A FIRST GRADUATE COURSE IN ALGEBRA

ABSTRACT ALGEBRA

DR. MOHAMMED SULIMAN EL-ATRASH

PROFESSOR OF MATHEMATICS

MATH. DEPARTMENT

ISLAMIC UNIVERSITY OF GAZA

GAZA, PALESTINE

TABLE OF CONTENTS

بسم ا الر ن الرحيم

Chapter I

1. Groups, definitions
2. Cyclic groups
3. Permutation groups
4. Cosets and normal subgroups
5. Factor groups
6. Group homomorphisms

1.1 Groups.

Modern definition of a group (Caley's definition).

1.1.1 DEFINITION. *A **group** (G, .) is a nonempty set G together with a binary operation . on G such that the following conditions hold:*

(i) Closure: For all a, b $\in$ G the element a.b is a uniquely defined element of G.

(ii) Associativity: For all a, b, c $\in$ G, we have a.(b.c) = (a.b).c.

*(iii) Identity: There exists an **identity element** e $\in$ G such that e.a = a and a.e = a for all a $\in$ G.*

*(iv) Inverses: For each a $\in$ G there exists an **inverse element** $a^{-1} \in$ G such that: $a.a^{-1} = e$ and $a^{-1}.a = e$.*

We will usually simply write ab for the product a.b.

Remark: Identity *e* is unique, and inverse of any element *a* is unique.

1.1.2 PROPOSITION. (***Cancellation Property for Groups***) Let G be a group, and let *a, b, c* $\in$ G.

(a) *If ab = ac*, then *b = c*.

(b) *If ac = bc*, then *a = b*.

Proof. For (a) multiply by a^{-1} from the left.

For (b) multiply by c^{-1} from the right.

1.1.3 Proposition. *Let G be a set with associative binary operation. Assume that $\exists\, e \in G$ such that:*

(a) ***Right identity :*** *$ae = a$.*

(b) ***Right inverse:*** *for every $a \in G$; $\exists\, b \in G$ with $ab = e$.*

Then G is a group.

Proof: For $x, y, u \in G$, if $xu = yu$; we claim that $x = y$.

By (b), choose $v \in G$ with $uv = e$. Now

$$x = xuv = yuv = ye = y.$$

Next, we want to show that e is left identity i.e., for every $a \in G$ we have $e.a = a$. Choose $b \in G$ with $ab = e$.

$$(ea)b = e(ab) = ee = e = ab.$$

Then, by our claim, $ea = a$.

It remains to show that if $ab = e$ then $ba = e$.

$$(ba)b = b(ab) = be = b = eb,$$

therefore again by the claim $ba = e$.

1.1.4 Definition. *A group G is said to be* ***abelian*** *if $ab = ba$ for all $a, b \in G$.*

1.1.5 Definition. *A group G is said to be a* ***finite group*** *if the set G has a finite number of elements. In this case, the number of elements is called the order of G, denoted by $|G|$.*

1.1.6 Definition. *Let a be an element of the group G. If there exists a positive integer n such that $a^n = e$, then a is said to have finite order, and the smallest such positive integer is called the* ***order*** *of a, denoted by $o(a)$.*

If there does not exist a positive integer n such that $a^n = e$, then a is said to have infinite order.

1.1.7 DEFINITION. *Let G be a group, and let H be a subset of G. Then H is called a* ***subgroup*** *of G if H is itself a group, under the operation induced by G. (we denote this by $H \leq G$).*

1.1.8 PROPOSITION. *Let G be a group with identity element e, and let H be a non-empty subset of G. Then H is a subgroup of G if and only if the following conditions hold:*
(i) $ab \in H$ for all $a, b \in H$;
(ii) $a^{-1} \in H$ for all $a \in H$.

PROOF: EXERCISE.

Theorem 1.1.8 states the sufficient conditions for a no-empty subset H to be a subgroup. I.e., instead of checking all four conditions of the group we only check two conditions.
In the following Exercise we can show even one condition is enough.

EXERCISE. Let G be a group with identity element e, and let H be a non-empty subset of G. Then $H \leq G$ if and only if the following conditions hold:

$$ab^{-1} \in H \text{ for all } a, b \in H;$$

REMARK. Identity in H is the same as the identity in G.

1.1.9 DEFINITION. *Let G be a group. Let $x \in G$. The* ***centralizer of x*** *is the set* $C_G(x) = \{ y \in G \mid xy = yx \}$.

EXERCISE. Show that $C_G(x)$ is a subgroup of G.

EXERCISE. Let π be a collection of subgroups of G. Show that the set H $= \cap\{K \mid K \in \pi \}$ is a subgroup of G.

1.1.10 DEFINITION. *The* ***center Z(G)*** $= \cap\{C_G(x)$ *for all* $x \in G\}$.

EXERCISE. Show that Z(G) is a subgroup of G.

1.2 Cyclic Groups

1.2.1 DEFINITION. *Let X be a non-empty set of G. The subgroup* ***generated*** *by X is* $\langle X\rangle = \cap\{H \le G \mid X \subset H\}$.
We write $\langle a\rangle$ *for* $\langle\{a\}\rangle$. $\langle a\rangle$ *is called the* ***cyclic subgroup generated by a***.
The group G is called a ***cyclic group*** *if there exists an element* $a \in G$ *such that* $G = \langle a\rangle$. *In this case a is called a* ***generator*** *of G.*

EXERCISE. Show that $\langle a\rangle = \{ a^n \mid$ for some $n \in \mathbf{Z}\}$.

1.2.2 DEFINITION. *For* $a \in G$, *the* ***order*** *of a (denoted by o(a)) is the least positive integer n such that* $a^n = e$. *If no such integer exist then we say that the order of a is infinite.*

1.2.3 PROPOSITION. *Let a be an element of the group G.*
(a) If a has infinite order, and $a^k = a^m$ *for integers k, m, then* $k = m$.
(b) If a has finite order and k is any integer, then $a^k = e$ *if and only if* $o(a) \mid k$.
(c) If a has finite order $o(a) = n$, *then for all integers k, m, we have* $a^k = a^m$ *if and only if* $k \equiv m \pmod n$. *Furthermore,* $|\langle a\rangle| = o(a)$.

PROOF. (a) Assume that $k > m$. Since $a^k = a^m$ then

$$a^{k-m} = a^{m-m} = a^0 = e,$$

Since o(a) is infinite then k-m = 0. Hence $k = m$.
(b) Let n = o(a). By division algorithm, we have

$$k = qn + r \text{ with } 0 \le r < n.$$

If $r > 0$, then

$$a^k = a^{qn+r} = a^{qn}\, a^r.$$

Therefore

$$a^r = a^k a^{-qn} = ee = e.$$

This contradicts that the order of a is n.

Therefore $r = 0$. Thus $n \mid k$.

(c) $$a^k = a^m \text{ iff } a^{k-m} = e.$$

Therefore by (b), $n \mid k\text{-}m$, then $k \equiv m \pmod{n}$.

Conversely if $k \equiv m \pmod{n}$ then $n \mid k\text{-}m$. Therefore $k\text{-}m = qn$ for some integer q, so

$$a^{k-m} = (a^n)^q = e^q = e.$$

Furthermore, the only different elements are

$$\{a^0 = e, a, a^2, \ldots, a^{n-1}\}.$$

Hence $|\langle a\rangle| = o(a)$.

EXERCISE. Let G be a group. And let $H \subset G$ with $|H| < \infty$.

Show that H is a subgroup of G iff $xy \in H$ for all $x, y \in H$.

1.2.4 **Lemma.** *Let G be a group and let $X \subset G$. Assume that $xy = yx$ for all $x, y \in X$. Then $\langle X\rangle$ is abelian subgroup of G.*

Proof. By hypothesis if $x \in X$ then $X \subset C(x)$.

Thus $\langle X\rangle \subset C(x)$ for all $x \in X$.

It follows that $x \in C(\langle X\rangle)$, for all $x \in X$.

Therefore $X \subset C(\langle X\rangle)$, and hence $\langle X\rangle \subset C(\langle X\rangle)$. The proof is complete.

1.3 Cosets and Normal Subgroups

1.3.1 **Definition.** *Let $H \le G$. for $a \in G$ the set $Ha = \{ha \mid h \in H\}$is called* ***right coset*** *of a. The set $aH = \{ah \mid h \in H\}$is called* ***left coset*** *of a.*

1.3.2 **Proposition.** *Let $H \le G$. let $a, b \in G$. Then the following hold*

(a) *$Ha = Hb$ iff $ab^{-1} \in H$.*

(b) *If $Ha \cap Hb \neq \varnothing$ then $Ha = Hb$.*

(c) *$G = \cup\{Ha \mid a \in G\}$.*

(d) *$|Ha| = |Hb| = |H|$.*

Proof. (a) Let $a \in Ha$ then $a = hb$ for some $h \in H$.

Thus $ab^{-1} = h \in H$.

Conversely if $ab^{-1} \in H$, then $ab^{-1} = h$ for some $h \in H$.

Therefore $a = hb$.

Now for $x \in Ha$;

$$x = h'a \text{ for } h' \in H,$$

thus $$x = h'hb \in H.$$

Hence $Ha \subset Hb$.

The converse is similar.

(b) Let $z \in Ha \cap Hb$ then

$$z = h'a = h''b \text{ for } h', h'' \in H.$$

It follows that $a = h'^{-1}h''b$. Therefore

$$ha = hh'^{-1}h''b, \text{ so } Ha \subset Hb.$$

The reverse inclusion is similar. Hence $Ha = Hb$.

(c) since $a \in Ha$ then $G \subset \cup\{Ha \mid a \in G\}$.

The reverse inclusion is obvious.

(d) The map ψ: $Ha \to Hb$ that maps $ha \to hb$ is 1-1 and onto.

1.3.3 DEFINITION. *The number of different cosets of a subgroup H of G is called the* ***index*** *of H in G. and is denoted by [G:H] or |G:H|.*

1.3.4 THEOREM. (**Lagrange's**) If H is a subgroup of the finite group G, then the order of H is a divisor of the order of G.

PROOF. $|G| = [G:H]|H|$.

1.3.5 COROLLARIES TO LAGRANGE'S THEOREM (RESTATED)*:*

(a) For any $a \in G$, $o(a)$ is a divisor of $|G|$.

(b) For any $a \in G$, $a^n = e$, for $n = |G|$.

(c) Any group of prime order is cyclic.

PROOF. EXERCISE.

1.3.6 THEOREM. *Every subgroup of a cyclic group is cyclic.*

PROOF. Let H be a subgroup of a cyclic group G. Let G = $\langle a \rangle$ with o(a) = n. Let m be the smallest positive integer with $a^m \in$ H. We will show that $b = a^m$ is the generator of H by showing that every element x of H; x is a power of b.

Now let $x \in$ H, since H $\subset$ G then $x = a^k$ for some integer k. Using division algorithm, there are two integers q, r such that

$$k = qm + r \text{ with } 0 \leq r < m.$$

It follows that $a^k = a^{qm + r}$. Then

$$a^r = a^{k - qm} = a^k (a^m)^{-q} \in \text{H}.$$

Then $a^r \in$ H. but $r < m$. Therefore $r = 0$.

Hence $x = a^k = (a^m)^q$.

Hence H is cyclic with H = $\langle a^m \rangle$.

1.4 Permutation Groups

1.4.1 DEFINITION. *Let G_1 and G_2 be groups, and let $\varphi : G_1 \to G_2$ be a function. Then φ is said to be a group* ***homomorphism*** *if φ satisfies*

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a,\ b \in G_1.$$

If φ is one-to-one and onto φ is called ***isomorphism****, in this case G_1 is said to be* ***isomorphic*** *to G_2, and this is denoted by $G_1 \approx G_2$.*

And in the case that G_1 is the same as G_2; φ is called an ***automorphism*** *of G_1.*

1.4.2 PROPOSITION. *Let $\varphi: G_1 \to G_2$ be an isomorphism of groups.*

(a) If a has order n in G_1, then $\varphi(a)$ has order n in G_2.

(b) If G_1 is abelian, then so is G_2.

(c) If G_1 is cyclic, then so is G_2.

1.4.3 DEFINITION. *A permutation of the set S is a one to one and onto function. The set of all permutations of a set S is denoted by Sym(S). The set of all permutations of the set {1,2,...,n} is denoted by S_n.*

1.4.4 PROPOSITION. *If S is any nonempty set, then Sym(S) is a group under the operation of composition of functions.*

1.4.5 DEFINITION. *The set of all automorphisms of a group G is called the* ***automorphism group*** *and is denoted by* ***Aut****(G) .*

1.4.6 EXERCISE. Let G be a group. Let $g \in$ G. define σ_g: G $\to$ G by $\sigma_g(x) = g^{1}xg$ for $x \in$ G. Show that σ_g is an automorphism of G.

(σ_g is called an ***inner automorphism*** *of G).*
The set of all inner automorphism of G is denoted by ***Inn****(G).*

Notation. Usually $g^{-1}xg$ is written as x^g because it follows the same rules of exponentiation. i.e., $h^{-1}(g^{-1}xg)h = (h^{-1}g^{-1})x\ (gh) = x^{gh}$.

EXERCISE.

(a) Show that $Aut(G)$ is a group.

(b) Show that $Inn(G) \leq Aut(G) \leq Sym(G)$.

(c) Show that σ_g is the identity automorphism *iff* $g \in \mathbf{Z}(G)$.

EXERCISE. Let S, T be two sets and let $\alpha : S \to T$ be a bijection. Show that $Sym(S) \cong Sym(T)$.

1.4.6 THEOREM. *Let G cyclic group.*

(a) If G is infinite, then $G \approx \mathbf{Z}$.

(b) If $|G| = n$, *then* $G \approx \mathbf{Z}_n$.

PROOF. **EXERCISE**.

1.4.7 PROPOSITION. *Let* $G = \langle a \rangle$ *be a cyclic group with* $|G| = n$.

(a) If $m \in \mathbf{Z}$, *then* $\langle a^m \rangle = \langle a^d \rangle$, *where* $d = gcd(m, n)$, *and* a^m *has order* n/d.

(b) The element a^k *generates G if and only if* $gcd(k, n) = 1$.

(c) The subgroups of G are in one-to-one correspondence with the positive divisors of n. (i.e., if $d \mid n$ *then there is a subgroup of order d.)*

(d) If m and k are divisors of n, then $\langle a^m \rangle \subset \langle a^k \rangle$ *if and only if* $k \mid m$.

PROOF. (a) Let $x \in \langle a^d \rangle$, then $x = (a^d)^k$ for some integer k.

We need to show that x is a power of a^m. To do this we use the fact that $d = (m, n)$ that is; there are two integers s, t such that

$$d = sm + tn.$$

It follows that

$$a^d = a^{sm + tn}$$

$$= (a^m)^s(a^n)^t$$

$$= (a^m)^s.$$

It follows that

$$x = (a^d)^k \in \langle a^m \rangle.$$

Hence $\langle a^d \rangle \subset \langle a^m \rangle$.

It follows that $\langle a^d \rangle = \langle a^m \rangle$.

The reverse inclusion is easier because $a^m \in \langle a^d \rangle$.

Thus $\langle a^m \rangle \subset \langle a^d \rangle$.

To see that the order of a^m is n/d note that

$$o(a^m) = o(a^d) = n/d.$$

(b) By part (a), a^k generates G iff $o(a^k) = n$ iff $1 = \text{g.c.d}(k, n)$.

Parts (c), (d) are left as an **EXERCISE.**

1.4.8 **COROLLARY.** *The number of generators of a cyclic group of order n is*

$\varphi(n) = |\{r \mid 1 \le r \le n-1, (r, n) = 1\}|$. ***Euler function*** $\boldsymbol{\varphi(n)}$.

1.4.9 **APPLICATION.** *Let $n > 0$. Then* $n = \sum_{d|n} \varphi(d)$

PROOF. Let G be a cyclic group of order n. write $\alpha(k)$ = number of elements in G of order k. Clearly $\sum_k \alpha(k) = n$.

If $x \in G$ has order k then $\langle x \rangle$ is the only subgroup of G of order k. Thus if $\alpha(k) \neq 0$ then $k \mid n$. So $n = \sum_{k|n} \alpha(k)$.

Now $G = \langle g \rangle$, If $x, y \in G$, $|\langle x \rangle| = |\langle y \rangle| = k$ then $o(x) = o(y) = k$.

But $\exists$ only one subgroup of order k. So there are exactly $\varphi(k)$ elements of order k, i.e., $\alpha(k) = \varphi(k)$. Hence $n = \sum_{k|n} \varphi(k)$.

1.4.10 DEFINITION. *Let G be a group. If there exists a positive integer N such that $a^N = e$ for all $a \in G$, then the smallest such positive integer is called the exponent of G.*

1.4.11 PROPOSITION. *Let G be a group, and let $a, b \in G$ be elements such that ab = ba. If the orders of a and b are relatively prime, then o(ab)=o(a)o(b).*

1.4.12 PROPOSITION. *Let G be a finite abelian group.*
(a) The exponent of G is equal to the order of any element of G of maximal order.
(b) The group G is cyclic if and only if its exponent is equal to its order.

PROOF. (a) **EXERCISE.**
(b) Let N be the exponent of G. By (a) there is an element $g \in$ G with o(g) = N = |G|, therefore G is cyclic.
Conversely if G = $\langle g \rangle$ is cyclic then o(g) = |G| = N.

1.4.13 COROLLARY. *Let G be a finite group of order n.*
(a) For any $a \in G$, o(a) is a divisor of n.
(b) For any $a \in G$, $a^n = e$.

EXAMPLE. (**Euler's theorem**) Let G be the multiplicative group of congruence classes modulo n. G = { k | $1 \leq k < n$, $(k, n) = 1$}

The order of G is given by $\varphi(n)$, and so by **COROLLARY** ( ), raising any congruence class to the power $\varphi(n)$ must give the identity element.

1.4.14 COROLLARY. *Any group of prime order is cyclic.*

PROOF. Let G be a group of order p where p is prime. Let $e \neq a \in$ G. $\langle a \rangle$ is a subgroup of G. By Lagrange's Theorem $|\langle a \rangle|$ divides the order of |G| = p.
It follows that $|\langle a \rangle| = p$. Hence $\langle a \rangle$ = G, i.e., G is cyclic.

