SEMESTER : I
CORE COURSE : I

Inst Hour	: 6
Credit	: 5
Code	: 18KP1M01

ALGEBRA

UNIT – I

Group Theory: A counting principle – Normal Subgroups and Quotient groups – Homomorphisms – Automorphisms.
Chapter 2: Sec 2.5, 2.6, 2.7, 2.8

UNIT – II

Group Theory: Cayley's theorem – Permutation groups – Another counting principle – Sylow's theorem.
Chapter 2: 2.9, 2.10, 2.11, 2.12

UNIT – III

Ring Theory: Homomorphisms - Ideals and quotient rings – More ideals and quotient rings – Euclidean Rings – A particular Euclidean Ring.
Chapter 3: Sec 3.3, 3.4, 3.5, 3.7, 3.8

UNIT – IV

Polynomial rings – Polynomials over the rational field – Polynomials over commutative rings – Inner Product spaces.
Chapter 3: Sec 3.9, 3.10, 3.11,
Chapter 4: Sec 4.4

UNIT – V

Fields: Extension fields – Roots of Polynomials – More about roots.
Chapter 5 : Sec 5.1, 5.3, 5.5

TEXT BOOK

1. I.N.Herstein, Topics in Algebra, Second Edition, Wiley Eastern Limited.

REFERENCES

1. David S.Dummit and Richard M. Foote, Abstract Algebra, Third Edition, Wiley Student Edition, 2015.
2. John, B. Fraleigh, A First Course in Abstract Algebra, Addison – Wesley Publishing company.
3. Vijay, K. Khanna, and S.K. Bhambri, A Course in Abstract Algebra, Vikas Publishing House Pvt Limited, 1993.
4. Joseph A.Gallian, Contemporary Abstract Algebra, Fourth Edition, Narosa Publishing House, 1999.

Question Pattern

Section A : 10 x 2 = 20 Marks, 2 Questions from each Unit.
Section B : 5 x 5 = 25 Marks, EITHER OR (a or b) Pattern, One question from each Unit.
Section C : 3 x 10 = 30 Marks, 3 out of 5, One Question from each Unit.

Unit - I

Definition: Group

A nonempty set of elements G is said to form a group if in G there is defined a binary operation, called the product and denoted by $\cdot$, such that (1) $a, b \in G$ implies that $a \cdot b \in G$ (closed) (2) $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative law) (3) There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$ (4) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition: Abelian

A group G is said to be abelian (or commutative) if for every $a, b \in G$, $a \cdot b = b \cdot a$

Definition: Subgroups

A nonempty subset H of a group G is said to be a subgroup of G if, under the product in G, H itself forms a group.

Lemma: A nonempty subset H of the group G is a subgroup of G if and only if (1) $a, b \in H$ implies that $ab \in H$ (2) $a \in H$ implies that $a^{-1} \in H$.

A counting principle

Lemma: HK is a subgroup of G if and only if $HK = KH$.

Proof: Suppose, first, that $HK = KH$; that is, if $h \in H$ and $k \in K$ then $hk = k_1 h_1$ for some $k_1 \in K$, $h_1 \in H$.

To prove that HK is a subgroup we must verify that it is closed and every element in HK has its inverse in HK.

Let's show the closure first.

So suppose $x = hk \in HK$ and $y = h'k' \in HK$

Then $xy = (hk)(h'k')$. but since $kh' \in KH = HK$

$kh' = h_2 k_2$ with $h_2 \in H$, $k_2 \in K$

Hence $xy = h(kh')k'$

$= h(h_2 k_2)k' = (hh_2)(k_2 k') \in HK$ (ie) $x \in HK, y \in HK \Rightarrow xy \in HK$

$\therefore HK$ is closed

Also, $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK \Rightarrow x^{-1} \in HK$

Thus HK is a subgroup of G.

