is normal. So aba'b' belongs to N_i

Similarly aba'b' belongs to N_j. So aba'b'=e So ab=ba

<u>Isomorphism</u>

If T is internal direct product of A_is, and G is external direct product of them

Then T is isomorphic to G

$(a_1,a_2….a_n)$-> $a_1a_2..a_n$

This map is well defined clearly

It is one one because of the unique way in which each element of G can be expressed.

It is clearly onto

Herstein Pg :108 (direct products)

<u>Problems:</u>

1)If A,B are groups,PT A **X** B isomorphic to B **X** A

(a,b)->(b,a)

2)G,H,I are groups.PT (G **X** H) **X** I isomorphic to G **X** H **X** I

((g,h),i) -> (g,h,i)

3)T = G_1 **X** G_2…**X** G_n.PT for all i there exists an onto homomorphism h(i) from T to G_i

What is the kernel of h(i)?

h(i) : $(g_1,g_2..g_n)$ -> g_i

Kernel of h(i) = $\{(g_1,g_2..g_{i-1},e_i,g_{i+1},…g_n)|\ g_j \text{ in } G_j\}$

4)T= G **X** G. D={(g,g)| g in G}.PT D is isomorphic to G and normal in T iff G is abelian

x:(g,g)->g.

if D is normal in T

⇨ (a,b)(g,g)(a',b') is in D

⇨ aga'=bgb' for any a,b

⇨ put b= e. so aga'=g

If G is abelian

⇨ (a,b)(g,g)(a',b')=(aga',bgb')=(g,g) which is in D .

5)Let G be finite abelian group.PT G is isomorphic to direct product of its sylow subgroups

Now since G is abelian,every subgroup is normal.In particular all sylow subgroups are normal.Let $O(G) = p_1^{a(1)}.p_2^{a(2)}..p_n^{a(n)}$ and H_i denote the p_i th sylow subgroup.

As G is abelian,$H_iH_j=H_jH_i$ .So H_iH_j is a subgroup

And $H_i \cap H_j$ ={e} as they are different sylow subgroups

So $O(H_iH_j)=p_ia(i)p_ja(j)$

Like wise $O(H_1H_2..H_n) = O(G)$

So $G = H_1H_2..H_n$

If $g = h_1h_2\ldots h_n = x_1x_2\ldots x_n$
Rearranging terms(Note G is abelian) we get $h_1x_1' = (h_2'x_2)\ldots(h_n'x_n)$
Order of h_1x_1' is a power of p_1 whereas RHS term's order is product of powers of $p_2,..p_n$
⇨ $h_i = x_i$
Hence done

6)PT G $= Z_m$ **X** Z_n is cyclic iff $(m,n)=1$
If $(m,n)=1$ then na is 1 mod m and mb is 1 mod n
Claim: (1,1) generates group
$(1,0) = (1,1)^{na}$
$(0,1) = (1,1)^{mb}$
$(x,y) = (1,0)^x(0,1)^y$

If $(m,n)=d$
If (x,y) generates G
$\Rightarrow (1,0) = (x,y)^k$
Note y cant be 0 as then elements like (1,1) cant be generated
⇨ k is a multiple of n say k'n
⇨ x(k'n) is 1 mod m
⇨ xnk' = qm +1
⇨ d/n , d/m =>d/1

7)Using 6 PT chinese reminder theorem(ie) (m,n)=1 and given u,v in Z there exists x in Z such that x = u mod m and x=v mod n
As (1,1) generates Z_m **X** Z_n,
$(u',v') = (1,1)^x$ where u=u' mod m (u'<m) and v=v' mod n (v'<n)
⇨ x=u' mod m
⇨ x= v' mod n

8)Give an ex of a group G and normal subgroups $N_1,N_2..N_k$ such that $G=N_1N_2..N_k$ and $N_i \cap N_j = \{e\}$ for i!=j and G in not the internal direct product
$G = \{ e, a, a^2, b, b^2, ab, a^2b^2\}$ $(ab=ba, a^3=b^3=e)$

$N_1=\{e,a,a^2\}$ $N_2=\{e,ab,a^2b^2\}$ $N_3=\{e,b,b^2\}$
All are normal as G is abelian
ab= a.e.b = e.ab.e (no unique representation)

9)PT G is internal direct product of N_is (normal) iff $G=N_1..N_k$ and $N_i \cap N_1N_2..N_{i-1}N_{i+1}..N_k = \{e\}$ for all i
Note : x_i belongs to N_i for any variable x in the following

If G is internal product ,then clearly $G=N_1N_2..N_k$
If the second condition isn't true
⇨ $n_i = n_1n_2..n_{i-1}n_{i+1}..n_k = e.e.e\ldots.n_i.e.e.e..e = n_1n_2\ldots n_{i-1}.e.n_{i+1}\ldots.n_k$
(no unique rep)

If the two conditions hold , PT any g in G has a unique rep as $n_1n_2..n_k$
If $n_1n_2..n_k = w_1w_2\ldots w_k$