1.4.15 DEFINITION. *Any subgroup of the symmetric group Sym(S) on a set S is called a* ***permutation group*** *or* ***group of permutations****.*

1.4.16 THEOREM. *(**Cayley**) Every group is isomorphic to a permutation group.*

PROOF. Let G be a group. For every $g \in$ G we will show that multiplication by g is a permutaion. Let

$$\pi_g : G \rightarrow G,$$

be defined as follows

$$\pi_g(x) = gx.$$

First π_g is 1-1

since $\pi_g(x) = \pi_g(y)$ iff $gx = gy$ iff $x = y$.

Second, π_g is onto,

since for every $y \in$ G, $\pi_g(g^{-1}y) = y$.

Hence $\pi_g \in Sym(G)$. Let

$$\sigma : G \rightarrow Sym(G) \text{ be defined by}$$

$$\sigma(g) = \pi_g.$$

To see that σ is 1-1,

let $\sigma(g) = \sigma(h)$, then $\pi_g = \pi_h$.

It follows that $\pi_g(e)= \pi_h(e)$, i.e., $ge = he$, and thus $g = h$.

To see that σ is a homeomorphism;

note that $\sigma(gh) = \pi_{gh} = \pi_g\pi_h = \sigma(g)\ \sigma(h)$.

(Note that composition of permutations here is that we apply π_g first and then π_h). This completes the proof.

Chapter II

2.1 Normal subgroups

2.1.1 DEFINITION. *Let $H \leq G$ then H is normal subgroup of G if $H^g = H$ for all $g \in G$. (we denote this by $H \lhd G$).*

Example.

(1) $\{e\} \lhd G$, $G \lhd G$.

(2) *If G is abelian then every subgroup of G is normal in G.*

2.1.2 PROPOSITION. *Let $H \leq G$ then $H \lhd G$ iff $H^g \subset H$ for all $g \in G$.*

PROOF. We need to show that $H^g = H$ for all $g \in G$.
Since $H^g \subset H$ for all $g \in G$, take g^{-1} for g i.e., $(H)^{g^{-1}} \subset H$. Then $((H)^{g^{-1}})^g \subset H^g$
It follows that $H \subset H^g$. Hence $H = H^g$.

1.56 EXERCISE. Show that for any group G; $Inn(G) \lhd Aut(G)$.

2.1.3 DEFINITION. *Let $H \leq G$, H is called* ***characteristic*** *in G if $\sigma(H) = H$ for all automorphisms $\sigma \in Aut(G)$.*

2.1.4 COROLLARY. *If H is characteristic in G then $H \lhd G$.*

2.1.5 DEFINITION. *For $x, y \in G$,*
we define the ***commutator*** *$[x, y] = x^{-1}y^{-1}xy$.*

2.1.6 COROLLARY. *$xy = yx$ iff $[x, y] = e$.*

2.1.7 DEFINITION. *The* ***derived or the commutator subgroup*** *of a group G (denoted by G') is the smallest subgroup generated by all commutators.*
i.e., $G' = \langle \{[x, y] \mid x, y \in G\} \rangle$.

2.1.8 COROLLARY. *G is abelian iff* $G' = \{e\}$.

EXERCISE. Show that G' is characteristic in G.

2.1.9 DEFINITION. *Let G be a group.* $\boldsymbol{G^{(n)}}$ *= the derived subgroup of* $G^{(n-1)}$.
By this definition we have :

$$G \geq G' \geq G'' \geq \ldots \geq G^{(n)} \geq \ldots$$

2.1.10 PROPOSITION. *If* $N \lhd G$*, M characteristic in N then* $M \lhd G$.

PROOF. For $g \in G$, let $\sigma_g \in Inn(G)$. We need to show that $\sigma_g(M) = M$. By normality of N we have: $\sigma_g(N) = N$. But $Inn(G) \leq Aut(G)$. Therefore σ_g is an automorphism of G, it follows then that σ_g an automorphism of N. Since M characteristic in N, then $\sigma_g(M) = M$.

EXERCISE. Let $C \lhd G$, where C is cyclic subgroup of G. Suppose that $|G| < \infty$. Show that if $K \leq C$ then $K \lhd G$.

1.67 EXERCISE If $M, N \lhd G$, $M \cap N = \{e\}$ then $M \leq C_G(N)$ (and $N \leq C_G(M)$).

2.2 Product of Sets

Let X, Y be two sets of a group G. Write $XY = \{ xy \mid x \in X, y \in Y \}$. We write Xy for $X\{y\}$, and if $H \leq G$, (as we have seen before Hx is called right coset, xH is called left coset).

2.2.1 THEOREM. *Let* $H, K \leq G$ *then HK is a subgroup of G iff HK = KH.*

PROOF. Assume $HK \leq G$, then we have $H \subset HK$, $K \subset HK$ and since HK is a subgroup i.e., closed under multiplication then $KH \subset HK$.
For the reverse inclusion, let $u \in HK$, then $u^{-1} \in HK$. Write $u^{-1} = hk$. It follows that $u = (hk)^{-1} = k^{-1}h^{-1} \in KH$. Thus HK = KH.

Conversely, Assume that HK = KH. Let $u, v \in$ HK, write $u = h_1k_1$, $v = h_2k_2$. It follows that $uv = h_1k_1h_2k_2$, but $k_1h_2 \in$ KH = HK, therefore $k_1h_2 = h_3k_3 \in$ HK.
We say that X and Y **permutes** if $XY = YX$.

2.2.2 PROPOSITION. *Let $N \lhd G$, and let $X \subset G$, then $NX = XN$.*

PROOF. Let $u \in$ NX, then $u = nx$, $n \in$ N, $x \in X$. write $u = xx^{-1}nx = xn^x \in x$N $\subset$ XN. Therefore, N$X \subset X$N. Similarly, XN $\subset$ NX. Hence XN = NX.

2.2.3 COROLLARY. *(a) Let $H \le G$, $N \lhd G$, then $HN \le G$.*
(b) Let $N \lhd G$, $g \in G$, then $Ng = gN$.

EXERCISE. Prove that the number of left cosets is the number of right cosets.

2.2.4 THEOREM. *Let $N \lhd G$. Define a binary operation on the set of all right cosets of N as follows: $(Nx)(Ny) = Nxy$. Then the set of all right cosets with this operation is a group.*

PROOF. First we will show that this operation is well defined. This means that if Nx = Nx', Ny = Ny' then (Nx)(Ny) = Nxy = (Nx')(Ny') = N$x'y'$. Now since (Nx) = (Ny) then by PROPOSITION (), $x'x^{-1} \in$ N, similarly $y'y^{-1} \in$ N. It follows that:
N$x'y'$ = N$x'x^{-1}xy'y^{-1}y$ = N$xy'y^{-1}y$ = (xN)$y'y^{-1}y$ = x(N$y'y^{-1}y$) = xNy = Nxy. Thus this binary operation is well defined.
The set of all cosets is closed under this operation. Associativity is clear. The identity element is Ne = N, since NNx = Nx. The inverse of Nx is Nx^{-1}.

2.2.5 DEFINITION. *The group defined in the last theorem is called the* ***Factor group (or quotient group).*** *And is denoted by G/N.*

Note. If $|G| < \infty$ then $|G/N| = |G|/|N|$.

EXERCISE. Let H ≤ G. Let S = {Hg | $g \in$ G}. Show that for the multiplication (Nx)(Ny) = Nxy to be defined H has to be normal in G.

EXAMPLE. For any group G, if N = $\{e\}$ then G/N $\cong$ G. and if N = G then G/N $\cong$ $\{e\}$.

EXAMPLE. For the group G = ($\mathbf{Z}$, +), if N = $n\mathbf{Z}$ then G/N = $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}_n$ (integers modulo n).

2.2.6 DEFINITION. *Let $N \lhd G$, the map $\pi : G \to G/N$ defined by $\pi(g) = Ng$ is a surjective homomorphism called the* ***canonical*** *(or* ***natural****) homomorphism.*

2.2.7 DEFINITION. *If $\theta : G \to K$ is a homomorphism, kernel of θ (denoted by $ker(\theta)$) = $\{ g \in G \mid \theta(g) = e_K\}$.*

EXERCISE. Show that $\ker(\theta) \lhd$ G.

EXERCISE. A subgroup H is normal in G iff H is a kernel of some homomorphism.

2.2.8 PROPOSITION. *Let $N \lhd G$, then G/N is abelian iff $G' \subset N$.*

PROOF. Let π be the canonical homomorphism, π is surjective thus elements of G/N are of the form $\pi(g)$ for some $g \in$ G. Now

G/N is abelian iff $[\pi(g), \pi(h)] = e$, for all $g, h \in$ G.

iff $\pi([g, h]) = e$, for all $g, h \in$ G.

iff $[g, h] \in \ker(\pi)$,for all $g, h \in$ G.

iff $[g, h] \in$ N, for all $g, h \in$ G.

iff $G' \subset$ N.

2.2.9 COROLLARY. *G/G' is abelian.*

In fact G' is minimal among all normal subgroups with abelian factor group. G/G' is called abelianization of G.

2.2.10 PROPOSITION. *Let $\varphi : G \to H$ be a homomorphism. Let $N = ker(\varphi)$. Then $\varphi(x) = \varphi(y)$ iff $Nx = Ny$, for all $x, y \in G$.*

PROOF. If $\varphi(x) = \varphi(y)$ then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e$. so $xy^{-1} \in N$, it follows that $Nx = Ny$. Conversely, assume that $Nx = Ny$ then $y = nx$ for some $n \in N$. Thus $\varphi(y) = \varphi(nx) = \varphi(n)\varphi(x) = e\varphi(x) = \varphi(x)$.

2.2.11 COROLLARY. *If φ is a homomorphism then φ is injective iff $ker(\theta) = e$.*

PROOF: EXERCISE.

2.3 Homomorphism Theorems

2.3.1 THEOREM. ***(First Homomorphism Theorem)**. Let φ: G $\to$ H be a surjective homomorphism with N = $ker(\varphi)$. Then G/N $\cong$ H. In fact $\exists!$ Surjective isomorphism θ : G/N $\to$ H such that $\pi\theta = \varphi$.*

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & H \\ & G/N \arrow[ur, "\theta"'] & \end{tikzcd}$$

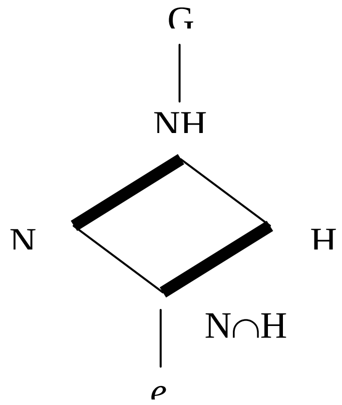
PROOF. If θ exist then for $g \in G$ we have $((g)\pi)\theta = (g)\varphi$. i.e., $(Ng)\theta = (g)\varphi$. This proves that θ is unique, also shows us how to define θ. So we define $\theta : G/N \to H$ by $(Ng)\theta = (g)\varphi$, we need to show that θ is well-defined. i.e., if $Nx = Ny$ then $(Nx)\theta = (Ny)\theta$, but by previous Proposition $Nx = Ny$ then $(x)\varphi = (y)\varphi$, since $N = \ker(\varphi)$. To show that θ is a homomorphism we note that $(NxNy)\theta = (Nxy)\theta = (xy)\varphi = (x)\varphi\ (y)\varphi = (Nx)\theta(Ny)\theta$. Therefore θ is a homomorphism. To show that θ is 1-1 note that $Nx \in \ker(\theta)$ iff $x \in \ker(\varphi)$ i.e., iff $x \in N$. To show that θ is onto we note that if $h \in H$ then there is $x \in G$ such that $h = (x)\varphi$. Thus $h = (Nx)\theta$. This completes the proof.

EXERCISE. Prove that $G/\mathbf{Z}(G) \cong Inn(G)$.

Note if φ is not surjective then we have this version $G/\ker(\varphi) \cong \varphi(G)$.

2.3.2 COROLLARY. *Let $N \lhd G$, $H \leq G$ then $N \cap H \lhd H$ and $NH/N \cong H/(H \cap N)$.*

PROOF. Let $\varphi : H \to G/N$ be defined by $\varphi(h) = Nh$ (i.e., $\varphi = \pi|_H$). We need to find $\ker(\varphi)$. $h \in \ker(\varphi)$ iff $Nh = N$ i.e., $h \in N$. i.e., $\ker(\varphi) = N \cap H$. Now Obviously $\varphi(H) = NH/N$. So by the Theorem $NH/N \cong H/(H \cap N)$.



2.3.3 THEOREM. *(Correspondence Theorem) Let $\varphi : G \to H$ be a surjective homomorphism with $\ker(\varphi) = N$. Let $S = \{ U \mid N \leq U \leq G\}$, $T = \{ V \mid V \leq H\}$. Then the following hold:*

(a) There is a bijective correspondence $\alpha : S \to T$ given by $\alpha(U) = \varphi(U)$. And $\alpha^{-1}(V) = \{ g \in G \mid \varphi(g) \in V\}$.
(b) If $V = \alpha(U)$ then $U \lhd G$ iff $V \lhd H$.
(c) If $V = \alpha(U)$ then $|G:U| = |H:V|$
(d) If $V = \alpha(U)$, $U \lhd G$, $V \lhd H$ then $G/U \cong H/V$.

PROOF. (a) Since $U \leq G$ then $\alpha(U) = \varphi(U)$ is a subgroup of H. Also if $V \leq H$ then $\alpha^{-1}(V) = \{ g \in G \mid \varphi(g) \in V\}$ is a subgroup of G containing N. Let $\beta(V) = \{ g \in G \mid \varphi(g) \in V\}$, $V \leq H$. So $\beta : T \to S$.
Now if we can show that $\beta(\alpha(U)) = U$ then α, β will be bijections and inverses of each other. Let $x \in \beta(\alpha(U))$ then $\varphi(x) \in \alpha(U) = \varphi(U)$, so $\varphi(x) = \varphi(u)$ for some $u \in U$. It follows that $Nx = Nu$. i.e., $x \in Nu \subset U$, therefore $x \in U$.

Conversely, Let $u \in U$ then $\varphi(u) \in \varphi(U) = \alpha(U)$. Thus $u \in \beta(\alpha(U))$. Similarly, we can show that $\alpha(\beta(V)) = V$.

(b) Let $\alpha(U) = V$. Assume that $U \lhd G$, let $h \in H$, therefore there is $g \in G$ with $\varphi(g) = h$. Now $V^h = \varphi(U)^{\varphi(g)} = \varphi(U^g) = \varphi(U) = V$. It follows that $V \lhd H$.

(c) Let $\alpha(U) = V$. Let θ:{all cosets of U in G}$\rightarrow${set of all cosets of V in H}, defined by $\theta\,(Ux) = V\varphi(x)$. It easy to show that θ is a bijection. Thus $|G:U| = |H:V|$.

(d) If $U \lhd G$, $V \lhd H$, $\varphi(U) = V$, the bijective map $\theta: G/U \rightarrow H/V$ is an isomorphism, since $(UxUy)\theta = (Uxy)\theta = \varphi(U)\varphi(xy) = \varphi(U)\varphi(x)\varphi(y) = \varphi(U)\varphi(x)\varphi(U)\varphi(y) = (Ux)\theta(Uy)\theta$. The proof is complete.

2.3.4 COROLLARY. *Let $N \lhd G$ then every subgroup of G/N has the form H/N for some subgroup H with $N \leq H \leq G$. Moreover $H/N \lhd G/N$ iff $H \lhd G$ and $(G/N)/(H/N) \cong G/H$.*

PROOF. EXERCISE.

2.4 Group Action

2.4.1 DEFINITION. *Given a set Ω and a group assume we have a rule which assigns an element of Ω for each $\alpha \in \Omega$, $g \in G$. we write $\alpha \bullet g \in \Omega$. So we have a function $f: \Omega \times G \rightarrow \Omega$, $f(\alpha, g) = \alpha \bullet g \in \Omega$, such that*

1. $(\alpha \bullet g)\bullet h = \alpha \bullet (gh)$ for all $\alpha \in \Omega$ and $g, h \in G$.
2. $\alpha \bullet e = \alpha$, for all $\alpha \in \Omega$.
*We say that G **acts** on Ω ($\bullet$ is the action).*

EXAMPLE. (1) Let $G \leq sym(\Omega)$ and let $\alpha \bullet g = (\alpha)g$ for all $\alpha \in \Omega$.

(2) Let G be a group, $\Omega = G$, define $x \bullet g = xg$. (this is called the regular action, or right multiplication action).
Note to define an action with left multiplication $x \bullet g = g^{-1}x$.

(3) Let G be a group, $\Omega = G$, define $x \bullet g = x^g = g^{-1}xg$ (called conjugation action).

(4) Let G be a group, $\Omega = \{H \mid H \leq G\}$, define $H \bullet g = H^g$ (called conjugation action on subgroups).

(5) Let G be a group, $\Omega = \{Hg \mid g \le G\}$, define $Hg \bullet x = Hgx$.

EXERCISE. Show that these are actions.

We use these actions for two reasons

(1) produce normal subgroups

(2) count things.

2.4.2 THEOREM. *Let G act on Ω. For any $g \in G$ define the map $\pi_g: \Omega \to \Omega$ as follows $(\alpha)\pi_g = \alpha \bullet g$. Then $\pi_g \in sym(\Omega)$. Furthermore the map $\theta: G \to sym(\Omega)$ defined by $\theta(g) = \pi_g$ is a homomorphism.*

PROOF. Let $g, h \in G$, $\alpha \in \Omega$. $((\alpha)\pi_g)\pi_h = (\alpha \bullet g)\pi_h = (\alpha \bullet g)h = (\alpha) \bullet (gh) = (\alpha)\pi_{gh}$. So $\pi_g\pi_h = \pi_{gh}$.

Now π_e is the identity permutation, since $(\alpha)\pi_e = \alpha \bullet e = \alpha$.

Thus $\pi_g\pi_g\text{-}1 = \pi_e$ therefore π_g is 1-1 and onto. Hence $\pi_g \in Sym(\Omega)$.

To see that θ is a homomorphism we have $\theta(gh) = \pi_{gh} = \pi_g\pi_h = \theta(g)\theta(h)$.

Note $\ker(\theta) = \{ g \in G \mid \alpha \bullet g = \alpha \text{ for all } \alpha \in \Omega\}$. Is called the **kernel** of the action.