Conversely, If HK is a subgroup of G, then for any $h \in H, k \in K \Rightarrow h^{-1}k^{-1} \in HK$ and so $kh = (h^{-1}k^{-1})^{-1} \in HK$. Thus $KH \subset HK \longrightarrow (1)$

Now if x is any element of HK,

$x^{-1} = hk \in HK$ and so $x = (x^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$ so $HK \subset KH \longrightarrow (2)$

Comparing (1) & (2) $HK = KH$

Thus completes the proof

Corollary: If H, K are subgroups of the abelian group G, then HK is a subgroup of G.

Theorem:

If H and K are finite subgroups of G of orders $o(H)$ and $o(K)$ respectively, then $o(HK) = \dfrac{o(H)o(K)}{o(H\cap K)}$

proof: Let $H\cap K = \{e = r_1, r_2 \ldots r_m\}$. Then $o(H\cap K) = m$

First list all the elements of HK with repetitions as $hk : h \in H,\ k \in K \longrightarrow ①$

There are $o(H)o(K)$ entries in the list ① (with repetitions).

We shall show that each element of HK is repeated exactly m (ie $o(H\cap K)$) times in the list ①.

Let $x \in HK$. Then $x = hk$ for some $h\in H$ and $k \in K$

For $i = 1, 2, 3 \ldots m$ take $h_i = hr_i$ and $k_i = r_i^{-1}k$

Then $x = h_1k_1 = h_2k_2 = \ldots = h_mk_m \longrightarrow ②$

Every element $x \in HK$ can be written as "an element of H times an element of K" in m distinct ways.

Suppose hk can be written as $h'k'$ for some $h' \in H$ and $k' \in K$.

Then we show that $h'k'$ is already listed in the representation in ②

claim $h'k'$ is already listed in ②

Suppose $hk = h'k' \Rightarrow (h')^{-1}h = k'k^{-1} \in H\cap K = \{e = r_1, r_2 \ldots r_m\}$

$$((h')^{-1}h)^{-1} = (k'k^{-1})^{-1} \in H\cap K$$

$$\Rightarrow h^{-1}h' = k(k')^{-1} \in H\cap K \Rightarrow h^{-1}h' = k(k')^{-1} = r_i \text{ for some } i$$

$h^{-1}h' = r_i \Rightarrow h' = hr_i = h_i$ and $k(k')^{-1} = r_i \Rightarrow k = r_ik' \Rightarrow k' = r_i^{-1}k = k_i$

Hence $h' = h_i$ and $k' = k_i$

Therefore, by ①, $o(HK) = \dfrac{o(H)o(K)}{m} = \dfrac{o(H)o(K)}{o(H\cap K)}$

Hence the proof.

Corollary: If H and K are subgroups of G and $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$, then $H\cap K \neq (e)$.

Proof: Since $HK \subset G$, $o(HK) \le o(G)$.

To prove $H\cap K \neq (e)$ (ie) $o(H\cap K) > 1$.

Suppose if possible, $o(H\cap K) = 1$ By above theorem

$$o(HK) = \frac{o(H)o(K)}{o(H\cap K)} > \frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H\cap K)} = \frac{o(G)}{1} = o(G) \text{ (ie) } o(HK) > o(G)$$

This is a contradiction.

Therefore $H\cap K \neq (e)$

Hence completes the corollary.

Proposition: If G is a group with $o(G) = pq$, where p and q are prime numbers such that $p > q$ then G has at most one subgroup of order p.

Proof: If G has no subgroup of order p, then we are done.

Suppose, if possible, H and K be subgroups of G with $o(H) = o(K) = p$.

We show that $H = K$. Now $pq < p^2$ $(\because p > q)$

$$\Rightarrow \sqrt{pq} < p \Rightarrow \sqrt{o(G)} < o(H) = o(K)$$

Then by previous corollary, $H \cap K \neq (e)$ (ie) $o(H \cap K) \neq 1$ (or) > 1

But $H \cap K$ is a subgroup of both H and K.

By Lagrange's theorem, $o(H \cap K) \mid o(H)$ and $o(H \cap K) \mid o(K)$

(ie) $o(H \cap K) \mid p$ Here $o(H \cap K) = 1$ (or) p

But $o(H \cap K) \neq 1$

$\therefore o(H \cap K) = p$

But $H \cap K \subset H$ and $o(H \cap K) = o(H) = p$.