- ⇨ $n_1'w_1=n_2..n_k.w_k'...w_2'$
- ⇨ $n_2...n_{k-1}(n_kw_k')..w_2' = n_2..n_{k-1}(x_k)w_{k-1}'..w_2'$
- ⇨ $= n_2...(n_{k-1}(x_k)n_{k-1}')n_{k-1}w_{k-1}'...w_2' = n_2..n_{k-2}(y_k)(x_{k-1})w_{k-2}'..w_2'$ (as N_k is normal)
- ⇨ $= n_2...n_{k-3}(n_{k-2}y_kn_{k-2}')(n_{k-2}x_{k-1}n_{k-2}')(n_{k-2}w_{k-2}')w_{k-3}'..w_2'$
- ⇨ $=n_2..n_{k-3}(l_k)(y_{k-1})(z_{k-2})w_{k-3}'..w_2'$
- ⇨ $...= s_ks_{k-1}..s_2$
- ⇨ $w_1'n_1=s_2'...s_k'$
- ⇨ $w_1=n_1$ etc(due to second cond)

10)Let G be a group .$K_1,K_2..K_n$ be normal subgroups.$K_1 \cap K_2..\cap K_n =\{e\}.V_i=G/K_i$

PT there is an isomorphism from G into V_1 X $V_2..V_n$

Phi:G→ V_1 X V_2..X V_n

g→ $(gK_1,gK_2...gK_n)$

Phi is a homomorphism

It is one one as

If $(gK_1,gK_2...gK_n)=(hK_1,..hK_n)$

- ⇨ h'g is in $K_1,K_2..K_n$
- ⇨ h'g= e
- ⇨ h=g

11,12 – I don't know

13)Give an example of a finite nonabelian group G which contains a subgroup H_0 != {e} such that H_0 is contained in all subgroups H !={e}

$G=\{e,a,a^2,a^3,b,b^2,b^3,ab,ba,ab^3,ba^3\}$

Where $a^2=b^2,a^4=b^4=e$ and $ab^3=ba$

(Hopefully this is a group ☺ .And $H_0 =\{e,a^2=b^2\}$)

Note $\{e,ab,a^2,a^3b\}$ is a group etc

14)PT every group of order p^2 is cyclic or direct product of 2 cyclic groups of order p(prime)

G of order p^2 is abelian(proved earlier..using conjugacy of classes)

And any element has order 1,p or p^2

If there is one element of order p^2 then cyclic

Else pick an element g of order p ,let H be the subgrp generated by g

And pick h not in H and let K be the subgrp generated by h

As G is abelian,H,K are normal

Also H ∩ K ={e}.So G = HK (the usual o(G)=o(H)o(K))

Also if $x=g^ah^b= g^ch^d \Rightarrow g^{a-c} = h^{d-b} \Rightarrow a=c, b= d$ (unique rep)

- ⇨ internal direct product

15) Let G =A X A whereA is cyclic of order p, p a prime.How many automorphisms?

p^2 ? (☹ this is a star problem !!)

$(e,a)\rightarrow (e,a^i)$ $(a,e)\rightarrow(a^j,e)$ fixes the automorphism

16) If G = K_1 X K_2..X K_n what is center of G?

Z_i = center of K_i

- ⇨ center of G = Z_1 X $Z_2...Z_n$

$((k_1,..k_n)(g_1,..g_n) =(g_1,..g_n)(k_1,..k_n)$ for all g_i)

17) Describe $N(g) = \{ x \text{ in } G \mid xg=gx\}$

$g=k_1k_2..k_n$

$N(g)=N(k_1) X N(k_2)..X N(k_n)$

(or so I think..verify)

18) If G is a finite group and $N_1,..N_k$ are normal subgrps such that $G=N_1N_2..N_k$ and $o(G)=o(N_1)o(N_2)..o(N_k)$, PT G is the direct product of these N_i's

Note : x_i belongs to N_i for any variable x in the following

by prob 9 enough to PT $N_i \cap N_1N_2..N_{i-1}N_{i+1}..N_k =\{e\}$ for all i

Since all N_i's are normal, $N_iN_jN_k..N_m$ is a subgrp

$O(G)=o(N_1N_2..N_k)=o(N_1)o(N_2..N_k)/o(N_1\cap N_2....N_k) =$

$o(N_1)o(N_2)o(N_3..N_k)/ o(N_1\cap N_2....N_k) o(N_2\cap N_3....N_k)$ and so on

$= o(N_1)o(N_2)o(N_3)\ldots o(N_k)/ o(N_1\cap N_2....N_k) o(N_2\cap N_3....N_k).. o(N_{k-1}\cap N_k)$

⇨ $o(N_i\cap N_{i+1}....N_k)=1$ for all i

if x is in $N_i\cap N_1.N_{i-1}N_{i+1}...N_k$

⇨ $x = n_1\ldots n_{i-1}n_{i+1}..n_k$

⇨ $n_1'=n_2\ldots n_k.x' =n_2..n_{k-1}x'x(n_k)x'=n_2..n_{k-1}x'm_k$ (as N_k is normal)

⇨ and so on…$= n_2\ldots n_{i-1}(s_i)s_{i+1}..s_k$

⇨ $n_1'= e$ as $o(N_1\cap N_2....N_k) =1$

⇨ and so $x = n_2\ldots n_{i-1}n_{i+1}..n_k$ and we can follow the same procedure to establish $n_2=e$ etc

⇨ $x = e$

** No idea abt : Prob 11,12 in direct products*

** Prob 25,26 in subgrps solved in finite abelian grps chapter*