2.4.3 THEOREM. *(n!) Let $H \le G$ and assume $|G:H| = n < \infty$. Then there is a normal subgroup $N \le H$ and $|G:N|$ divides $n!$.*

PROOF. Let $\Omega = \{Hx \mid x \in G\}$ then $|\Omega| = n$. G acts on Ω by right multiplication. Let N = kernel of the action then $N \lhd G$. To see that $N \le H$, for $x \in N$ then x fixes H i.e., $Hx = H$, therefore $x \in H$. Hence $N \le H$.

Now, $G/N = G/\ker(\theta) \cong \theta(G) \le sym(\Omega)$. Therefore by Lagrange's Theorem $|G/N|$ divides $|sym(\Omega)| = n!$.

EXERCISE. Prove that the $\ker(\theta) = \cap\{H^g \mid g \in G\}$.

EXERCISE. Prove that if $|G:H| = 2$ then $H \lhd G$.

EXERCISE. Prove that if $|G:H| = p$ with p is the smallest prime dividing $|G|$ then $H \lhd G$.

EXERCISE. Prove that if $H \leq G$ with $|G:H| < \infty$ then there is $N \lhd G$ with $|G:N| < \infty$.

2.4.4 DEFINITION. *Let G be a group acting on Ω, let $\alpha \in \Omega$ then the* ***orbit*** *of α under the given action is $O_\alpha = \{ \alpha \bullet g \mid g \in G\}$.*

2.4.5 THEOREM. *Let G acts on Ω, let O_α be the orbit of α, $\alpha \in \Omega$. Then the following hold:*

(1) If $\beta \in O_\alpha$ then $\beta \bullet g \in O_\alpha$ for all $g \in G$.
(2) If $\beta, \gamma \in O_\alpha$ then $\gamma = \beta \bullet g$ for some $g \in G$.
(3) If $\beta \in O_\alpha$ then $O_\alpha = O_\beta$.
(4) If $O_\alpha \cap O_\beta \neq \varnothing$ then $O_\alpha = O_\beta$.

PROOF. EXERCISE.

2.4.6 COROLLARY. *Ω is partitioned by the different orbits.*
PROOF. EXERCISE.

EXAMPLE.(1) Let $H \leq G$, let H acts on G by right multiplication. i.e., $g \bullet h = gh$ then the orbit $O_g = gH$.
(2) If G acts on G by conjugation then for $x \in G$; $O_x =$ is the **conjugacy class** of $x = cl_G(x) = \{ y \in G \mid y = x^g \text{ for some } g \in G\}$.

EXERCISE. Show that if $|cl_G(x)| = 1$ iff $x \in Z(G)$.

2.4.7 DEFINITION. *An action is called* ***transitive*** *if there is only one orbit.*

EXAMPLE. The regular action is transitive, since for every pair of elements x, y there is $g \in G$ such that $xg = y$.

Note that elements of the same conjugacy class have the same order. Elements of order 2 are called involutions.

2.4.8 DEFINITION. *Let G act on Ω, let $\alpha \in \Omega$. The set $G_\alpha = \{ g \in G \mid \alpha \bullet g = \alpha\}$ is called the* ***stabilizer*** *of α.*

EXERCISE. Show that $G_\alpha \leq G$.

2.4.9 THEOREM. *(Fundamental Counting Principle) Let G act on Ω, let O_α be an orbit for $\alpha \in \Omega$. Then there is a bijection between $\{G_\alpha x \mid x \in G\}$ and O_α (i.e., $|O_\alpha| = |G:G_\alpha|$).*

PROOF. Define the mapping

$$\varphi : \{G_\alpha x \mid x \in G\} \to O_\alpha \text{ as follows}$$

$\varphi(G_\alpha x) = \alpha \bullet x$.

We need to show that φ is well-defined, i.e., if $G_\alpha x = G_\alpha y$ then $\alpha x = \alpha \bullet y$.

But if $G_\alpha x = G_\alpha y$ then $y \in G_\alpha x$ i.e., $y = gx$ for some $g \in G_\alpha$ (i.e., g fixes α). Therefore $\alpha \bullet y = \alpha \bullet gx = (\alpha \bullet g) \bullet x = \alpha \bullet x$. To show that φ is 1-1, let $\alpha \bullet x = \alpha \bullet y$ then $\alpha = \alpha xy^{-1}$therefore $xy^{-1} \in G_\alpha$ hence $x \in G_\alpha y$, thus $G_\alpha x = G_\alpha y$. To show that φ is onto, let $\beta \in O_\alpha$ we know that there is $g \in G$ with $\beta = \alpha \bullet x$. So $\varphi(G_\alpha g) = \alpha \bullet g = \beta$. Hence φ is a bijection.

2.4.10 COROLLARY.

(1) $|O_\alpha| = |G:G_\alpha|$.

(2) If $|G| < \infty$ then $|O_\alpha| = |G|/|G_\alpha|$.

(3) Let $x \in G$, then $|cl_G(x)| = |G:C_G(x)|$.

(4) If $|G| < \infty$ and G has only two conjugacy classes then $|G| = 2$.

PROOF. EXERCISE.

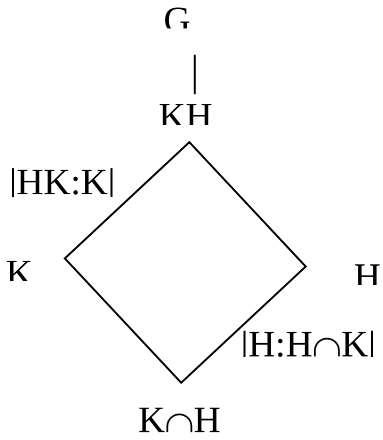
2.4.11 DEFINITION. *Let G act on the set of subgroups of G by conjugation. For $H \leq G$, $G_H = \mathbf{N}_G(H)$. is called the* ***normalizer*** *of H in G.*

EXERCISE. Show that

(1) $H \leq \mathbf{N}_G(H)$

(2) Show that $\mathbf{N}_G(H)$ is the largest subgroup in which $H \lhd \mathbf{N}_G(H)$.

2.4.12 Theorem. *Let* $H, K \leq G$, $|H|, |K| < \infty$ *then* $|HK| = |H||K|/|H \cap K|$.



Proof. $HK = \cup\{Hk \mid k \in K\}$, thus $|HK| = |H||\{Hk \mid k \in K\}|$. Let K act on $\Omega = \{Hg \mid g \in G\}$ therefore the set $\{Hk \mid k \in K\}$ forms one orbit of H under the action. Therefore, by The Fundamental Counting Principle, $|\{Hk \mid k \in K\}| = |K:K_H|$, where K_H is the stabilizer of H in K. Now given $x \in K$, we have $x \in K_H$ iff $Hx = H$ iff $x \in H$. In other words $K_H = K \cap H$. Therefore $|HK| = |H||K:K \cap H| = |H||K|/|H \cap K|$.

2.4.13 Definition. *Let p be a prime number, a finite p-group is a group G with* $|G| = p^n$ *for some integer* $n \geq 0$.

2.4.14 Proposition. *Let P be a p-group and assume that P acts on* Ω. *If p does not divide* $|\Omega|$ *then P fixes some element of* Ω.

Proof. Write $|\Omega| = |O_1| + |O_2| + \ldots + |O_k|$, where O_i are the different orbits. Thus $\exists$ an orbit O_i such that p does not divide $|O_i|$. By Fundamental Counting Principle, $|O_i|$ divides $|P|$. Therefore $|O_i| = 1$. Thus there is $\alpha \in \Omega$ such that $O_\alpha = \{\alpha\}$, and hence, $\alpha \bullet g = \alpha$ for all $g \in P$.

2.4.15 THEOREM. *Let P be a p-group and $N \lhd P$, assume that $|N| > 1$. Then $|N \cap Z(P)| > 1$.*

PROOF. Let P act by conjugation on $\Omega = N \backslash \{e\}$, then $|\Omega| = |N| - 1$. But $|N| = p^{\alpha}$ for some $\alpha > 0$. So $|\Omega| = p^{\alpha} - 1$, which is not divisible by p. therefore there is some element $x \in N$ fixed under P, i.e., $x^g = x$ for all $g \in G$. Thus $x \in Z(P)$, it follows that $x \in N \cap Z(P)$.

2.4.16 COROLLARY. *Let P be a p-group, $|P| > 1$. Then $|Z(P)| > 1$.*

PROOF. EXERCISE.

2.4.17 DEFINITION. *A group G is called **simple** if G has no proper normal subgroups.*

2.4.18 COROLLARY. *If $|G| = p^{\alpha}$, p prime, G is simple then $\alpha = 1$.*

PROOF. EXERCISE.

Chapter III

1. Sylow Theory
2. Nilpotent Groups
3. Direct Product
4. Permutation Groups

3.1 Sylow Theory

3.1.1 DEFINITION. *Let $|G| = n = p^{\alpha}k$ where p does not divide k. p^{α} is called the p-part of n. A subgroup $H \leq G$ is called a **sylow p-subgroup** if $|H| = p^{\alpha}$. The set of all sylow p-subgroups of G is denoted by $syl_p(G)$.*

Remark: (1) If $H \leq G$, $H \in syl_p(G)$ iff $|H|$ is a power of p and p does not divide $|G:H|$.

(2) If $H \in syl_p(G)$, $g \in G$ then $H^g \in syl_p(G)$.

3.1.2 PROPOSITION. *If p is a prime number, then*

$$\binom{p}{i} \equiv 0 \ (\mathrm{mod}\ p), \text{ for all } 1 \leq i \leq p.$$

3.1.3 COROLLARY. *For every integer x, $(x + 1)^p \equiv (x^p + 1) \bmod p$.*

3.1.4 PROPOSITION. $\binom{p^{\alpha}k}{p^{\alpha}} \equiv k \ (\mathrm{mod}\ p)$, *for prime p.*

3.1.5 THEOREM. *(**Sylow Existence**) For a prime p, if G is finite then $syl_p(G) \neq \varnothing$.*

PROOF. Let $n = |G| = p^{\alpha}k$, p does not divide k. Let $\Omega = \{X \subset G \mid |X| = p^{\alpha}\}$. Then $|\Omega| = \binom{p^{\alpha}k}{p^{\alpha}} \equiv k \ (\mathrm{mod}\ p) \neq 0 \bmod p$. Let G act on Ω by right multiplication, i.e., $X \bullet g = Xg$, for all $g \in G$.

So, there must be an orbit O_X with $|O_X|$ is not congruent to 0 (mod p). Then by The Fundamental Counting Principle, $|O_X| = |G:G_X|$, and p does not divide $|G:G_X|$. Therefore p does not divide $|G|/|G_X|$, it follows that $p^{\alpha} \mid |G_X|$. Therefore $p^{\alpha} \le |G_X|$. To get the reverse inequality we know that $Xh = X$ for $h \in G_X$. Fix $x \in X$, then $xh \in X$ for all $h \in G_X$. It follows that $xG_X \subset X$. Thus $|G_X| \le |X|$. Hence $|G_X| = |X|$, $G_X \in syl_p(G)$.

3.1.6 THEOREM. *(Sylow Conjugacy and Development Theorem). Let G be a finite group. Let $P \le G$ be a p-group and let $S \in syl_p(G)$. Then $P \le S^x$ for some $x \in G$.*

PROOF: Let $\Omega = \{Sx \mid x \in G\}$ and let P act on Ω by right multiplication. Then we have $|\Omega| = |G:S|$ which is not divisible by p, since S is a sylow p-subgroup. Therefore there is an orbit O_α with p does not divide $|O_\alpha|$. But since P is a p-group then all orbits must divide $|P|$. It follows that there is an orbit with $|O_\alpha| = 1$. So P stabilizes Sx for some $x \in G$, i.e.,if $y \in P$ then $Sx = Sxy$ and hence $x^{-1}Sx = x^{-1}Sxy$ i.e., $S^x = S^xy$. Therefore $y \in S^x$ i.e., $P \subset S^x$.

3.1.7 COROLLARY. *(Sylow conjugacy Theorem) Let P, Q be two sylow p-group, for a prime number p. Then there is an element $x \in G$ such that $P^x = Q$.*

PROOF. Take S in the Theorem to be Q. then $Q \le P^x$. Now since both have the same cardinality $|Q| = |P^x|$, then $Q = P^x$.

3.1.8 COROLLARY. *(Sylow development Theorem) Let P be a p-group, for a prime number p. Then there is a sylow p-group Q such that $P \le Q$.*

PROOF. Take S^x in the Theorem to be Q. then $P \le Q$.

3.1.9 COROLLARY. *Let G be a finite group, let $P \in syl_p(G)$.*
Then $|syl_p(G)| = |G:\mathbf{N}_G(P)|$. In particular $|syl_p(G)|$ divides $|G:P|$.
PROOF: EXERCISE.

3.1.10 COROLLARY. *Let $S \in syl_p(G)$. Then the following are equivalent:*
(i) $S \lhd G$.
(ii) S is the unique sylow p-subgroup of G.
(iii) Every p-subgroup of G is contained in S.
(iv) S is characteristic in G.

PROOF: EXERCISE.

Write $n_p = |syl_p(G)|$, now if $|G| = p^\alpha m$. Then $n_p \mid m$.

3.1.11 THEOREM. *(Sylow Counting) Let G be a finite group. Then $n_p \equiv 1 \mod p$.*

PROOF: Let $P \in syl_p(G)$. Let P act by conjugation on $\Omega = syl_p(G)$. Then $\{P\}$ forms one orbit by itself. Now we claim that every other orbit has size strictly bigger than one. To see this, let $S = S^x$, $x \in P$ then $x \in N_G(S)$, So $P \leq N_G(S)$. Since $P \in syl_p(G)$ then $syl_p(N_G(S))$. $S \lhd N_G(S)$ implies that S is the unique sylow p-subgroup of $N_G(S)$. Therefore $P = S$. Therefore $n_p = 1 + |O_1| + |O_2| + \dots |O_k|$. where p divides $|O_i|$ since $|O_i|$ divides $|P|$. Hence $n_p \equiv 1 \mod p$.

3.1.12 COROLLARY. *Let $Q \in syl_p(G)$, P any p-subgroup of G. Suppose that $P \leq N_G(Q)$ then $P \leq Q$.*

PROOF. EXERCISE.

3.1.13 COROLLARY. *If $|G| = 72$ then G is not simple.*

PROOF. $72 = 2^3 3^2$. We will compute $n_3(G)$. Since n_3 must divide 2^3, then $n_3 \in \{1, 2, 4, 8\}$. Since $n_3 \equiv 1 \mod 3$, then $n_3 \in \{1, 4\}$.
If $n_3 = 1$ then G is not simple since it contains a normal subgroup of order 9. If $n_3 = 4$ then $|G:\mathbf{N}(S)| = 4$ for some $S \in syl_3(G)$. Therefore by (n!) Theorem there is a normal subgroup $N \subset N(S)$. If $|N| > 1$ then G is not simple. So, assume that $|N| = 1$, then $|G| = |G/N| \mid 4!$, but 72 does not divide 24. Thus $n_3 \neq 4$. Therefore G is not simple.

3.1.14 COROLLARY. *If $|G| = pq$ where p, q are primes with $p > q$, then*
(a) G has a normal sylow p-subgroup
(b) G is cyclic unless $q \mid (p-1)$.

PROOF: $n_p \mid q$ so $n_p = 1$ or $n_p = q$. But if $n_p = q$ then $q \equiv 1(\text{mod } p)$, i.e., $q \geq p + 1$ which contradicts the hypothesis that $q < p$. Thus $n_p = 1$.
Now assume that q does not divide $p - 1$. i.e., p is not congruent to 1 mod q. $n_q = 1 \text{mod } q$, therefore $n_q = 1$. Let $P \in syl_p(G)$, $Q \in syl_q(G)$. Then $P \lhd G$, $Q \lhd G$, $P \cap Q = \{e\}$. Therefore elements of P commutes with elements of Q. Let $x \in P$, $y \in Q$ with $x \neq e \neq y$ therefore $xy = yx$, therefore $o(xy) = pq$, Thus $G = \langle xy \rangle$.

3.1.15 COROLLARY. *Let $|G| = p^2q$, $q \neq p$ be primes. Then G has a normal subgroup.*

PROOF: Assume $n_p > 1$, $n_q > 1$ then $n_p \mid q$ and therefore $n_p = q$. it follows that $q \equiv 1 \text{ mod } p$ and this gives that $q = 1 + kp$. Hence $n_q = p$ or $n_q = p^2$.
If $n_q = p$ then $p \equiv 1 \text{ mod } q$, therefore $p > q$, contradicting the fact that $q > p$. If $n_q = p^2$, then the number of elements of order q is $p^2(q\text{-}1)$, so the rest of the elements is $p^2q - p^2(q - 1) = p^2$, but this is only the number of elements in one sylow p-subgroup, i.e., $n_p = 1$ contradicting our assumption that $n_p > 1$. Therefore either $n_p = 1$ or $n_q = 1$.

3.1.16 COROLLARY. *Let $|G| = p^3q$, $p \neq q$ primes. Then G has a normal sylow subgroup except when $|G| = 24$.*

PROOF: EXERCISE.

3.1.17 THEOREM. ***(Burnside)*** *If $|G| = p^{\alpha}q^{\beta}$, where p, q are primes, then α, $\beta \geq 1$, $|G|$ is not simple.*

PROOF: Omitted.

3.1.18 THEOREM. ***(Frattini Argument)*** *Let $N \lhd G$, with $|N| < \infty$. Let $P \in syl_p(N)$. Then $G = \mathbf{N}_G(P)N$.*

Proof: Let $g \in G$. Then $P^g \subset N^g = N$. But $|P^g| = |P|$. Therefore $P^g \in syl_p(N)$. It follows by Sylow Conjugacy Theorem that P^g, P are conjugate in N. Thus there is an element $n \in N$ such that $P^g = P^n$. It follows that $gn^{-1} \in \mathbf{N}_G(P)$. Hence $g \in \mathbf{N}_G(P)N$, i.e., $G = \mathbf{N}_G(P)N$.

3.1.19 Definition. *Let $\varphi(G) = \cap\{ H \leq G \mid H$ is maximal subgroup in $G\}$. $\varphi(G)$ is called Frattini subgroup.*

3.1.20 Proposition. *Let $|G| < \infty$ and let $H \leq G$. If $\varphi(G)H = G$ then $H = G$.*

Proof: Exercise.