Then we must have $H \cap K = H$ and similarly $H \cap K = K$

Hence $H = K$.

Normal subgroups and Quotient Groups:

Definition: A subgroup N of G is said to be a normal subgroup of G if for every $g \in G$ and $n \in N$, $gng^{-1} \in N$.

Lemma: N is a normal subgroup of G if and only if $gNg^{-1} = N$ for every $g \in G$

Proof: If $gNg^{-1} = N$ for every $g \in G$, certainly $gNg^{-1} \subset N$, so N is normal in G

Suppose that N is normal in G. Thus if $g \in G$, $gNg^{-1} \subset N$ and $g^{-1}Ng \Rightarrow$

$$g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N.$$

Now, since $g^{-1}Ng \subset N$, $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$

whence $N = gNg^{-1}$.

Lemma: The subgroup N of G is a normal subgroup of G if and only if every left coset of N in G is a right coset of N in G.

Proof: If N is a normal subgroup of G, then for every $g \in G$, $gNg^{-1} = N$

whence $(gNg^{-1})g = Ng$

$$gN(g^{-1}g) = Ng \Rightarrow gN = Ng$$

and so the left coset gN is the right coset Ng.

Conversely, that every left coset of N in G is a right coset of N in G.

Thus, for $g \in G$, gN, being a left coset, must be a right coset.

Since $g = ge \in gN$, whatever right coset gN turns out to be, it must contain the element g; however, g is in the right coset Ng, and two distinct right cosets have no element in common.

So this right coset is unique. Thus $gN = Ng$ follows

In other words, $gNg^{-1} = (gN)g^{-1} = Ngg^{-1} = N$

and so N is a normal subgroup of G.

Hence the Lemma

Lemma: A subgroup N of G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Proof:

Suppose that N is a normal subgroup of G and that $a, b \in G$. Consider $(Na)(Nb)$. Since N is normal in G, $aN = Na$, and so

$$NaNb = N(aN)b = N(Na)b = NNab = Nab$$

Hence the proof.

Theorem: If G is a group, N be a normal subgroup of G, then G/N is also a group. It is called the quotient group or factor group of G by N.

Proof: Let G/N denote the collection of right cosets of N in G

(ie) the elements of G/N are certain subsets of G and we use the Product of subsets of G to yield for us a product in G/N.

For this product we claim

1. $X, Y \in G/N \Rightarrow XY \in G/N$
   for $X = Na$, $Y = Nb$ for some $a, b \in G$, and $XY = NaNb = Nab \in G/N$
2. $X, Y, Z \in G/N$, then $X = Na$, $Y = Nb$, $Z = Nc$ with $a, b, c \in G$ and so $(XY)Z = (NaNb)Nc = N(ab)Nc = N(ab)c = Na(bc)$
   (Since G is associative) $= Na(Nbc)$
   $= Na(NbNc)$
   $= X(YZ)$.

   Thus the product in G/N satisfies the associative Law.
3. Consider the element $N = Ne \in G/N$. If $X \in G/N$, $X = Na$, $a \in G$ so $XN = NaNe = Nae = Na = X$, and similarly $NX = X$. consequently, Ne is an identity element for G/N.
4. Suppose $X = Na \in G/N$ (where $a \in G$); thus $Na^{-1} \in G/N$ and $NaNa^{-1} = Naa^{-1} = Ne$.
   III^{ly} $Na^{-1}Na = Ne$. Hence Na^{-1} is the Inverse of Na in G/N.

Thus G/N is a group.

Hence completes the proof.

Lemma: If G is a finite group and N is a normal subgroup of G, then $o(G/N) = o(G)/o(N)$

Proof: If G is a finite group and N is a normal subgroup of G

(i) $G = \{a_1, a_2, a_3, \ldots a_n\}$

Let be $o(G/N) = n$, we know that

$$G = \bigcup_{i=1}^{n} a_i N = a_1 N \cup a_2 N \cup a_3 N \cup \ldots \cup a_n N$$

then $o(G) = \sum_{i=1}^{n} o(a_i N) = \sum_{i=1}^{n} o(N) = n\, o(N)$

$o(a_i N) = o(N)$ then $o(G)/o(N) = n = o(G/N)$

(ii) $o(G/N) = o(G)/o(N)$.

Hence the proof.

Homomorphisms:

A mapping ϕ from a group G into a group $\bar{G}$ is said to be a homomorphism if for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Example:

1. $\phi(x) = e$ for all $x \in G$.

Here $\phi(y) = e$ for all $y \in G$

By the definition, $x, y \in G$, $\phi(xy) = e = e \cdot e = \phi(x)\phi(y) \Rightarrow \phi$ is a homomorphism

2. Let G be the group of all real numbers under addition (ie, ab for $a, b \in G$ is really the real number $a+b$). and let $\bar{G}$ be the group of nonzero real numbers with the product being ordinary multiplication of real numbers.

Define $\phi : G \to \bar{G}$ by $\phi(a) = 2^a$

$a, b \in G \Rightarrow \phi(ab) = 2^{ab} = 2^{a+b} = 2^a \cdot 2^b = \phi(a)\phi(b)$

$\Rightarrow \phi$ is a homomorphism

3. Let $G = S_3 = \{e, \phi, \psi, \psi^2, \phi\psi, \phi\psi^2\}$ and $\bar{G} = \{e, \phi\}$.

Define the mapping $f : G \to \bar{G}$ by $f(\phi^i \psi^j) = \phi^i$. Thus $f(e) = e$, $f(\phi) = \phi$, $f(\psi) = e$, $f(\psi^2) = e$, $f(\phi\psi) = \phi$, $f(\phi\psi^2) = \phi$.

Here $\phi, \phi\psi \in G \Rightarrow f(\phi \cdot \phi\psi) = f(\phi^2\psi) = f(\phi^2\psi') = \phi^2 = \phi \cdot \phi$
$= f(\phi) \cdot f(\phi\psi)$

$\Rightarrow f$ is homomorphism.

4. Let G be the group of integers under addition and let $\bar{G} = G$. For the integer $x \in G$ define ϕ by $\phi(x) = 2x$.

$\phi(x+y) = 2x + 2y = \phi(x) + \phi(y) \Rightarrow \phi$ is homomorphism.

5. Let G be the group of nonzero real numbers under multiplication, $\bar{G} = \{1, -1\}$, where $1 \cdot 1 = 1$, $(-1)(-1) = 1$, $1(-1) = (-1)1 = -1$. Define $\phi : G \to \bar{G}$ by $\phi(x) = 1$ if x is Positive, $\phi(x) = -1$ if x is negative.

The fact that ϕ is a homomorphism

6. Let G be the group of integers under addition. Let G_n be the group of integers under addition modulo n. Define ϕ by $\phi(x)$ = remainder of x on division by n. One can easily verify this is a homomorphism.

7. Let G be the group of positive real numbers under multiplication and let $\bar{G}$ be the group of all real numbers under addition.

Define $\phi : G \to \bar{G}$ by $\phi(x) = \log_{10} x$. Thus $\phi(xy) = \log_{10}(xy) = \log_{10} x + \log_{10}(y)$

Since the operation, on the right side, in $\bar{G}$ is in fact addition $= \phi(x) \cdot \phi(y)$

Thus ϕ is a homomorphism of G into $\bar{G}$. In fact, not only is ϕ a homomorphism but, in addition, it is one-to-one and onto.

8. Let G be the group of all real 2x2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad-bc \neq 0$ under matrix multiplication. Let $\bar{G}$ be the group of all nonzero real numbers under multiplication. Define $\phi : G \to \bar{G}$ by $\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc$.

Lemma: Suppose G is a group, N be a normal subgroup of G; define the mapping ϕ from G to G/N by $\phi(x) = Nx$ for all $x \in G$. Then ϕ is a homomorphism of G onto G/N.