3.1.21 Theorem. *If $|G| < \infty$ then every sylow subgroup of $\varphi(G)$ is normal.*

Proof: Let $F = \varphi(G)$ and let $P \in syl_p(F)$. we know that $F \triangleleft G$ (in fact F is characteristic in G). By Frattini argument $\mathbf{N}_G(P)F = G$, and then by the proposition $\mathbf{N}_G(P) = G$, therefore $P \triangleleft G$.

3.2 Nilpotent Groups

Let P be a finite p-group, $|P| > 1$ the P has a non-trivial center, let $Z_1 = Z(P)$, Z_1 is characteristic in P. If P is not abelian then $Z(P) \neq P$, and hence $P/Z(P)$ is again a p-group and then we do the same, i.e., we find a subgroup Z_2 with $Z_2/Z_1 = Z(P/Z_1)$. Therefore we have the following series of subgroups

$$\{e\} = Z_0 \leq Z_1 \leq Z_2 \leq \ldots \leq Z_k = P.$$

with each Z_i is called ith center, and $(Z_{i+1})/Z_i = Z(P/ Z_i)$.

Note. In p-groups we always get $Z_k = P$ for some k. But in general it might not be true.

3.2.1 DEFINITION. *A set of subgroups $G_0, G_1, \ldots, G_k$ in G is a central series if* $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_k = G$

where each $G_i \lhd G$, and $(G_{i+1})/G_i \subset Z(G/G_i)$, for $0 \le i \le k$, k is finite.

3.2.2 COROLLARY. *A finite p-group has a central series.*

3.2.3 DEFINITION. *A group is called **nilpotent** if it has a central series.*

3.2.4 COROLLARY. *A finite p-group is nilpotent.*

REMARK. Every abelian group is nilpotent.

3.2.5 PROPOSITION. *If $1 < |G| < \infty$ and all its sylow subgroups are normal then $|Z(G)| > 1$.*

PROOF. If $p \mid |G|$, p is prime. Let $P \in syl_p(G)$. Let $Z = Z(P)$. we know that $|Z| > 1$. We claim that $Z \subset Z(G)$. To prove this claim, let $C = C_G(Z)$, we will show that $C = G$, by showing that $|G:C| = 1$. So assume $|G:C| > 1$. Let q be a prime number with $q \mid |G:C|$. Let $Q \in syl_q(G)$. Since $q \mid |G:C|$ we have $Q \neq C$. If $q = p$ then $P = Q$ and because $n_p = 1$, $Z = Z(P)$ thus $P \subset C(Z) = C$ which is a contradiction since $P = Q \not\subset C$. Thus $q \neq p$, and therefore $P \cap Q = \{e\}$, $P \lhd G$, $Q \lhd G$, thus $Q \subset C(P) \subset C$ another contradiction.

3.2.6 THEOREM. *Let G be a finite group. Then the following are equivalent:*

(i) G is nilpotent.

(ii) If $H < G$ then $\mathbf{N}_G(H) > H$. (normalizers grow)

(iii) If M is maximal in G then $M \lhd G$.

(iv) Each sylow of G is normal in G { $\exists!$ Sylow subgroups}

(v) If $N \lhd G$ with $N \neq G$ then $|Z(G/N)| > 1$. { if $N = \{e\}$ then $|Z(G)| > 1$}.

PROOF. (i) $\to$ (ii) Given $H < G$, we have a central series

$$\{e\} = G_0 \le G_1 \le G_2 \le \ldots \le G_k = G.$$

Choose $G_i \subset H$ such that $G_{i+1} \not\subset H$.

Now $H/G_i \subset G/G_i$, $G_{(i+1)}/G_i \subset Z(G/G_i) \subset \mathbf{N}(H/G_i) = N/G_i$ for some $N \leq G$. and $H/G_i \lhd N/G_i$ then by correspondence Theorem $H \lhd N$. Therefore $G_{i+1} \subset N \subset \mathbf{N}_G(H) > H$.

(ii) $\rightarrow$ (iii) Let M be maximal in G, then $M < G$ and by (ii) $\mathbf{N}_G(M) > M$, thus $\mathbf{N}_G(M) = G$ by maximality. Hence $M \lhd G$.

(iii) $\rightarrow$ (iv) Let $P \in syl_p(G)$ for some p, p prime. Let $N = \mathbf{N}_G(P)$. If $N < G$ then by finiteness, $\exists$ a maximal subgroup M with $N \subset M$ then $M \lhd G$. Note $P \subset M$ thus $P \in syl_p(M)$, by Frattini Argument $G = \mathbf{N}_G(P)M = NM = M$, this of course a contradiction. So $N = G$, so $P \lhd G$.

(iv) $\rightarrow$ (v) Given $N \lhd G$, to show that $Z(G/N) > \{e\}$, it suffices by the Proposition to show that each sylow of G/N is normal. We will use property (iv) to prove the same condition on G/N.

Let p be prime, let $P \in syl_p(G)$. Look at $(PN)/N \subset G/N$. $P \lhd G$ by (iv), $N \lhd G$ implies that $PN \lhd G$. Therefore $PN/N \lhd G/N$.

Now we will show that $PN/N \in syl_p(G/N)$. $|PN/N|$ is a p-power, $|G:PN|$ is not divisible by p. Therefore G/N has a normal sylow p-subgroup.

(v) $\rightarrow$ (i) Let $G_0 = \{e\}$, by induction define G_i, $i > 0$, by the formula $G_i/G_{i-1} = Z(G/G_{i-1})$, not all $G_i \lhd G$. If $G_{i-1} < G$ then by (v) $Z(G/G_{i-1}) > \{e\}$. i.e., $G_i/G_{i-1} > \{e\}$ implies that $G_i > G_{i-1}$, and by finiteness of G we have $G_k = G$ for some k. Thus G is nilpotent.

3.2.7 **COROLLARY**. *Let $P \neq \{e\}$ be a finite p-group. Let M be any maximal subgroup of P. Then $M \lhd P$ and P/M is cyclic of order p.*

PROOF: We have $M \lhd P$ since P is nilpotent. Subgroup of P/M are in bijection correspondence with $S = \{U \mid M \leq U \leq P\}$. Maximality implies that $S = \{M, P\}$. Thus P/M has just two subgroups; itself and the identity. Therefore P/M is cyclic of prime order p.

3.2.8 **COROLLARY**. *Last corollary states that if M is maximal than $|P:M|$ $= p$.*

3.2.9 COROLLARY. *If* $|P| = p^{\alpha}$ *and* $0 \le \beta \le \alpha$, *then* $\exists$ *subgroup* $Q \subset P$ *with* $|Q| = p^{\beta}$.

PROOF. EXERCISE.

3.2.10 COROLLARY. *If* $|G| < \infty$, *and* $p^{\beta} \mid |G|$, *where* p *is prime, then there is a subgroup* $Q \subset G$ *with* $|Q| = p^{\beta}$.

PROOF: EXERCISE.

EXERCISE. If $|G| < \infty$, show that $\varphi(G)$ is nilpotent.

EXERCISE. Let G be a finite group.

(i) If $G/\varphi(G)$ is nilpotent show that G is nilpotent.

(ii) If G is nolpotent, $N \lhd G$, show that G/N is nilpotent.

3.3 Direct Product

Give two groups U, V. Let $G = \{(u, v) \mid u \in U, v \in V\}$, i.e., $G = U \times V$. Define the multiplication on G component wise by

$$(u, v)(u', v') = (uu', vv').$$

Identity of G is (e_1, e_2), where e_1 , e_2 is the identity of U, V respectively. And inverse of $(u, v)^{-1}$ is (u^{-1}, v^{-1}). G is a group called the **external direct product** of U, V. Of course $|G| = |U||V|$.

Let $\underline{U} = \{(u, e_2) \mid u \in U\}$, $\underline{V} = \{(e_1, v) \mid v \in V\}$. Easy to see that $\underline{U}$, $\underline{V}$ are subgroups of G. In fact $\underline{U}, \underline{V} \lhd G$, and $\underline{U} \cong U$, $\underline{V} \cong V$.

Similarly, if $U_1, U_2, \dots U_n$ are n groups. Then the external direct product

$G = \{(u_1, u_2, \dots u_n) \mid u_i \in U_i, i = 1, 2, \dots, n\}$.

This product is denoted by $\prod_{i=1}^{n} U_i$. or $\sum_{i=1}^{n} U_i$.

Let $\underline{U}_i = \{(e_1, e_2, \dots, u_i, \dots, e_n) \mid u_i \in U_i,\}$, $i = 1, 2, \dots, n$.

EXERCISE. (i) Show that $\underline{U}_i \lhd G$ for $i = 1, 2, \dots, n$.

(ii) Show that $\underline{U}_i \cong U_i$ for $i = 1, 2, \ldots, n$.

3.3.1 THEOREM. *Let $U_1, U_2, \ldots U_n$ be finite p-groups (Possibly for different primes). Let $G = \prod_{i=1}^{n} U_i$. Then G is nilpotent.*

PROOF: We may assume that U_i is a p_i -group with $p_i \neq p_j$, for $i \neq j$.

Note $|G| = \prod_{i=1}^{n} |U_i|$. Thus $|U_i|$ is the order of a sylow p_i-subgroup of G. But $\underline{U}_i$ has the order equal to U_i and so $\underline{U}_i \in syl_p(G)$. Therefore for each prime $p_i \mid |G|$ a sylow p_i -subgroup is normal in G. Hence G is nilpotent.

3.3.2 DEFINITION. *Given a group G, suppose $M_1, M_2, \ldots, M_n \lhd G$. Assume $G = M_1M_2 \ldots M_n$. Assume also that each $g \in G$ the decomposition $g = x_1\ x_2\ \ldots x_n$ with $x_i \in M_i$ is unique. Then we say that G is the internal direct product of M_i ., $i = 1, 2, 3, \ldots, n$. and this product is denoted by $\prod_{i=1}^{n} \bullet M_i$ or $\sum_{i=1}^{n} \bullet M_i$ if the notation is addition.*

3.3.3 THEOREM. *Let $G = \prod_{i=1}^{n} \bullet M_i$, then*

(i) $(\prod_{i \neq j}^{n} M_i \cap) M_j = \{e\}$.

(ii) $M_i \subset C_G(M_j)$, if $i \neq j$.

(iii) $G \cong \prod_{i=1}^{n} M_i$.

PROOF: (i) Let $g \in \prod_{i \neq j}^{n} M_i \cap M_j$, then $g = x_1\, x_2\, \ldots\, x_n$, $x_j = e_i$. and since $g \in M_i$ thus $g = ee \ldots g \ldots e$. Therefore $g = x_i = e$. by uniqueness of the decomposition.

(ii) By (i) $M_i \cap M_j = \{e\}$ for $i \neq j$. Normality of M_i implies that $M_i \subset C(M_j)$.

(iii) Let $\theta: \prod_{i=1}^{n} M_i \to G$, defined by $\theta((x_1, x_2, \ldots, x_n)) = x_1\, x_2 \ldots x_n$. Clearly θ is an isomorphism.

EXAMPLE. Let $G = Z_{30}$. Let $M_1 = \{0, 15\}$, $M_2 = \{0, 10, 20\}$, $M_3 = \{0, 6, 12, 18, 24\}$. Then by the Theorem, we have $G = M_1 \oplus M_2 \oplus M_3$, Since $M_1 \oplus M_2 \cap M_3 = \{e\}$, $M_1 \cap M_2 = \{e\}$.

3.3.4 COROLLARY. *If G is the direct product of M, N. Then $G/N \cong M$.*

PROOF: EXERCISE.

EXERCISE. If G is the direct product $M \times N$ and $M \times L$, then $N \cong L$. (Cancelation).

3.3.5 THEOREM. *Let $M_1, M_2, \ldots M_n \lhd G$. Assume that $(\prod_{i=1}^{r-1} M_i \cap) M_r = \{e\}$. Then the product $G = M_1 M_2 \ldots M_n$ is direct.*

PROOF: Suppose that $x_1 x_2 \ldots x_n = y_1 y_2 \ldots y_n$, where $x_i, y_i \in M_i$, $i = 1, 2, \ldots, n$. To show that $x_i = y_i$ for all $i = 1, 2, \ldots, n$. Assume that $x_r \neq y_r$ for some r, choose r as larg as possible so that $x_i = y_i$ for $i > r$. Use cancelation to get $x_1 x_2 \ldots x_r = y_1 y_2 \ldots y_r$. Let $u = x_1 x_2 \ldots x_{r-1}$, $v = y_1 y_2 \ldots y_{r-1}$ then $ux_r = vy_r$. Now $v^{-1}u = y_r x_r^{-1} \in M_r$, $u, v \in \prod_{i=1}^{r-1} M_i$ thus $v^{-1}u \in \prod_{i=1}^{r-1} M_i$. Therefore $y_r x_r^{-1} \in (\prod_{i=1}^{r-1} M_i \cap) M_r = \{e\}$. Hence $x_r = y_r$ and this is a contradiction.

EXERCISE. Let G be a finite group. $G = \prod_{i=1}^{n} M_i$, $M_i \lhd G$. Show that $|G| \leq \prod_{i=1}^{n} |U_i|$ with equality holds iff G is the direct product .

3.3.6 COROLLARY. *Assume that G is a finite nilpotent group. Let $P_1, P_2, \ldots, P_n \in syl_{p_i}(G)$ for different primes p_i. then G is the direct product $G = \prod_{i=1}^{n} P_i$.*

PROOF: we know that $P_i \lhd G$, $|G| = \prod_{i=1}^{n} |P_i|$ also $|\prod_{i=1}^{n} P_i|$ is divisible by $|P_i|$, thus $G = \prod_{i=1}^{n} P_i$ and this product is direct.

EXERCISE. Prove that every finite group G is nilpotent iff G is the (direct) product of p-groups.

EXERCISE. Prove that every p-group G is isomorphic to a (direct) product of cyclic groups.

3.3.7 THEOREM. *(**Fundamental Theorem of Finite Abelian Groups**). If G is finite abelian group then G is isomorphic to the direct product of cyclic groups of prime power order i.e.,* $G \cong \prod_{\imath=1}^{\nu} C_i$, $|C_i| = p_i^{\alpha_i}$, $\alpha_i \geq 0$.

3.4 Permutation groups

3.4.1 DEFINITION. *The set of all permutations of a set S is denoted by Sym(S).*

The set of all permutations of the set $\{1,2,\ldots,n\}$ is denoted by S_n.

3.4.2 PROPOSITION. *If S is any nonempty set, then Sym(S) is a group under the operation of composition of functions.*

3.4.3 DEFINITION. *A k-cycle (or a cycle of length k) is a permutation* $\pi = (a_1\ a_2\ \ldots\ a_k)$ *where* $\pi(a_i) = a_{i+1}$, *for* $1 \leq i < k$, *and* $\pi(a_k) = a_1$. π *fixes every other element of S.*

EXERCISE. Show that the order of a cycle of length k is k.

EXERCISE. Show that the order of disjoint cycles is the least common multiple of their lengths.

EXERCISE. If $C = (a_1, a_2, \ldots, a_k)$, $\pi \in S_n$. Prove that

$\pi\,(a_1, a_2, \ldots, a_k)\pi^{-1} = (\pi(a_1), \pi(a_2), \ldots, \pi(a_k))$.

EXERCISE. Let $x, y \in S_n$. Show that x, y are conjugate iff x, y, have the same cycle structure.

3.4.4 DEFINITION. *A transposition is a cycle of length 2.*

EXERCISE. Prove that a k-cycle is the product of k-1 transpositions

3.4.5 THEOREM. *Every permutation in S_n can be written as a product of disjoint cycles. The cycles that appear in the product are unique.*

3.4.6 PROPOSITION. *If a permutation in S_n is written as a product of disjoint cycles, then its order is the least common multiple of the lengths of its cycles.*

3.4.7 DEFINITION. *Any subgroup of the symmetric group Sym(S) on a set S is called a* ***permutation group*** *or* ***group of permutations****.*

3.4.8 THEOREM. *(**Cayley**) Every group is isomorphic to a permutation group.*

3.4.9 DEFINITION. *Let $n > 2$ be an integer. The group of rigid motions of a regular n-gon is called the $n^{\underline{th}}$ dihedral group, denoted by D_n.*

We can describe the $n^{\underline{th}}$ dihedral group as

$$D_n = \{ a^k, a^k b \mid 0 \le k < n \},$$

subject to the relations $o(a) = n$, $o(b) = 2$, and $ba = a^{-1}b$.

3.4.10 THEOREM. *If a permutation is written as a product of transpositions in two ways, then the number of transpositions is either even in both cases or odd in both cases.*

3.4.11 DEFINITION. *A permutation is called* ***even*** *if it can be written as a product of an even number of transpositions, and* ***odd*** *if it can be written as a product of an odd number of transpositions.*

3.4.12 PROPOSITION. *The set of all even permutations of S_n is a subgroup of S_n.*

3.4.13 DEFINITION. *The set of all even permutations of S_n is called the **alternating group** on n elements, and will be denoted by A_n.*

EXERCISE. Show that $|S_n:A_n| = 2$.

3.4.14 THEOREM. *Let G be a group, Ω be a finite set. Assume that there is $g \in G$ that acts " oddly" on Ω. Then $\exists N \triangleleft G$ with $|G:N| = 2$.*

PROOF: The action gives a homeomorphism $\theta: G \to Sym(\Omega)$.
$\theta(g)$ is an odd permutation.
Therefore, $\theta(G) \cap Alt(\Omega) < \theta(G)$, since $\theta(G)$ has an odd permutation. Then we have $|\theta(G):\theta(G) \cap Alt(\Omega)| = 2$. θ is surjective, therefore there is a normal subgroup $N = \theta^{-1}(\theta(G) \cap Alt(\Omega))$ of index 2.

COROLLARY. *Let G be simple, with $|G| > 2$. Let $H \leq G$ such that $|G:H| = n > 1$. Then $|G| \mid n!/2$.*

3.4.15 COROLLARY. *Let $|G| = 2n$ with n odd. Then G has a normal subgroup of order n.*

PROOF: Let $x \in G$ with $o(x) = 2$. We claim that x acts oddly on G. To prove this, let π be the permutation of G induced by x. Since $x^2 = e$, we have $\pi^2 = e$. in fact π fixes no element of G, since If $\pi(g) = g$ then $gx = g$ and this would imply that $x = e$, this is a contradiction. The cycle structure of π consists just of 2-cycles. Thus π is n different cycles, then π is an odd permutation. So N exist.