Proof:

Given G is a group, N be a normal subgroup of G and $\phi : G \to G/N$ by $\phi(x) = Nx$ for all $x \in G$. To prove ϕ is a homomorphism.

That ϕ is onto is trivial, for every element $X \in G/N$ is of the form $X = Ny$, $y \in G$, so $X = \phi(y)$.

To verify the multiplicative property required in order that ϕ be a homomorphism one just notes that if $x, y \in G$,

$$\phi(xy) = Nxy = NxNy = \phi(x)\phi(y)$$

Hence the proof.

Definition: (Kernel)

If ϕ is a homomorphism of G into $\bar{G}$, the kernel of ϕ, K_ϕ is defined by $K_\phi = \{x \in G \mid \phi(x) = \bar{e}, \bar{e} = \text{identity element of } \bar{G}\}$.

Lemma: If ϕ is a homomorphism of G into $\bar{G}$, then 1. $\phi(e) = \bar{e}$, the unit element of $\bar{G}$. 2. $\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \in G$.

Proof: To prove (1) we merely calculate $\phi(x)\bar{e} = \phi(x) = \phi(xe) = \phi(x)\phi(e)$, so by the cancellation property in $\bar{G}$, we have that $\phi(e) = \bar{e}$.

(2) one notes that $\bar{e} = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$, so by the very definition of $\phi(x)^{-1}$ in $\bar{G}$, we obtain the result that $\phi(x^{-1}) = \phi(x)^{-1}$

Lemma: If ϕ is a homomorphism of G into $\bar{G}$ with kernel K, then K is a normal subgroup of G.

Proof: First we must check whether K is a subgroup of G. To see this one must show that K is closed under multiplication and has inverses in it for every element belonging to K.

If $x, y \in K$, then $\phi(x) = \bar{e}$, $\phi(y) = \bar{e}$, where $\bar{e}$ is the identity element of $\bar{G}$, and so $\phi(xy) = \phi(x)\phi(y) = \bar{e}\bar{e} = \bar{e}$, whence $xy \in K$. Also, if $x \in K$, $\phi(x) = \bar{e}$, so by previous Lemma, $\phi(x^{-1}) = \phi(x)^{-1} = \bar{e}^{-1} = \bar{e}$, thus $x^{-1} \in K$.

K is, accordingly, a subgroup of G.

To prove the normality of K one must establish that for any $g \in G$, $k \in K$, $gkg^{-1} \in K$; in other words, one must prove that $\phi(gkg^{-1}) = \bar{e}$ whenever $\phi(k) = \bar{e}$

But $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\,\bar{e}\,\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = \bar{e}$

Hence completes the proof

Lemma: If ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is given by Kx, where x is any particular inverse image of $\bar{g}$ in G.

Proof: Let ϕ now be a homomorphism of the group G onto the group $\bar{G}$ and suppose that K is the kernel of ϕ. If $\bar{g} \in \bar{G}$, we say an element $x \in G$ is an inverse image of $\bar{g}$ under ϕ if $\phi(x) = \bar{g}$. By the definition of K is all the inverse images of $\bar{g}$ (ie) $\bar{g} = \bar{e}$.

Suppose $x \in G$ is one inverse image of $\bar{g}$, clearly for if $k \in K$, and if $y = kx$, then $\phi(y) = \phi(kx) = \phi(k)\phi(x) = \bar{e}\bar{g} = \bar{g}$. Thus all the elements Kx are in the inverse image of $\bar{g}$ whenever x is.

Let us suppose that $\phi(z) = \bar{g} = \phi(x)$. Ignoring the middle term we are left with $\phi(z) = \phi(x)$ and so $\phi(z)\phi(x)^{-1} = \bar{e}$. But $\phi(x)^{-1} = \phi(x^{-1})$. whence $\bar{e} = \phi(z)\phi(x)^{-1} = \phi(z)\phi(x^{-1}) = \phi(zx^{-1})$, in consequence of which $zx^{-1} \in K$; thus $z \in Kx$. In other words, we have shown that Kx accounts for exactly all the inverse images of $\bar{g}$ whenever x is a single such inverse image.

Hence completes the proof.

Definition: A homomorphism ϕ from G into $\bar{G}$ is said to be an isomorphism if ϕ is one-to-one

Definition: Two groups G, G^* are said to be isomorphic if there is an isomorphism of G onto G^*. In this case we write $G \approx G^*$

Theorem: Isomorphism is an equivalence relation among groups. (ie) (i) $G \approx G$ (ii) $G \approx G^*$ implies $G^* \approx G$ (iii) $G \approx G^*$, $G^* \approx G^{**}$ implies $G \approx G^{**}$

Proof: (i) For any group G, $i_G : G \to G$ is clearly an isomorphism.

Hence $G \approx G$. Therefore the relation is reflexive

(ii) Now, let $G \approx G^*$ and let $f : G \to G^*$ be an isomorphism.

Then f is a bijection. $\therefore f^{-1} : G^* \to G$ is also a bijection.

Now let $x^*, y^* \in G^*$

Let $f^{-1}(x^*) = x$ and $f^{-1}(y^*) = y$. Then $f(x) = x^*$ and $f(y) = y^*$

$\therefore f(xy) = f(x)f(y) = x^* y^* \Rightarrow f^{-1}(x^* y^*) = xy = f^{-1}(x^*) f^{-1}(y^*)$

Hence f^{-1} is an isomorphism. Thus $G^* \approx G$ and hence the relation is symmetric.

(iii) Now let $G \approx G^*$ and $G^* \approx G^{**}$.

Then there exist isomorphisms $f : G \to G^*$ and $g : G^* \to G^{**}$

Since f and g are bijections, $g \circ f : G \to G^*$ is also a bijection.

Now let $x, y \in G$. Then $(g \circ f)(xy) = g[f(xy)] = g[f(x) f(y)]$ [Since f is an isomorphism]

$= g[f(x)]\, g[f(y)]$ [Since g is an isomorphism]

$= g \circ f(x) \cdot g \circ f(y)$

Hence $g \circ f$ is an isomorphism. Thus $G \approx G^{**}$ and hence the relation is transitive.

$\therefore$ Isomorphism is an equivalence relation among groups.

Corollary: A homomorphism ϕ of G into $\bar{G}$ with kernel K_ϕ is an isomorphism of G into $\bar{G}$ if and only if $K_\phi = (e)$.

(FUNDAMENTAL THEOREM OF HOMOMORPHISM)

Theorem: Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. Then $G/K \approx \bar{G}$.

Proof: Consider the diagram

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \bar{G} \\ \sigma \downarrow & & \\ G/K & & \end{array}$$

where $\sigma(g) = Kg$.

We should like to complete this to

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \bar{G} \\ \sigma \downarrow & \nearrow \psi & \\ G/K & & \end{array} \qquad \text{(i.e)} \qquad \begin{array}{ccc} g & \longrightarrow & \phi(g) \\ \downarrow & \nearrow \psi & \\ Kg & & \end{array}$$

Define $\psi : G/K \to \bar{G}$ by $\psi(Kg) = \phi(g)$.

Step (i) ψ is well defined and ψ is one-one

Let $X \in G/K$, $X = Kg$ then $\psi(Kg) = \phi(g)$.

If $X \in G/K$, it can be written as Kg in several ways (for instance, $Kg = Kkg$, $k \in K$) but if $X = Kg = Kg'$, $g, g' \in G$ then on one hand $\psi(X) = \phi(g)$, and on the other, $\psi(X) = \phi(g')$. For the mapping ψ to make sense it had better be true that $\phi(g) = \phi(g')$.

So, suppose $Kg = Kg'$; then $g = kg'$ where $k \in K$ hence $\phi(g) = \phi(kg')$.

$\phi(g) = \phi(kg') = \phi(k)\phi(g') = \bar{e}\,\phi(g') = \phi(g')$ since $k \in K$, the kernel of ϕ.