3.4.16 THEOREM. *A_5 is simple.*

PROOF: If $N \triangleleft G$, assume $N < A_5$. We can show that $N = \{e\}$. Choose N as large as possible. If $3 \mid |N|$ then if $P \in syl_3(N)$ we have $P \in syl_3(A_5)$. Thus by sylow conjugacy N contains all $syl_3(G)$ subgroups of A_5 and therfore it contains all elements of order 3 in A_5. Now if $x \in A_5$, $o(x) = 3$, then the cycle structure of x is $1^2 3$. But we have 20 elements of those 3-cycles, it follows that $|N| \geq 21$, hence $|N| = 30$. And similarly if $5 \mid |N|$ we get $|N| = 30$. It follows that in either case $|N| = 30$. This would imply that $|N| > 1 + 20 + 24 > 30$, which is a contradiction. If $|N| = 2$, or 4, then $|G/N| = 30$ or 15. But G/N is simple by maximality of N, however there is no such group. Thus $N = \{e\}$.

3.4.17 THEOREM. *A_n is simple for all $n \geq 5$.*

PROOF: Omitted.

EXERCISE. Show that if $|G| = 180$ then G is not simple.

EXERCISE. Show that if $|G| = 396$ then G is not simple.

3.5 Operator Groups

3.5.1 DEFINITION. *Given a set S (may be empty), and given a group G (may be infinite). Assume that for every $s \in S$ and for every $g \in G$ there is an element $g^s \in G$ that satisfies $(gh)^s = g^s h^s$. Then G is called a group with operator set S.*

Note. Each $s \in S$ induces an indomorphism (a homomorphism of G into G).

EXAMPLE. Let S = G, action is conjugation.

EXAMPLE. If V is a vector space over a field F. V is a group with operator set F.

3.5.2 DEFINITION. *H is called an s-subgroup of a group G with operator set S (denoted by $H \leq_s G$) if $H \leq G$ and $h^s \in H$ for all $h \in H$.*

3.5.3 DEFINITION. *H is called s-normal in G (denoted by $H \lhd_s G$) if $H \lhd G$ and $H \leq_s G$.*

3.5.4 LEMMA. *If G is a group with operator set S, $H \lhd_s G$, then G/H is a group with operator set S.*

PROOF. Define the action of S on G/H by $(Hg)^s = H g^s$. We need to show that $(Hx)^s = (Hy)^s$ if $Hx = Hy$. Now $x \in H y$ implies that $x = hy$. Then $x^s = (hy)^s = h^s y^s \in Hy^s$. Therefore $(Hx)^s = (Hy)^s$.

3.5.5 DEFINITION. *A homomorphism $\theta : G_1 \to G_2$ is called an s-homomorphism of groups G_1, G_2 with operator set S if $\theta(g^s) = \theta(g)^s$. If θ is onto and 1-1 then θ is called an s-isomorphism.*

3.5.6 LEMMA. *If $\theta : G_1 \to G_2$ is a surjective s-homomorphism then $G_1/ker(\theta) \cong_s G_2$ (G_1 is s-isomorphic to G_2).*

3.5.7 DEFINITION. *A group G is called s-simple if the only s-normal subgroups of G are $\{e\}$, G.*

3.5.8 DEFINITION. *The series $\{G_0, G_1, G_2, \ldots, G_n\}$ is called s-composition series for G if $\{e\} = G_0 \lhd_s G_1 \lhd_s \ldots \lhd_s G_n = G$, with G_{i+1}/G_i are s-simple, $i = 0, 1, \ldots, n-1$.*

3.5.9 LEMMA. *Let G be a group that have an s-composition series. Let $N \lhd_s G$ then N has an s-composition series.*

PROOF: Let $\{e\} = G_0 \lhd_s G_1 \lhd_s \ldots \lhd_s G_n = G$ be an s-composition series for G, let $N_i = N \cap G_i$, Then $\{e\} = N_0 \lhd_s N_1 \lhd_s \ldots \lhd_s N_n = N$, note that $N_{i+1} \lhd G_{i+1}$, since $N \lhd G$. Also $G_i \lhd G_{i+1}$. Thus $G_i \lhd G_iN_{i+1} \lhd G_{i+1}$, it follows that either $G_iN_{i+1} = G_i$ or $G_iN_{i+1} = G_{i+1}$.

Case 1.

$N_{i+1} \subset G_iN_{i+1} = G_i$, So $N_{i+1} \subset G_i$, Thus $N_i = N \cap G_i \supseteq N \cap N_{i+1} = N_{i+1}$.

Case 2.

$G_iN_{i+1} = G_{i+1}$ therefore, $G_{i+1}/G_i = G_iN_{i+1}/G_i \cong N_{i+1} /(G_i \cap N_{i+1}) = N_{i+1}/N_i$. Therefore, N_{i+1}/N_i is s-simple. From case 1 and case 2 we have either $N_{i+1} = N_i$ or N_{i+1}/N_i is s-simple. Delete repeats to get an s-composition series for N.

3.5.10 THEOREM. ***(Jordan Hölder)*** *Let G be an s-group, suppose that*

$\{e\} = N_0 \lhd_s N_1 \lhd_s \ldots \lhd_s N_n = G$

$\{e\} = M_0 \lhd_s M_1 \lhd_s \ldots \lhd_s M_m = G$, be two s-composition series for G. Then

(i) $m = n$.

(ii) Up to possible rearrangements the two series have s-isomorphic factors.

PROOF: We may assume that $n < m$, we will pursue the proof by induction on n. If $n = 1$ then G is s-simple, and so $M_{m-1} = \{e\}$. Thus $m = 1$.

If $N_{n-1} = M_{m-1} = K$ we may assume that $n > 1$.

Case 1. We get

$\{e\} = M_0 \lhd_s M_1 \lhd_s \ldots \lhd_s M_{m-1} = K$

$\{e\} = N_0 \lhd_s N_1 \lhd_s \ldots \lhd_s N_{m-1} = K$.

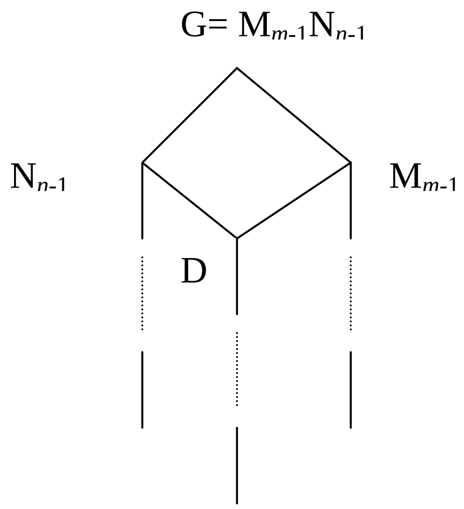
Then by inductive hypothesis in K we get n-1 = m-1, so $n = m$.

Case 2.

If $N_{n-1} \neq M_{m-1}$ but $N_{n-1}M_{m-1}$ is s-normal in G and G/ N_{n-1} ,G/M_{m-1} are s-simple, then $N_{n-1}M_{m-1}$ = G. Let D = $N_{n-1} \cap M_{m-1}$, then D has an s-composition series by the lemma (say)

$\{e\} = D_0 \lhd_s D_1 \lhd_s \ldots \lhd_s D_k = D$

Now inductive hypothesis in N_{n-1} we get n-1 = k +1, and M_{m-1} has one of length k+1 and the other one of length m-1. Hence m-1 = k + 1. It follows that



$m = n$.

3.5.11 Definition. *A group G is called* ***solvable*** *if there is a series*
$\{e\} = N_0 \lhd_s N_1 \lhd_s \ldots \lhd_s N_n = G$, *where each* $N_i \lhd G$ *and each* N_{i+1}/N_i *is abelian.*

Example. Abelian groups are solvable, nilpotent groups are solvable too.

3.5.12 Lemma. *A group G is solvable iff* $G^{(n)} = \{e\}$ *for some* $n < \infty$.

Proof: If $G^{(n)} = \{e\}$ then we have

$\{e\} = G^{(n)} \leq G^{(n-1)} \leq \ldots \leq G' \leq G$, where each one is normal in G and factors are abelian. Conversely, suppose that we have a series

$\{e\} = N_0 \lhd_s N_1 \lhd_s \ldots \lhd_s N_m = G$ with N_{i+1}/N_i abelian thus $N_{m-1} \lhd G$, G/N_{m-1} abelian implies that $G' \subset N_{m-1}$. $G' \subset N_{m-1}$, thus $G'' \subset (N_{m-1})' \subset N_{m-2}$ (since N_{m-2}/N_{m-1} is abelian). Continue to get $G^{(k)} \subset N_{m-k}$. Thus $G^{(m)} \subset N_0$.

3.5.13 THEOREM. *The following are equivalent for a finite group G.*

(i) G is solvable

(ii) Every composition factor is of prime order

(iii) $G^{(n)} = \{e\}$, *for some finite n.*

PROOF: (i) → (ii) Let $\{e\} = N_0 \leq N_1 \leq \ldots \leq N_m = G$, where $N_i \lhd G$, N_{i+1}/N_i abelian. Now insert groups between the N_i's so this series can be refined to be a composition series, say,

$$\{e\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G,$$

with G_{i+1}/G_i are abelian, $i = 0, 1, \ldots, n-1$, and it is a composition factor, so it is simple. Simple and abelian implies that they have prime order.

(ii) → (iii), and (iii) → (i) are done before.

EXERCISES. 1. If G is solvable, $H \leq G$ then H is solvable.

EXERCISES. 2. If G is solvable, $N \lhd G$ then G/N is solvable.

EXERCISES. 3. $N \lhd G$, N is solvable, G/N is solvable then G is solvable.

Chapter IV

4.1 Rings

4.1.1 DEFINITION. *A **ring** R is a non-empty set with two binary operations, denoted by addition and multiplication "+", ".", such that the following properties hold:*

(i) For all a, b, c $\in$ R, a + (b + c) = (a + b) + c and a(bc) = (ab)c.

(ii) For all a, b $\in$ R, a + b = b + a.

(iii) For all a, b, c $\in$ R, a(b + c) = ab + ac and (a + b)c = ac + bc.

(iv) The set R contains an additive identity element, denoted by 0, and a multiplicative identity element, denoted by 1, such that a + 0 = a, 1a = a, and a1 = a, for all a $\in$ R.

(v) For each a $\in$ R, the equation a + x = 0 has a solution x = -a in R, the additive inverse of a.

A ring R is called ***commutative*** if $ab = ba$ for all elements $a, b \in$ R.

commutative examples

EXAMPLE. 1 (**Z**, +, .) is a ring.

EXAMPLE. 2 ($\mathbf{Z}_n$, $\oplus$, $\otimes$) is a ring for any positive integer $n \geq 2$.

Non-commutative examples

We want to include, among other examples, the study of $n\times n$ matrices. Recall that if F is a field, then the set of $n\times n$ matrices $M_n(F)$ corresponds to the set of linear transformations of an n-dimensional
vector space over F. This is a special case of the most general example of a ring. Just as permutation groups are the generic groups (as shown by Cayley's theorem), the generic examples of rings are found in studying endomorphisms of abelian groups.

EXAMPLE. (**Endomorphisms of abelian groups**) Let A be an abelian group, with its operation denoted by +. Let R be the set of all endomorphisms of A. That is, R is the set of all group homomorphisms $f : A \to A$. We can define addition and multiplication of elements of R as follows: if $f, g \in R$, then $(f + g)(x) = f(x) + g(x)$ and $(f.g)(x) = f(g(x))$ for all $x \in A$.
R forms a ring and is denoted by $End(A)$.

EXAMPLE. (**Polynomial Rings**) Let R be any ring. We let R[x] denote the set of infinite tuples $(a_0, a_1, a_2, \ldots)$ such that $a_i \in R$ for all i, and $a_i \neq 0$ for only finitely many terms a_i. Two sequences are equal if and only if all corresponding terms are equal. We introduce addition and multiplication as follows:
$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$
$(a_0, a_1, a_2, \ldots).(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$,
where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.
With these operations it can be shown that $R[x]$ is a ring.
We can identify $a \in R$ with $(a, 0, 0,\ldots) \in R[x]$, then $(1, 0, 0, \ldots)$ is an identity for $R[x]$. If we let $x = (0, 1, 0,\ldots)$, then the elements of $R[x]$ can be expressed in the form

$$a_0 + a_1x + \ldots + a_{m-1}x^{m-1} + a_mx^m,$$

allowing us to use our previous notation for the ring of polynomials over R in the indeterminate x.
Note that although the elements of R need not commute with each other, they do commute with the indeterminate x.
If n is the largest nonnegative integer such that $a^n \neq 0$, then we say that the polynomial has degree n, and a^n is called the leading coefficient of the polynomial.

EXAMPLE. (**Differential operator rings**) Consider the homogeneous linear differential equation $a_n(x)D^ny + \ldots + a_1(x)Dy + a_0(x)y = 0$, where the solution $y(x)$ is a polynomial with complex coefficients, and the terms $a_i(x)$ also belong to C[x]. The equation can be written in compact form as L(y) = 0, where L is the differential operator

$$a_n(x)D^n + \ldots + a_1(x)D + a_0(x) = 0,$$

with D = d/dx. Thus the differential operator can be thought of as a polynomial in the two indeterminates x and D, but in this case the indeterminates do not commute, since $D(xy(x)) = y(x) + x\,D(y(x))$,
yielding the identity $Dx = 1 + xD$.
Repeated use of this identity makes it possible to write the composition of two differential operators in the standard form

$$a_0(x) + a_1(x)D + \ldots + a_n(x)D^n,$$

and we denote the resulting ring by C[x][D].

EXAMPLE. (**Group algebras**) Let K be a field, and let G be a finite group of order n, with elements $1 = g_1, g_2, \ldots, g_n$. The group algebra KG is defined to be the n-dimensional vector space over K with the elements of G as a basis. Vector addition is used as the addition in the ring. Elements of KG can be described as sums of the form $\sum_{i=0}^{n} c_i g_i$ and multiplication is defined as for polynomials, where the product $g_i\, g_j$ is given by the product in G.

EXAMPLE. (Matrix rings) Let R be a ring. We let $M_n(R)$ denote the set of all $n\times n$ matrices with entries in R. For $[a_{ij}]$ and $[b_{ij}]$ in $M_n(R)$, we use componentwise addition $[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}]$ and the multiplication is given by $[a_{ij}].[b_{ij}] = [c_{ij}]$ where $[c_{ij}]$ is the matrix whose j, k-entry is $c_{jk} = \sum_{i=0}^{n} a_{ji}b_{ik}$.

4.1.2 DEFINITION. *Let R be a ring, and let $a \in R$. If $ab = 0$ for some nonzero $b \in R$, then a is called a* ***left zero divisor****. Similarly, if $ba = 0$ for some nonzero $b \in R$, then a is called a* ***right zero divisor****. If a is neither a left zero divisor nor a right zero divisor, then a is called a regular element.*
The element $a \in R$ is said to be ***invertible*** *if there exists an element $b \in R$ such that $ab = 1$ and $ba = 1$. The element a is also called a unit of R, and its multiplicative inverse is usually denoted by a^{-1}. The set of all units of R is denoted by U(R).*

EXERCISE. In any ring R, show that the following is true for all $a, b \in$ R:

(a) $0.a = 0$.

(b) $(-1)a = -a$.

(c) $(-a)b = a(-b) = -ab$.

(d) if u is a unit then u is not a zero divisor.

4.1.3 PROPOSITION. *Let R be a ring. Then the set U(R) of units of R is a group under the multiplication of R.*

PROOF. EXERCISE.

4.1.4 DEFINITION. *A ring R in which each nonzero element is a unit is called a division ring or skew field.*

4.1.5 DEFINITION. *A commutative ring R in which each nonzero element is a unit is called a field.*

EXAMPLE. Let R_1, R_2 be two rings. Let $R = R_1 \oplus R_2 = \{(r_1, r_2) \mid r_1 \in R_1, r_2 \in R_2\}$. Then R is a ring with addition and multiplication defined componentwise.

4.1.6 DEFINITION. *Let R be a ring. A nonempty subgroup I of R under addition is called an* ***ideal*** *of R if $ra, ar \in I$, for all $a \in I$ and $r \in R$. I is called* ***left ideal*** *if only $ra \in I$, and is called* ***right ideal*** *if only $ar \in I$.*

4.1.7 PROPOSITION. *Let R be a commutative ring. Then R is a field if and only if it has no proper nontrivial ideals.*

PROOF. Assume that R is a field. Let I be an ideal, if there is $a \in$ I, $a \neq 0$. Then a has an inverse a^{-1}. Therefore $aa^{-1} \in$ I, by definition of I. Therefore $1 \in$ I, it follows that for every $b \in$ R, $b = b.1 \in$ I. Thus R $\subset$ I.

Conversely, If R is a ring with no proper ideals then for every $a \in$ R, $a \neq 0$ the ideal Ra = R, thus there is an element $b \in$ R, such that $ba = 1$. Therefore, a is a unit. Hence R is a field.

4.1.8 DEFINITION. *A ring R with no proper ideals is called* ***simple***.

EXAMPLE. Let R = **Z**, nZ = $\{nz \mid z \in \mathbf{Z}\}$ is an ideal for every $n \in \mathbf{Z}$.

4.1.9 DEFINITION. *Let I be a proper ideal of the commutative ring R. Then I is said to be a* ***prime ideal*** *of R if for all a, b $\in$ R it is true that ab $\in$ I implies a $\in$ I or b $\in$ I.*

4.1.10 DEFINITION. *The ideal I is said to be a* ***maximal ideal*** *of R if for all ideals J of R such that I $\subset$ J $\subset$ R, either J = I or J = R.*

4.1.11 DEFINITION. *For an ideal I of a commutative ring R, the set $\{a + I \mid a \in R\}$ of cosets of I in R (under addition) is denoted by R/I. The set R/I forms a group under addition.*

The next theorem justifies calling R/I the factor ring of R modulo I.

4.1.12 THEOREM. *If I is an ideal of the commutative ring R, then R/I is a commutative ring, under the operations*

$$(a + I) + (b + I) = (a + b) + I \text{ and } (a + I)(b + I) = ab + I, \text{ for all } a, b \in R.$$

PROOF. EXERCISE.

4.1.13 DEFINITION. *Let R, S be rings. A function $\varphi : R \to S$ is called a* ***ring homomorphism*** *from R into S if the following two conditions hold:*

(a) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(b) $\varphi(ab) = \varphi(a)\varphi(b)$, for all a, b $\in$ R.