Step (ii) ψ is onto

For, if $\bar{x} \in \bar{G}$, $\bar{x} = \phi(g)$, $g \in G$ (since ϕ is onto) so $\bar{x} = \phi(g) = \psi(Kg)$

Step (iii) ψ is a homomorphism

If $X, Y \in G/K$, $X = Kg$, $Y = Kf$, $g, f \in G$ then $XY = KgKf = Kgf$

so that $\psi(XY) = \psi(Kgf) = \phi(gf) = \phi(g)\phi(f)$ since ϕ is a homomorphism of G onto $\bar{G}$.

But $\psi(X) = \psi(Kg) = \phi(g)$, $\psi(Y) = \psi(Kf) = \phi(f)$.

So we see that $\psi(XY) = \psi(X)\psi(Y)$ and ψ is a homomorphism of G/K onto $\bar{G}$.

To prove that ψ is an isomorphism of G/K onto $\bar{G}$ all that remains is to demonstrate that the kernel of ψ is the unit element of G/K. Since the unit element of G/K is $K = Ke$, we must show that if $\psi(Kg) = \bar{e}$ then $Kg = Ke = K$.

This is now easy, for $\bar{e} = \psi(Kg) = \phi(g)$, so that $\phi(g) = \bar{e}$, whence g is in the kernel of ϕ, namely K. But then $Kg = K$ since K is a subgroup of G. All the pieces have been put together. We have exhibited a one-to-one homomorphism of G/K onto $\bar{G}$.

Thus $G/K \approx \bar{G}$. Hence completes the proof.

(CAUCHY'S THEOREM FOR ABELIAN GROUPS)

Suppose G is a finite abelian group and $p \mid o(G)$, where p is a prime number. Then there is an element $a \neq e \in G$ such that $a^p = e$.

Proof: If G has no subgroups $H \neq (e)$, G, by the result of a problem earlier in the chapter, G must be cyclic of prime order. This prime must be p and G certainly has $p-1$ elements $a \neq e$ satisfying $a^p = a^{o(G)} = e$.

So suppose G has a subgroup $N \neq (e), G$. If $p \mid o(N)$, by our induction hypothesis, since $o(N) < o(G)$ and N is abelian, there is an element $b \in N$, $b \neq e$, satisfying $b^p = e$; since $b \in N \subset G$ we would have exhibited an element of the type required.

So we may assume that $p \nmid o(N)$. Since G is abelian, N is a normal subgroup of G, so G/N is a group. Moreover, $o(G/N) = o(G) / o(N)$, and since $p \nmid o(N)$, $p \mid \frac{o(G)}{o(N)} < o(G)$.

Also, since G is abelian, G/N is abelian. Thus by our induction hypothesis there is an element $X \in G/N$ satisfying $X^p = e_1$, the unit element of G/N, $X \neq e_1$. By the very form of the elements of G/N, $X = Nb$, $b \in G$, so that $X^p = (Nb)^p = Nb^p$.

Since $e_1 = Ne$, $X^p = e_1$, $X \neq e_1$ translates into $Nb^p = N$, $Nb \neq N$. Thus $b^p \in N$, $b \notin N$. Using one of the corollaries to Lagrange's theorem, $(b^p)^{o(N)} = e$.

That is, $b^{o(N)p} = e$. Let $c = b^{o(N)}$; certainly $c^p = e$. In order to show that c is an element that satisfies the conclusion of the theorem we must finally show that $c \neq e$. However, if $c = e$, $b^{o(N)} = e$, and so $(Nb)^{o(N)} = N$. Combining this with $(Nb)^p = N$, $p \nmid o(N)$, p be a prime number, we find that $Nb = N$, and so $b \in N$, a contradiction. Thus $c \neq e$, $c^p = e$ and we have completed the induction.

This proves the result.