We denote $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$.

A ring homomorphism that is one to one and onto is called **isomorphism**, and in this case R and S are called **isomorphic** and denoted by R $\cong$ S. If R = S then it is called an **automorphism** of R.
of course (a) says that φ is a group homomorphism. This implies that all homomorphism theorems for groups hold for rings.

EXERCISE. Show that if φ is a homomorphism then kerφ is an ideal.

4.2 Integral domains

4.2.1 DEFINITION. *A commutative ring R is called an* ***integral domain*** *if for all a, b $\in$ R, ab = 0 implies a = 0 or b = 0.*

The ring of integers Z is the most fundamental example of an integral domain. The ring of all polynomials with real coefficients is also an integral domain, but the larger ring of all real valued functions is not an integral domain. The cancellation law for multiplication holds in R if and only if R has no nonzero divisors of zero. One way in which the cancellation law holds in R is if nonzero elements have inverses in a larger ring; the next two results characterize integral domains as subrings of fields (that contain the identity 1).

4.2.2 DEFINITION. *A subset S of a ring R is called a* ***subring*** *if*
(a) (S, +) is a subgroup of R.
(b) multiplication is a binary operation on S.
i.e., a subring is a subset of R that is a ring under the same operations of R.
Subrings of R do not have to have the same multiplicative identity of R. We can see this clear in the following example.

EXAMPLE. Let R = $M_{2\times 2}(\mathbf{R})$. Let S = { $[a_{ij}]$ | $a_{12} = 0$, $a_{21} = 0$, $a_{22} = 0$}. S is a subring under matrix addition and multiplication with multiplicative identity $[a_{ij}]$ with $a_{11} = 1$, $a_{12} = 0$, $a_{21} = 0$, $a_{22} = 0$. This is of course different than the identity of R.

Subrings with the same multiplicative identity is called **unital subrings**.

4.2.3 THEOREM. *Let F be a field . Any unital subring of F is an integral domain.*

PROOF. EXERCISE.

4.2.4 THEOREM. *Any finite integral domain must be a field.*

PROOF. EXERCISE.

4.2.5 DEFINITION. *Let R be a ring. An integer n is called the characteristic of R if n is the smallest integer such that na = 0, for all $a \in R$.*

EXERCISE. Show that n is the characteristic of R iff $n1 = 0$.

4.2.6 PROPOSITION. *An integral domain has characteristic 0 or p, for some prime number p.*

4.2.7 PROPOSITION. *Let I be a proper ideal of the commutative ring R.*
(a) The factor ring R/I is a field if and only if I is a maximal ideal of R.
(b) The factor ring R/I is a integral domain if and only if I is a prime ideal of R.
(c) If I is maximal, then it is a prime ideal.

PROOF. (a) Let R/I be a field. Let J be an ideal with $I \subset J \subset R$. Then J/I is an ideal of R/I, however R/I is a field, therefore either J/I = I or J/I = R/I. It follows that either J = I or J = R. Thus I is maximal. Conversely, If I is maximal then R/I has no proper ideals therefore by **EXERCISE** () R/I is a field.
(b) Assume that R/I is an integral domain. Let $ab \in I$, we would like to show that either $a \in I$ or $b \in I$. Note that $(I + a)(I + b) = (I + ab) = I$, but R/I is an integral domain i.e., it has no zero-divisors, it follows that either $(I + a) = I$, or $(I + b) = I$, i.e., $a \in I$ or $b \in I$. i.e., I is prime. Conversely, assume that I is prime. To show that R/I does not have zero-divisors. Let $(I + a)(I + b) = (I + ab) = I$, this implies that $ab \in I$, and since I is prime then either $a \in I$ or $b \in I$. Thus either $(I + a) = I$, or $(I + b) = I$, i.e., R/I has no zero-divisors.
(c) I is maximal implies, by (a), that R/I is a field and, by (b), every field is an integral domain, so R/I is an integral domain, therefore , by (b), I is prime.

4.2.8 DEFINITION. *Let R be a commutative ring, and let $a \in R$. The ideal*

$$Ra = \{x \in R \mid x = ra \text{ for some } r \in R\}$$

is called the ***principal ideal*** *generated by a. An integral domain in which every ideal is a principal ideal is called a* ***principal ideal domain*** *denoted by PID.*

EXAMPLE. (Z is a principal ideal domain) Theorem [] shows that the ring of integers Z is a principal ideal domain. Moreover, given any nonzero ideal I of Z, the smallest positive integer in I is a generator for the ideal.

4.2.9 THEOREM. *Every nonzero prime ideal of a principal ideal domain is maximal ideal.*

PROOF. EXERCISE.

EXAMPLE. (Ideals of F[x]) Let F be any field. Then F[x] is a principal ideal domain, since by Theorem [] the ideals of F[x] have the form I = $\langle f(x)\rangle$, where $f(x)$ is the unique monic polynomial of minimal degree in the ideal. The ideal I is prime (and hence maximal) if and only if $f(x)$ is irreducible. If $p(x)$ is irreducible, then the factor ring $F[x]/\langle p(x)\rangle$ is a field.

For any ring R, it is clear that the set {0} is an ideal, which we will refer to as the trivial ideal. Another ideal of R is the ring R itself.

4.2.10 DEFINITION. *Let R be a ring, and let $a \in R$. The left ideal*

$$Ra = \{x \in R \mid x = ra \text{ for some } r \in R\}$$

is called the ***principal left ideal*** *generated by a.*

4.2.11 PROPOSITION. *Let R be a ring, and let I, J be left ideals of R. The following subsets of R are left ideals.*

(a) $I \cap J$;

(b) $I + J = \{x \in R \mid x = a + b \text{ for some } a \in I,\ b \in J\}$;

(c) $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I,\ b_i \in J,\ n \in Z\}$.

PROOF. EXERCISE.

EXAMPLE. (Ideals of $M_{n\times n}(R)$)

Let R be a ring, and let $M_{n\times n}(R)$ be the ring of matrices over R. If I is an ideal of R, then the set $M_{n\times n}(I)$ of all matrices with entries in I is an ideal of S. Conversely, every ideal of S is of this type.

4.2.12 PROPOSITION. *Any ring R is isomorphic to a subring of an endomorphism ring End(A), for some abelian group A.*

PROOF. For $a \in R$, Let $r_a : R \to R$ be defined by $r_a(x) = xa$. r_a is an endomorphism of abelian group (R, +), since $(x + y)r_a = (x + y)a = xa + ya = (x)r_a + (y)r_a$. Let θ: $R \to End(R)$ defined by $\theta(a) = r_a$. θ is a ring isomorphism. To see that we need to show that (1) $\theta(ab) = \theta(a)\theta(b)$. (2) $\theta(a + b) = \theta(a) + \theta(b)$. (3) $\ker(\theta) = \{0\}$.

For (1) we need to show that $r_{ab} = r_a r_b$, but this means that, for $x \in R$ $(x)ab = (xa)b$, and this is the associativity in R. For (2) we use the left distributive law in R. For (3) $a \in \ker(\theta)$ iff $r_a = 0$, i.e., $0 = (1)r_a = 1a = a$. So $\ker(\theta) = 0$. This completes the proof.

4.2.13 THEOREM. (***Fundamental Homomorphism Theorem for Rings***)
Let $\varphi : R \to S$ be a ring homomorphism. Then $\varphi(R)$ is a subring of S, $R/ker(\varphi)$ is a ring, and $R/ker(\varphi) \cong \varphi(R)$.

PROOF. Let $N = \ker(\theta)$. Let θ be the homomorphism $\theta : R/N \to \varphi(R)$, defined by $\theta(Nx) = \varphi(x)$. we have seen before that this is a group isomorphism. So we have $R/N \cong \varphi(R)$ as abelian groups under +. To show that it is a ring homomorphism we need to show that $\theta(NaNb) = \theta(Na)\theta(Nb)$, i.e., but this is true since $\theta(NaNb) = \theta(Nab) = \varphi(ab) = \varphi(a)\varphi(b) = \theta(Na)\theta(Nb)$.

4.2.14 PROPOSITION. *Let I be an ideal of the ring R.*

(a) The natural projection mapping $\pi: R \to R/I$ defined by $\pi(a) = a + I$ for all $a \in R$ is a ring homomorphism, and $\ker(\pi) = I$.

(b) There is a one-to-one correspondence between the ideals of R/I and ideals of R that contain I.

(c) If K is an ideal of R with $I \leq K \leq R$, then $(R/I)/(K/I) \cong R/K$.

PROOF. EXERCISE.

4.2.15 THEOREM. (***Chinese Remainder Theorem***) *Let R be a ring, and let I_1, I_2 be ideals of R such $I_1 + I_2 = R$. Then*

$$(R / I_1) \oplus (R / I_2) \cong R / (I_1 \cap I_2).$$

PROOF. Let $\theta : R \to (R / I_1) \oplus (R / I_2)$ be a function defined as follows

$$\theta(r) = (r + I_1, r + I_2)$$

To see that θ is a homomorphism $\theta(a + b) = (a + b + I_1, a + b + I_2) = (a + I_1 + b + I_1, a + I_2 + b + I_2) = (a + I_1, a + I_2) + (b + I_1, b + I_2) = \theta(a) + \theta(b)$.

$\theta(ab) = (ab + I_1, ab + I_2) = ((a + I_1)(b + I_1), (a + I_2)(b + I_2)) = (a + I_1, a + I_2)(b + I_1, b + I_2) = \theta(a)\theta(b)$.

$\ker \theta = \{ r \in R \mid (r + I_1, r + I_2) = (I_1, I_2)\}$

$= \{ r \in R \mid (r \in I_1 \text{ and } r \in I_2)\}$

$= \{ r \in R \mid (r \in I_1 \cap I_2)\}$.

θ is surjective, since if $(a + I_1, b + I_2) \in (R / I_1) \oplus (R / I_2)$, we need to find $r \in R$ with $r + I_1 = a + I_1$, $r + I_1 = b + I_2$. But since $I_1 + I_2 = R$ then $a - b = r_2 - r_1$ where $r_1 \in I_1$, $r_2 \in I_2$ and then $a = b + r_2 - r_1$. Let $r = a + r_1 = b + r_2$. Then $r \in a + r_1 + I_1 = a + I_1$ and $r = b + r_2 \in b + r_2 + I_2 = b + I_2$. Then by Fundamental theorem $(R / I_1) \oplus (R / I_2) \cong R / (I_1 \cap I_2)$.

4.3 Definition of a module

4.3.1 DEFINITION. *Let R be a ring, and let M be an abelian group. Then M is called a* ***left R-module*** *if there exists a scalar multiplication*

$\psi: R \times M \to M$ denoted by $\psi(r, m) = r\, m$, for all $r \in R$ and all $m \in M$, such that for all $r, r_1, r_2 \in R$ and all $m, m_1, m_2 \in M$,

(i) $r(m_1 + m_2) = rm_1 + rm_2$

(ii) $(r_1 + r_2)\, m = r_1 m + r_2 m$

(iii) $r_1(r_2 m) = (r_1\, r_2)\, m$

(iv) $1\, m = m$.

To denote that M is a left R-module we write ${}_R M$.

EXAMPLE. If R is a ring then R itself is an R-Module, Left R-module and right R-module. So when we want to stress the fact that R is a left R-module we write ${}_R R$.

EXAMPLE. (Vector spaces over F are F-modules) If V is a vector space over a field F, then it is an abelian group under addition of vectors. The familiar rules for scalar multiplication are precisely those needed to show that V is a module over the ring F.

EXAMPLE. (Abelian groups are Z-modules) If A is an abelian group with its operation denoted additively, then for any element $x \in$ Z and any positive integer n, we have defined nx to be the sum of x with itself n times. This is extended to negative integers by taking sums of $-x$. With this familiar multiplication, it is easy to check that A becomes a Z-module.

Another way to show that A is a Z-module is to define a ring homomorphism $\varphi : Z \to End(A)$ by letting $\varphi(n) = n1$, for all $n \in$ Z. This is the familiar mapping that is used to determine the characteristic of the ring End(A). The action of Z on A determined by this mapping is the same one used in the previous paragraph.

If M is a left R-module, then there is an obvious definition of a **submodule** of M: any subset of M that is a left R-module under the operations induced from M. The subset {0} is called the trivial submodule, and is denoted by (0). The module M is a submodule of itself, an improper submodule. It can be shown that if M is a left R-module, then a subset $N \subset M$ is a submodule if and only if it is nonempty, closed under sums, and closed under multiplication by elements of R.

If N is a submodule of ${}_RM$, then we can form the factor group M/N. There is a natural multiplication defined on the cosets of N: for any $r \in R$ and any $x \in M$, let $r(x + N) = rx + N$. If $x + N = y + N$, then $x\text{-}y \in N$, and so $rx\text{-}ry = r(x\text{-}y)N$, and this shows that scalar multiplication is well-defined. It follows that M/N is a left R-module, called **left factor R-module**

Any submodule of ${}_RR$ is a left ideal of R. A submodule of ${}_RR$ is called a ideal of R, and it is clear that a subset of R is an ideal if and only if it is both a left ideal and a right ideal of R.

For any element m of the module M, we can construct the submodule

$$Rm = \{ x \in M \mid x = rm \text{ for some } r \in R \}.$$

This is the smallest submodule of M that contains m, so it is called the cyclic submodule generated by m. More generally, if X is any subset of M, then the intersection of all submodules of M which contain X is the smallest submodule of M which contains X. We will use the notation $\langle X \rangle$ for this submodule, and call it the submodule generated by X. We must have $Rx \subset \langle X \rangle$ for all $x \in X$, and then it is not difficult to show that

$$\langle X \rangle = \sum_{x \in X} a_X x .$$

4.3.2 **DEFINITION**. *The left R-module M is said to be **finitely generated** if there exist $m_1, m_2, \ldots, m_n \in M$ such that*

$$M = \sum_{i=1}^{n} Rm_i.$$

In this case, we say that $\{ m_1, m_2, \ldots, m_n \}$ *is a set of generators for M. The module M is called a* ***free module*** *if there exists a subset* $X \subset M$ *such that each element* $m \in M$ *can be expressed uniquely as a finite sum*

$$m = \sum_{i=1}^{n} a_i x_i, \text{ with } a_1, \ldots, a_n \in R \text{ and } x_1, \ldots, x_n \in X.$$

We note that if N is a submodule of M such that N and M/N are finitely generated, then M is finitely generated. In fact, if $x_1, \ldots, x_n$ generate N and $y_1 + N, y_2 + N, \ldots, y_m + N$ generate M/N, then $x_1, \ldots, x_n, y_1, \ldots, y_m$ generate M.

The module ${}_RR$ is the prototype of a free module, with generating set {1}. If ${}_RM$ is a module, and $X \subset M$, we say that the set X is linearly independent if $\sum_{i=1}^{n} a_i x_i = 0$ implies $a_i = 0$ for $i = 1, \ldots, n$, for any distinct $x_1, \ldots, x_n \in X$ and any $a_1, a_2, \ldots, a_n \in R$. Then a linearly independent generating set for M is called a basis for M, and so M is a free module if and only if it has a basis.

4.3.3 **Definition**. *Let M and N be left R-modules. A function* $f : M \to N$ *is called an R-homomorphism if*

$$f(m_1 + m_2) = f(m_1) + f(m_2) \text{ and } f(rm) = rf(m)$$

for all $r \in R$ and all $m, m_1, m_2 \in M$. The set of all R-homomorphisms from M into N is denoted by

$$\mathrm{Hom}_R(M, N) \text{ or } \mathrm{Hom}({}_RM, {}_RN).$$

For an R-homomorphism $f \in \mathrm{Hom}_R(M, N)$ we define its kernel as

$$\ker(f) = \{ m \in M \mid f(m) = 0 \}.$$

We say that f is an isomorphism if it is both one-to-one and onto. Elements of $\mathrm{Hom}_R(M, M)$ are called endomorphisms, and isomorphisms in $\mathrm{Hom}_R(M, M)$ are called automorphisms. The set of endomorphisms of ${}_RM$ will be denoted by $\mathrm{End}_R(M)$.

4.3.4 PROPOSITION. *Let M be a free left R-module, with basis X. For any left R-module N and any function $\varphi : X \to N$ there exists a unique R-homomorphism*

$$f : M \to N \text{ with } f(x) = \varphi(x), \text{ for all } x \in X.$$

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "\varphi"'] & M \arrow[d, "f"] \\ & N \end{tikzcd}$$

PROOF. Since X is a basis for M, then every element of M can be written as a linear combination of elements of the basis i.e., for $m \in M$ there is $a_1, \ a_k \in R$ such that $m = \sum a_i x_i$, with $x_i \in X$. Define $f : M \to N$ by the rule $f(m) = \sum a_i \varphi(x_i)$, then by definition the right hand side belongs to N. It is easy to see that f is a R-homomorphism that satisfies the given equation $f(x) = \varphi(x)$, for all $x \in X$.

4.3.5 THEOREM. *Let N, N_0, M_0 be submodules of ${}_RM$.*

(a) $N_0 / (N_0 \cap M_0) \cong (N_0 + M_0) / M_0$.

(b) If $N_0 \subset N$, *then* $(M / N_0) / (N / N_0) \cong M / N$.

(c) If $N_0 \subset N$, *then* $N \cap (N_0 + M_0) = N_0 + (N \cap M_0)$.

PROOF. EXERCISE.

4.3.6 DEFINITION. *A non-empty set P is called a* ***poset*** *(Partially ordered set), if there is a relation $\leq$ on the elements of P satisfies the following conditions:*

(i) $\leq$ *is reflexive, i.e., for every* $x \in P$; $x \leq x$.

(ii) $\leq$ *is antisymmetric, i.e., if* $x \leq y$ *and* $y \leq x$ *then* $x = y$.

(iii) $\leq$ *is transitive, i.e., if* $x \leq y$ *and* $y \leq z$ *then* $x \leq z$.

4.3.7 LEMMA. ***(Zorn)*** *Given a poset $P \neq \varnothing$. Assume that for every linearly ordered subset $L \subset P$, there is $b \in P$ such that $b \geq x$ for all $x \in L$. Then there exists $m \in P$ such that m is maximal in P.*

4.3.8 LEMMA. *Let X be any subset of the module $_RM$. Any submodule N with $N \cap X \subset (0)$ is contained in a submodule maximal with respect to this property.*

PROOF. Let $H = \{ N \leq M \mid N \cap X = (0)\}$. $H \neq \phi$, since $(0) \in H$. We would like to show that H has a maximal submodule. By Zorn's Lemma, it is enough to show that every linearly ordered set of H has a maximal submodule. So let $N_1 \subset N_2 \subset N_3 \subset \ldots$, be a series of submodules in H. Let $N = \cup_i N_i$. N is a submodule (prove !) in H, since $N_i \cap X = (0)$ for all i. So every linearly ordered set of H has a maximal submodule. Thus H has a maximal submodule N.

REMARK. Here, I want to remark that the maximal submodule that we have proved to exist in the last lemma is not maximal in the sense that there is no submodule larger than it, except the whole module, but it is maximal having the property that it has no elements common with the set X. i.e., If L is another submodule with this property $N \cap X \subset (0)$ then it must contain $L \subset N$.

A submodule N of the left R-module M is called a **maximal submodule** if $N \neq M$, and for any submodule K with $N \subset K \subset M$, either $N = K$ or $K = M$. Consistent with this terminology, a left ideal A of R is called a **maximal left ideal** if $A \subset R$ and for any left ideal B with $A \subset B \subset R$, either $A = B$ or $B = R$. Thus A is maximal precisely when it is a maximal element in the set of proper left ideals of R, ordered by inclusion. It is an immediate consequence of Lemma ( ) that every left ideal of the ring R is contained in a maximal left ideal, by applying the proposition to the set $X = \{1\}$. Furthermore, any left ideal maximal with respect to not including 1 is in fact a maximal left ideal.

4.3.9 PROPOSITION. *For any nonzero element m of the module $_RM$ and any submodule N of M with m not in N, there exists a submodule N* maximal* *with respect to N^* containing N with m not in N^*. Moreover, M/N^* has a minimal submodule contained in every nonzero submodule.*

PROOF. EXERCISE.

4.3.10 COROLLARY. *Any proper submodule of a finitely generated module is contained in a maximal submodule.*

4.3.11 DEFINITION. *Let R be a ring, and let M be a left R-module. For any element $m \in M$, the left ideal*

$$Ann(m) = \{ r \in R \mid rm = 0 \}$$

is called the ***annihilator*** *of m. The ideal*

$$Ann(M) = \{ r \in R \mid rm = 0 \text{ for all } m \in M \}.$$

is called the **annihilator** of M.

The module M is called **faithful** if $Ann(M) = (0)$.

4.3.12 DEFINITION. *A nonzero module $_RM$ is called* ***simple*** *(or* ***irreducible****) if its only submodules are (0) and M.*

We first note that a submodule $N \subset M$ is maximal if and only if M/N is a simple module. A submodule $N \subset M$ is called a **minimal submodule** if $N \neq (0)$ and for any submodule K with $(0) \subset K \subset N$, either $N = K$ or $K=(0)$. With this terminology, a submodule N is minimal if and only if it is simple when considered as a module in its own right.

4.3.13 LEMMA. (***Schur***) *If $_RM$ is simple, then $End_R(M)$ is a division ring.*

PROOF. $End_R(M)$ has ring structure under addition and composition of maps, defined as follows: Let $\varphi, \theta \in End_R(M)$, let $x \in M$, then

$$(\varphi + \theta)(x) = \varphi(x) + \theta(x),$$

$$(\varphi \,.\, \theta)(x) = \varphi(\theta(x)).$$

It is easy to see that $End_R(M)$ has ring structure with the 0, 1 as the zero endomorphism and identity endomorphism.

The only thing we need to prove is that every non-zero endomorphism φ has an inverse φ^{-1}. But this holds since $ker\varphi$ is an R-submodule of M, therefore by simplicity of M $ker\varphi = 0$. Thus φ is one to one. Since $\varphi(M)$ is also an R-submodule of M, therefore by simplicity of $\varphi(M) = M$ provided that φ is not the zero endomorphism.

4.3.14 PROPOSITION. *The following conditions hold for a left R-module M.*
(a) The module M is simple if and only if $Rm = M$, for each nonzero $m \in M$.
(b) If M is simple, then $Ann(m)$ is a maximal left ideal, for each nonzero $m \in M$.
(c) If M is simple, then it has the structure of a left vector space over a division ring.

PROOF. (*a*) Let M be a simple R-module. The set Rm is a submodule of M. It follows by simplicity of M that Rm = M.
Conversely, if Rm = M for all $0 \neq m \in M$ then M has no proper submodules. I.e., M is simple.

(b) Let M be a simple R-module. Let $m \in M$. Let $\theta : R \to M$ be defined by
$\theta(r) = rm$. θ is a R-homomorphism,
since $\theta(s + r) = (s + r)m = sm + rm = \theta(s) + \theta(r)$ and
$\theta(sr) = (sr)m = s(rm) = s\theta(r)$. Then by homomorphism theorem we have ${}_RR/ker(\theta) \cong M$ (Note that θ is onto by simplicity of M).
Now $ker(\theta) = \{ r \in R \mid rm = 0\} = ann(m)$. Thus $R/ker(\theta) \cong M$. Simplicity of M now implies that $ann(m)$ is maximal.

(c) **EXERCISE.**

4.4 The Jacobson Radical

4.4.1 DEFINITION. *Let M be a left R-module. The intersection of all maximal submodules of M is called the* ***Jacobson radical of M****, and is denoted by* ***J(M)****.*

This would make $J(R) = \cap\{I \mid I \text{ is maximal left ideal of } R\}$.

4.4.2 PROPOSITION. *$J(R) = \cap\{ann(M) \mid M$ is simple left R-module$\}$.*

PROOF. By Proposition () ann(M) is maximal left ideal of R. It follows that J(R) $\subset \cap\{ann(M) \mid$ M is simple left R-module$\}$. For the reverse inclusion, let I be a maximal left ideal of R. Let $u \in \cap\{ann(M) \mid$ M is simple left R-module$\}$. We will show that $u \in$ I. Since I is maximal left ideal then R/I is a simple left R- module. It follows that u(R/I) = I (0 in R/I). So, $u(a + I) = I$ for all $a \in R$. Take $a = 1$, then $u + I = I$. Thus $u \in$ I. Hence $\cap\{ann(M) \mid$ M is simple left R-module$\} \subset \cap\{I \mid$ I is maximal left ideal of R$\}$. Hence they are equal.

4.4.3 LEMMA. (**Nakayama**) *If ${}_RM$ is finitely generated and $J(R)M = M$, then $M = (0)$.*

PROOF. EXERCISE.

4.4.4 LEMMA. *Let U be a proper left ideal of the ring R, then there exits a maximal left ideal V of R such that $U \subset V$.*

PROOF. Let $P = \{ I \subset R \mid$ I is left ideal of R , $U \subset I \neq R\}$. $P \neq \emptyset$ since $U \in P$. P is a poset ordered by inclusion. Let L be a set of linearly ordered ideals of P. we need to find $I \in P$ such that $J \subset I$ for all $J \in L$. Let $I = \cup \{ J \mid J \in L\}$. Show that I is an ideal containing U. Then by Zorn's Lemma there is an ideal V that satisfies the lemma.

4.4.5 PROPOSITION. *For any ring R, J(R) is two sided ideal.*

PROOF. Let $r \in R$, let $x \in J(R)$ and Let M be a simple left R-module. Since xM = 0 then rxM = 0. Since rM = M by simplicity of M then $x(rM) = (xr)M = xM = 0$, it follows that $xr \in J(R)$. Thus J(R) is a right ideal of R. Whence it is two sided ideal.

4.4.6 DEFINITION. *If R is a ring, $x \in R$ is called right-quasi-regular if 1 - x has a right inverse (denoted rqr). Similarly x is left-quasi-regular if 1 - x has a left inverse (denoted lqr) and x is called quasi-regular if 1 - x is both rqr and lqr (denoted qr).*

Note x is *qr* iff x is a unit in R.

4.4.7 PROPOSITION. *Let $x \in J(R)$ then x is lqr.*

PROOF. R(1 - x) is a left ideal of R. If R(1 - x) = R, then $1 \in$ R(1 - x), so there is $r \in$R such that 1 = r(1 - x), so r is the right inverse of (1 - x). Thus x is *lqr*.
Now assume that R(1 - x) < R. By Zorn's Lemma there is a maximal ideal I with R(1 - x) $\subset$ I. Thus 1 - $x \in$ I, but $x \in$ I then $1 \in$ I implying that I = R contradicting the maximality of I.

4.4.8 COROLLARY. *Let $x \in K(R) = \cap\{I \mid I$ is maximal right ideals of $R\}$ then x is rqr.*

PROOF. EXERCISE.

4.4.9 THEOREM. *Let I be any left ideal of R with the property that every element of I is lqr then $I \subset J(R)$.*

PROOF. Let M be a maximal left ideal of R. We will show that I $\subset$ M. If not , i.e., if I is not contained in M then there is an ideal I + M which is a left ideal of R containing M properly, therefore I + M = R. Thus there is $u \in$ I, $m \in$ M such that $u + m = 1$. Then $m = 1 - u$. Since u is *lqr* then there is a left inverse of 1- $u = m$. It follows that $1 \in$ R$m \subset$ M, contradicting the maximality of M. Hence I $\subset$ M.

4.4.10 THEOREM. *For a ring R, $J(R) = \cap\{I \mid I$ is maximal right ideals of $R\}$.*

PROOF. Let K(R) = $\cap$\{I | I is maximal right ideals of R\}. Let $u \in$ J(R), to show that $u \in$ I for every maximal right ideal I of R. It is enough to show that every element $u \in$ J(R) is *rqr*. Since u is *lqr* then there is $r \in$R such that $r(1 - u) = 1$. Let $z = 1 - r$. Then $(1 - z)(1 - u) = 1$. It follows that $1 - z - u + zu = 1$. Thus $z = zu - u$. This implies that $z \in$ J(R) i.e., z is *lqr*. Hence $1 - z$ has a left inverse. I.e., y has a right inverse and it must be $1 - u$. So, $y(1 - u) = (1 - u)y = 1$. Thus u is a *rqr*. So $u \in$ K(R). The reverse inclusion is similar.

4.4.11 COROLLARY. (**Jacobson-Perlis Condition**). *$x \in J(R)$ iff $1 - rx$ has left inverse for all $r \in R$.*

PROOF. $x \in$ J(R) then $rx \in$ J(R) since J(R) is left ideal of R. Therefore rx is *lqr*, i.e., $1 - rx$ has left inverse. Conversely, suppose that $1 - rx$ has left inverse for all $r \in$ R. Therefore all the elements of the ideal Rx are *lqr* then by Theorem ( ) R$x \subset$ J(R), so $x \in$ J(R).

4.4.12 DEFINITION. *An element x is called nilpotent if $x^n = 0$, for some $n \geq 0$. An additive subgroup U is called nil if each element of U is nilpotent.*

EXERCISE. Let I be a nil left ideal of R. Show that I $\subset$ J(R).

4.4.13 THEOREM. *The Jacobson radical J(R) of the ring R is equal to each of the following sets:*

(1) The intersection of all maximal left ideals of R;

(2) The intersection of all maximal right ideals of R;

(3) $\{x \in R \mid rx$ is lqr for all $r \in R\}$;

(4) $\{x \in R \mid xr$ is rqr for all $r \in R\}$;

(5) The largest ideal J of R such that $1 - x$ is invertible in R for all $x \in J$.

(6) The largest ideal J of R such that J containing nil left ideals of R.

4.4.14 DEFINITION. *The ring R is said to be semiprimitive if J(R) = (0).*

Chapter V

5.1 Chain Conditiions

5.1.1 DEFINITION. *Let P be a poset with order relation ≤. We say that P satisfies the* ***ascending chain condition*** *(ACC) if for every chain* $x_1 \le x_2 \le x_3 \le \ldots \le x_n \le \ldots$ *.there is an integer n such that* $x_n = x_{n+1} = x_{n+2} = x_{n+3} = \ldots$.

And We say that P satisfies the ***descending chain condition*** *(DCC) if for every chain* $x_1 \ge x_2 \ge x_3 \ge \ldots \ge x_n \ge \ldots$ *.there is an integer n such that* $x_n = x_{n+1} = x_{n+2} = x_{n+3} = \ldots$.

P is said to satisfy the ***maximal condition*** *(MaxC) if for every non-empty set* $S \subset P$ *there is a maximal element* $x \in S$*, such that if* $y \in S$ *then* $y \le x$.

P is said to satisfy the ***minimal condition*** *(MinC) if for every non-empty set* $S \subset P$ *there is a minimal element* $x \in S$*, such that if* $y \in S$ *then* $y \ge x$.

5.1.2 DEFINITION. *An s-group G is said to be* ***Noetherian*** *if the poset of all s-subgroups of G satisfies the (ACC). Similarly, G is said to be* ***Artinian*** *if the poset of all s-subgroups of G satisfies the (DCC).*

5.1.3 DEFINITION. *A module* $_RM$ *is said to be* ***Noetherian*** *if the poset of all sumodules of* $_RM$ *satisfies the (ACC). Similarly, M is said to be* ***Artinian*** *if the poset of all sumodules of* $_RM$ *satisfies the (DCC).*

EXAMPLE. Z is Notherian but not Artinian, since

$$\langle 2\rangle \supset \langle 4\rangle \supset \langle 8\rangle \supset \ldots .$$

5.1.4 DEFINITION. *A ring R is said to be* ***left Noetherian*** *if the module* $_RR$ *is Noetherian. A ring R is said to be* ***left Artinian*** *if the module* $_RR$ *is Artinian. If R satisfies the conditions for both right and left ideals, then it is simply said to be* ***Noetherian*** *or* ***Artinian****.*

5.1.5 THEOREM. *Let P be a poset. P satisfies (ACC) iff P satisfies the (MaxC). And P satisfies (DCC) iff P satisfies the (MinC).*

PROOF. Assume that P satisfies the (MaxC), to show that P satisfies the (ACC), let $x_1 \le x_2 \le \ldots$ be an ascending chain in P. Let S = $\{ x_i \mid i \ge 1\}$. S is non-empty. Therefore by the (MaxC) there is $x \in$ S with x maximal. I.e., $x = x_n$ for some n. Then $x_n = x_{n+1} = x_{n+2} = x_{n+3} = \ldots.$

Conversely, assume that P satisfies the (ACC). Let $S \subset P$, $S \neq \varnothing$. Assume that there is no maximal element in S. Then for $x \in S$ the set $S_x = \{ y \in S \mid y > x \} \neq \varnothing$. So by the axiom of choice there is a function $\varphi : S \to S$ such that $\varphi(x) \in S_x$. i.e., $x < \varphi(x) < \varphi(\varphi(x) < \varphi^3(x) < \ldots < \varphi^n(x) < \ldots$ which is a chain that is not eventually contant. Contradicting that P satisfies the (ACC).

Similarly for the (DCC).

5.1.6 COROLLARY. *The following conditions are equivalent for a module $_RM$:*

(1) M is Noetherian;

(2) every nonempty set of submodules of M has a maximal member.

EXERCISE. Let A, B, K be left submodules of a left R-module M. If $A \subset B$ and $A + K = B + K$ and $A \cap K = B \cap K$ then $A = B$.

5.1.7 PROPOSITION. *The following conditions hold for a module $_RM$ and any submodule N.*

(a) M is Noetherian if and only if N and M/N are Noetherian.

(b) M is Artinian if and only if N and M/N are Artinian.

PROOF. (a) Assume that M is Noetherian. Let $N_1 \le N_2 \le \ldots$, be an ascending chain of submodules of N, $K_1/N \le K_2/N \le \ldots$ be an ascending chain of submodules of M/N. Then both $N_1 \le N_2 \le \ldots$ and $K_1 \le K_2 \le \ldots$ are ascending chains of submodules of M. Therefore by the (ACC) of M both are eventually constant. I.e., N, M/N satisfy the (ACC). Conversely, assume that both N, M/N satisfy the (ACC).

Let $M_1 \leq M_2 \leq \dots$, be an ascending chain in M. Consider the ascending chains

$$N \cap M_1 \leq N \cap M_2 \leq \dots \ ,$$

$$(N + M_1)/N \leq (N + M_2)/N \leq \dots$$

in N, M/N respectively. Since both N, M/N satisfy the (ACC) then there is a finite integer m such that

$$N \cap M_m = N \cap M_{m+1} = \dots \ ,$$

$$(N + M_m)/N = (N + M_{m+1})/N = \dots$$

Thus $N + M_m = N + M_{m+1}$ and $N \cap M_m = N \cap M_{m+1}$. Hence by the **EXERCISE** $M_m = M_{m+1} = \dots$. whence M satisfies the (ACC).

(b) The proof is similar.

EXERCISE. For an R-Module M, show that M is finitely generated iff M is Noetherian

5.1.8 COROLLARY. *A finite direct sum of modules is Noetherian if and only if each summand is Noetherian; it is Artinian if and only if each summand is Artinian.*

5.1.9 PROPOSITION. *A ring R is left Noetherian if and only if every finitely generated left R-module is Noetherian; it is left Artinian if and only if every finitely generated left R-module is Artinian.*

5.1.10 THEOREM. (**Hilbert basis theorem**) *If R is a left Noetherian ring, then so is the polynomial ring R[x].*

PROOF. Suppose that R is Noetherian. Let $I \subset R[x]$ be a left ideal. It is enough to show that I has a finite generating set. For $n \geq 0$, define $A_n = \{ a \in R \mid a$ is a leading coefficient of some polynomial $f \in I$ with degree of $f = n\} \cup \{0\}$. We claim that A_n is an ideal of R. To see this, let $a, b \in A_n$, we want to show that $a - b \in A_n$, we may assume that $a \neq b$ and $a, b \neq 0$. So there are two polynomials $f, g \in I$ with leading coefficient of $f = a$, and leading coefficient of $g = b$. Thus $a - b$ is the leading coefficient of $f - g$ and so is all R multiples of $a - b$. Hence A_n is a left ideal for all n.

Note that $A_1 \subset A_2 \subset \ldots \subset A_n \subset \ldots$ is a chain of left ideals. Since if $a \in A_n$ then there is a polynomial f for which a is the leading coefficient, then $xf \in A_{n+1}$ is a polnomial in I with leading coefficient a, so $a \in A_{n+1}$.

Since R is Noetherian then there is N such that $A_N = A_{N+1} = \ldots$. Choose a finite generating set S_i for A_i with $1 \leq i \leq N$. Let $S_i = \{ a_{i1}, a_{i2}, a_{i3}, \ldots, a_{ik}\}$. Let f_{ij} be polynomials in I with leading coefficients a_{ij} and degree i. We claim now that I is generated by all these polynomials f_{ij}. To prove that, let J be the ideal generated by all f_{ij}. Since $f_{ij} \in$ I then J $\subset$ I. Assume that there is $f \in$ I, $f \notin$ J. Assume also that the degree of f is minimal. Let m = degree of f. We have two cases:

Case 1. If $m \leq N$, let a = leading coefficient of f thus $a \in A_m$ and threfore a is an R-linear combination of a_{mj}. Let g be the R-linear of f_{mj} with same coefficients. Then $g \in$ J thus a is a leading coefficient of $g \in$ J, degree of $g = m$. Now $f - g \notin$ J, degree $(f - g) < m$ thus $f - g \in$ I. A contradiction because f was such example.

Case 2. $M > N$. a is a leading coefficient of g, $a \in A_m = A_N$. Therefore a is an R-linear combination of a_{Nj}. Get g as an R-linear combination of f_{Nj}. Thus $g \in$ J, degree of $g = N$ and the leading coefficient og g is a. Now $x^{m-N}g \notin$ J and $f - x^{m-N}g \in$ I. But degree of $f - x^{m-N}g < m$. a contradiction.�

We can now give some fairly wide classes of examples of Noetherian and Artinian rings. If D is a principal ideal domain, then D is Noetherian since each ideal is generated by a single element. It follows that the polynomial ring $D[x_1, x_2, \ldots, x_n]$ is also Noetherian. If F is a field, then $F[x]/I$ is Artinian, for any nonzero ideal I of $F[x]$, since $F[x]$ is a principal ideal domain. This allows the construction of many interesting examples. Note that $D[x]/I$ need not be Artinian when D is assumed to be a principal ideal domain rather than a field, since $Z[x]/\langle x\rangle$ is isomorphic to Z, which is not Artinian.

5.2 Semiprimitive Rings

5.2.1 DEFINITION. *Let A, B be additive subgroups of a ring R. AB = the additive subgroup generated by all products a b i.e.,*

$$AB = \langle \{a\, b \mid a \in A,\ b \in B\}\rangle$$

Note it can be shown easily that

$$AB = \{ a_1b_1 + a_2b_2 + \ldots + a_nb_n \mid a_i \in A,\ b_i \in B\}$$

EXERCISE. Show that if A is left ideal then AB is left ideal, and if B is right ideal then AB is right ideal.

5.2.2 DEFINITION. *Let $A \subset R$ be an additive subgroup. A is called* ***nilpotent*** *if $A^n = 0$, for some $n > 0$.*

5.2.3 THEOREM. *If R is right Artinian then J(R) is nilpotent.*

PROOF. Let J = J(R). Consider the descending chain

$$J \supseteq J^2 \supseteq J^3 \supseteq \ldots\ .$$

Since R is Artinian then $\exists$ integer n such that $J^n = J^{n+1} = \ldots$.

To show that $J^n = 0$, let $I = J^n$. Assume $I \neq 0$. Note $I^2 = J^{2n} = J^n = I$.

Let $S = \{ N \subset I \mid N \text{ is right ideal of R and } NI \neq 0\}$. Since $I \in S$ then $S \neq \varnothing$.

Since R is Artinian then S has a minimal ideal, say N. Note that $N \subset I$, $NI \neq 0$.

So there is $x \in N$ such that $xI \neq 0$.

Now $(xI)I = xI \neq 0$ therefore $xI \supseteq N$ by minimality of N. But $x \in N$ thus $xI = N$.

therefore, $\exists\, y \in I$ such that $x\, y = x$. It follows that $x(1 - y) = 0$.

Since $y \in I \subset J$, then $\exists\, z \in R$ such that $(1 - y)z = 1$.

It follows that $0 = 0.z = x(1 - y)\, z = x\, 1 = x$, a contradiction.

5.2.4 COROLLARY. *If R is right Artinian then any nil right ideal is nilpotent.*

PROOF. If I is nil right ideal then $I \subset J(R)$, but J(R) is nilpotent, then $I^n \subset J^n = 0$, for some $n > 0$.

Also any nil left ideal of R is nilpotent.

5.2.5 COROLLARY. *Let R be left Artinian then TFAE.*

(i) $J(R) = 0$.(R is semiprimitive)

(ii) If I is left ideal and $I^2 = 0$ then $I = 0$.(I is semiprime)

(iii) If I is an ideal and $I^2 = 0$ then $I = 0$.

PROOF. (i) $\rightarrow$ (ii) $I^2 = 0$ implies that I is nil, therefore $I \subset J(R) = 0$, thus $I = 0$.

(ii) $\rightarrow$ (iii) straightforward.

(iii) $\rightarrow$ (i) we know that $J(R)^n = 0$ for some $n \geq 1$. Take smallest such n, then $J^{n-1} \neq 0$.

Let $I = J(R)^{n-1}$. It follows that $I^2 = J(R)^{2n-2}.= 0$, then $I = 0$ by (iii), a contradiction.

5.2.6 DEFINITION. *A ring R is called a **Wedderburn ring** if it is Artinian and semiprimitive.*

5.2.7 PROPOSITION. *Let I be a minimal left ideal of R. Assume that $I^2 \neq 0$ then $I = Re$ for some $e \in R$, $e^2 = e$ (e is called idempotent).*

PROOF. $\exists\ a \in I$, $Ia \neq 0$. $Ia \subset I$ since $a \in I$ and I is left ideal. Ia is a left ideal then by minimality of I $Ia = I$. Thus $\exists\ e \in I$, such that $ea = a$. Therefore $e^2a = ea = a$. it follows that $a(e^2 - e) = 0$.

Let $S = \{ x \in I \mid xa = 0\}$. S is a left ideal, $S \subset I$. Thus $S = 0$ or $S = I$. but $I \neq 0$, so $S = 0$. $e^2 - e \in S$. then $e^2 - e = 0$. Hence $e^2 = e$. Since $e \in I$ then $Re \subset I$, then $Re = I$ by minimality of I.

5.2.8 PROPOSITION. (***Pierce Decomposition***). *Let I be a left ideal of R, let $e \in I$ with $e^2 = e$ then $I = Ie \oplus I(1 - e)$.*

PROOF. $x \in I$ then $x(1 - e) \in I$ and $Ie \subset I$. Hence $I \supseteq Ie \oplus I(1 - e)$. we need to show that $Ie \cap I(1 - e) = 0$. If $x \in Ie \cap I(1 - e)$, then $x = ye$ for some $y \in I$, and $x = (1 - e)z$, $z \in I$.

$x = ey = e(ez) = e(1 - e)z = (e - e)z = 0z = 0$.

5.2.9 THEOREM. *Every Wedderburn ring is the direct sum of finitely many minimal left ideals.*

PROOF. we will prove a more general assertion. We will show that every left ideal is the sum of finitely many minimal left ideals. Suppose false. Let S = { I $\subset$ R| I is not the direct sum of finitely many minimal left ideals}. S $\neq \varnothing$. Since R is Artinian ring then S has a minimal element I. I $\neq$ 0. Let M be minimal left ideal with M $\subset$ I, such ideal exists, again because R is Artinian and the set of all ideals contained in I has a minimal one. M $\neq$ 0, $M^2 \neq 0$, since R is semiprimitive. Thus M = Re, for some idempotent element $e \in$ M, with $e \neq 0$. Now using Pierce decomposition then I = I$e \oplus$ I(1 - e) = M $\oplus$ I(1 - e). Let K = I(1 - e), then I = M $\oplus$ K. Since M $\neq$ 0, K < I. then K $\notin$ S. therefore K is the direct sum of finitely many minimal left ideals of R. It follows that I is the direct sum of minimal left ideals of R, contradicting our assumption. Therefore S = $\varnothing$. Hence R is the direct sum of minimal left ideals.

Note this theorem could have been stated as follows: if R is Artinian ring then $_R$R is the dircet sum of simple left R-modules.

5.2.10 COROLLARY. *If $_RR$ is the finite direct sum of minimal left ideals $\{M_i\}^m_{i=1}$ then every minimal left ideal of R is isomorphic to one of the M_i's.*

5.2.11 COROLLARY. *If $_RR$ is the direct sum of simple left R-modules $\{M_i\}^m_{i=1}$ then every simple left simple R-module of R is isomorphic to one of the M_i's.*

PROOF. Let S be any simple left R-module, let $s \in$ S, $s \neq 0$.write $1 = e_1 + e_2 + \ldots + e_n$, for idempotent elements $e_i \in M_i$, $i = 1, 2, \ldots, n$.

$0 \neq s = 1.s = (e_1 + e_2 + \ldots + e_n)s = e_1s + e_2s + \ldots + e_ns$. thus $e_is \neq 0$ for some i.

Fix such i. we will show that S $\cong M_i$.

Let $\theta : M_i \to$ S be defined by $\theta(x) = sx$, for all $x \in M_i$. It is easy to show that θ is an R- homomorphism. $\theta(e_i) = e_is \neq 0$.then by simplicity of S, $\theta(M_i)$= S. again by simplicity of M_i , kernel of θ is 0. Thus they are isomorphic.

EXERCISES

1. An element γ of a ring R, is called **central** if $\gamma r = r\gamma$ for all elements $r \in$ R. Prove that the set of all central elements Z(R) forms a ring.

2. Let φ be an R-homomorphism of a left R-module M into a left R-module N; i.e., $\varphi : M \to N$. Let U be a subset of M and L be the left submodule of M generated by U. Prove that the left submodule of N generated by $\varphi(U)$ is $\varphi(L)$.

3. Let $\{A_i\}_{i\in I}$ be a family of subsets of a left R-module M, and let N_i be the left submodule generated by A_i . Show that $\Sigma_i N_i$ is generated by $\cup_i A_i$.

4. Let N be a left submodule of a left R-module M. Let $\{A_i\}_{i\in I}$ be a family of submodules of M with $N \subset A_i \subset M$ for all $i \in I$. Show that $(\Sigma_i A_i)/N = \Sigma_i (A_i/N)$ and $(\cap_i A_i)/N = \cap_i (A_i/N)$.

5. Let m be a positive integer and p be prime. Prove that $m\mathrm{Z}/mp\mathrm{Z}$ is a simple Z-module.

6. Let Ω denote the set of all rational numbers that can be expressed in the form $m/2^k$, where m, k are integers. Show that Ω is a Z-module having Z itself as a submodule. Also show that

(i) each proper submodule of Ω/Z contains only a finite number of elements.

(ii) Ω/Z satisfies the (MinC) but not the (MaxC)

(iii) Ω/Z as a Z-module is not finitely generated.

7. Show that an integral domain that satisfies the (DCC) is a field.

8. Two ideals A, B are called **comaximal** if A + B = R. If A, B are comaximal show that $AB = A\cap B$.

9. If the rings $R_1, R_2, \ldots, R_n$ are left noetherian show that the direct sum $R = R_1 \oplus R_2 \oplus \ldots\oplus R_n$ is left noetherian.

10. Let M be a left R-module. Let M[X] denotes the formal set of " polynomials" elements of the form $m_0 + m_1X + m_2X^2 + \ldots + m_kX^k$, for some integer k. Show that M[X] is an R[X]-module and if M satisfies the (ACC) then so is M[X].

5.3 Composition series

5.3.1 DEFINITION. *A composition series of length n for a nonzero module M is a chain of n + 1 submodules*

$$M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n = (0)$$

such that M_{i-1}/M_i is a simple module for i = 1, 2, ..., n. These simple modules are called the ***composition factors*** *of the series.*

5.3.2 THEOREM. (**Jordan-Holder**) *If a module M has a composition series, then any other composition series for M is equivalent to it.*

PROOF. EXERCISE.

As an immediate consequence of the Jordan-Holder theorem, if a module ${}_RM$ has a composition series, then all composition series for M must have the same length, which we denote by **λ(M)**. This is called **the length of the module**, and we simply say that the module has finite length. Since any ascending chain of submodules can be refined to a composition series, λ(M) gives a uniform bound on the number of terms in any properly ascending chain of submodules. We also note that if M_1 and M_2 have finite length, then

$$\lambda(M_1 \oplus M_2) = \lambda(M_1) + \lambda(M_2).$$

5.3.3 PROPOSITION. *A module has finite length if and only if it is both Artinian and Noetherian.*

A module ${}_RM$ is said to be **indecomposable** if its only direct summands are (0) and M. As our first example, we note that Z is indecomposable as a module over itself, since the intersection of any two nonzero ideals is again nonzero. To give additional examples of indecomposable Z-modules, recall any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order. Using this result, we see that a finite Z-module is indecomposable if and only if it is isomorphic to Z_n, where $n = p^k$ for some prime p.

5.3.4 PROPOSITION. If $_RM$ has finite length, then there exist finitely many indecomposable submodules $M_1, M_2, \ldots, M_n$ such that

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_n.$$

5.3.5 LEMMA. **[Fitting]** Let M be a module with length n, and let f be an endomorphism of M. Then

$$M = \mathrm{Im}(f^n) \oplus \ker(f^n) .$$

5.3.6 PROPOSITION. *Let M be an indecomposable module of finite length. Then for any endomorphism f of M the following conditions are equivalent.*

(1) f is one-to-one;

(2) f is onto;

(3) f is an automorphism;

(4) f is not nilpotent.

5.3.7 PROPOSITION. *Let M be an indecomposable module of finite length, and let* f_1, f_2 *be endomorphisms of M. If* $f_1 + f_2$ *is an automorphism, then either* f_1 *or* f_2 *is an automorphism.*

5.3.8 LEMMA. *Let* X_1, X_2, Y_1, Y_2 *be left R-modules, and let*

$$f: X_1 \oplus X_2 \to Y_1 \oplus Y_2$$

be an isomorphism. Let

$$i_1 : X_1 \to X_1 \oplus X_2$$

and

$$i_2 : X_2 \to X_1 \oplus X_2$$

be the natural inclusion maps, and let

$$p_1 : Y_1 \oplus Y_2 \to Y_1$$

and

$$p_2 : Y_1 \oplus Y_2 \to Y_2$$

be the natural projections. If

$$p_1 \circ f \circ i_1 : X_1 \to Y_1$$

is an isomorphism, then

$$p_2 \circ f \circ i_2 : X_2 \to Y_2$$

is an isomorphism.

5.3.9 **THEOREM.** (**Krull-Schmidt**) *Let* $\{X_j,\ j = 1, 2, \ldots, m\}$ *and* $\{ Y_i,\ i = 1, 2, \ldots, n \}$ *be indecomposable left R-modules of finite length. If*

$$X_1 \oplus \ldots \oplus X_m \cong Y_1 \oplus \ldots \oplus Y_n,$$

then $m = n$ *and there exists a permutation* $\pi \in S_n$ *with* $\pi(j) = i$ *and* $X_j \cong Y_i$, *for* $1 \leq j \leq m$.

5.4 Semisimple Modules

5.4.1 DEFINITION. *Let M be a left R-module. The sum of all minimal submodules of M is called the **socle** of M, and is denoted by **Soc(M)**. The module M is called **semisimple** if it can be expressed as a sum of minimal submodules.*

A semisimple module $_RM$ behaves like a vector space in that any submodule splits off, or equivalently, that any submodule N has a complement N' such that N + N' = M and $N \cap N' = 0$.

5.4.2 THEOREM. *Any submodule of a semisimple module has a complement that is a direct sum of minimal submodules.*

5.4.3 COROLLARY. *The following conditions are equivalent for a module $_RM$.*

(1) M is semisimple;
(2) Soc(M) = M.
(3) M is completely reducible;
(4) M is isomorphic to a direct sum of simple modules.

5.4.4 COROLLARY. *Every vector space over a division ring has a basis.*

5.4.5 DEFINITION. *The module $_RQ$ is said to be injective if for each one-to-one R-homomorphism $i: {_RM} \to {_RN}$ and each R-homomorphism $f: M \to Q$ there exists an R-homomorphism $f^*: N \to Q$ such that $f^*i = f$.*

5.4.6 THEOREM. *The following conditions are equivalent for the ring R.*

(1) R is a direct sum of finitely many minimal left ideals;

(2) R R is a semisimple module;

(3) every left R-module is semisimple;

(4) every left R-module is projective;

(5) every left R-module is injective;

(6) every left R-module is completely reducible.

5.4.7 COROLLARY. *Let D be a division ring, and let R be the ring $M_n(D)$ of all $n \times n$ matrices over D. Then every left R-module is completely reducible.*

Let R be a ring, and let G be a group. The group ring RG is defined to be a free left R-module with the elements of G as a basis. The multiplication on RG is defined by

$$\left(\sum_{w \in G} a_w w \right)\left(\sum_{x \in G} b_x\, x \right) = \sum_{z \in G} c_z z \text{ where } c_z = \sum_{z=wx} a_w b_x .$$

The crucial property of a group ring is that it converts group homomorphisms from G into the group of units of a ring into ring homomorphisms. To be more precise, let S be a ring, let $\varphi : G \to S^x$ be a group homomorphism, and let $\theta : R \to Z(S)$ be any ring homomorphism. (Recall that S^x denotes the group of invertible elements of S and Z(S) denotes the center of S.) Then there is a unique ring homomorphism $\psi : RG \to S$ such that

$$\psi(g) = \varphi(g) \text{ for all } g \in G \text{ and } \psi(r) = \theta(r) \text{ for all } r \in R.$$

5.4.8 THEOREM. (**Maschke**) *Let G be a finite group and let K be a field such that $|G|$ is not divisible by chr(K). Then every KG-module is completely reducible.*

5.4.9 Theorem. (**Baer's criterion**) *For any left R-module Q, the following conditions are equivalent.*

(1) The module Q is injective;

(2) for each left ideal A of R and each R-homomorphism $f : A \to Q$ *there exists an extension* $f^*: R \to Q$ *such that* $f^*(a) = f(a)$ *for all* $a \in A$;

(3) for each left ideal A of R and each R-homomorphism $f : A \to Q$ *there exists* $q \in Q$ *such that* $f(a) = aq$, *for all* $a \in A$.

5.4.10 Proposition. *Let D be a principal ideal domain, with quotient field Q.*

(a) The module ${}_DQ$ *is injective.*

(b) Let I be any nonzero ideal of D, and let R be the ring D/I. Then R is an injective module, when regarded as an R-module.

Index