SYLOW'S THEOREM FOR ABELIAN GROUPS

If G is an abelian group of order $o(G)$, and if p is a prime number, such that $p^\alpha \mid o(G)$, $p^{\alpha+1} \nmid o(G)$, then G has a subgroup of order p^α.

Proof: If $\alpha = 0$, the subgroup (e) satisfies the conclusion of the result. So suppose $\alpha \neq 0$. Then $p \mid o(G)$. By Application 1, there is an element $a \neq e \in G$ satisfying $a^p = e$.

Let $S = \{x \in G \mid x^{p^n} = e$ some integer $n\}$. Since $a \in S$, $a \neq e$, it follows that $S \neq (e)$. We now assert that S is a subgroup of G. Since G is finite we must only verify that S is closed. If $x, y \in S$, $x^{p^n} = e$, $y^{p^m} = e$ so that

$(xy)^{p^{n+m}} = x^{p^{n+m}} y^{p^{n+m}} = e$ (we have used that G is abelian) proving that $xy \in S$. We next claim that $o(S) = p^{\beta}$ with β an integer $0 < \beta \leq \alpha$. For, if some prime $q \mid o(S)$, $q \neq p$, by Cauchy's theorem for Abelian groups, there is an element $c \in S$, $c \neq e$, satisfying $c^q = e$. However, $c^{p^n} = e$ for some n since $c \in S$.

Since p^n, q are relatively prime, we can find integers λ, μ such that $\lambda q + \mu p^n = 1$, so that $c = c^1 = c^{\lambda q + \mu p^n} = (c^q)^{\lambda} (c^{p^n})^{\mu} = e$, contradicting $c \neq e$. By Lagrange's thm, $o(S) \mid o(G)$, so that $\beta \leq \alpha$. Suppose that $\beta < \alpha$; consider the abelian group G/S. Since $\beta < \alpha$ and $o(G/S) = o(G)/o(S)$, $p \mid o(G/S)$, there is an element Sx, $(x \in G)$ in G/S satisfying $Sx \neq S$, $(Sx)^{p^n} = S$ for some integer n.

But $S = (Sx)^{p^n} = Sx^{p^n}$, and so $x^{p^n} \in S$ consequently

$e = (x^{p^n})^{o(S)} = (x^{p^n})^{p^\beta} = x^{p^{n+\beta}}$. Therefore, x satisfies the exact requirements needed to put it in S; in other words, $x \in S$.

Consequently $Sx = S$ contradicting $Sx \neq S$. Thus $\beta < \alpha$ is impossible and we are left with the only alternative, namely, that $\beta = \alpha$. S is the required subgroup of order p^{α}. Corollary 1 Proof:

[Suppose T is another subgroup of G of order p^{α}; $T \neq S$. Since G is abelian $ST = TS$, so that ST is a subgroup of G.

$$o(ST) = \frac{o(S)\,o(T)}{o(S \cap T)} = \frac{p^{\alpha} p^{\alpha}}{o(S \cap T)}$$

and since $S \neq T$, $o(S \cap T) < p^{\alpha}$, leaving us with $o(ST) = p^{\gamma}$, $\gamma > \alpha$. Since ST is a subgroup of G, $o(ST) \mid o(G)$; thus $p^{\gamma} \mid o(G)$ violating the fact that α is the largest power of p which divides $o(G)$.

Thus no such subgroup T exists, and S is the unique subgroup of order p^{α}.]

COROLLARY 1 If G is abelian of order $o(G)$ and $p^{\alpha} \mid o(G)$, $p^{\alpha+1} \nmid o(G)$, there is a unique subgroup of G of order p^{α}.

Lemma Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K. For $\bar{H}$ a subgroup of $\bar{G}$ let H be defined by $H = \{x \in G \mid \phi(x) \in \bar{H}\}$. Then H is a subgroup of G and $H \supset K$; if $\bar{H}$ is normal in $\bar{G}$, then H is normal in G. Moreover, this association sets up a one-to-one mapping from the set of all subgroups of $\bar{G}$ onto the set of all subgroups of G which contain K.

Proof Suppose ϕ is a homomorphism of G onto $\bar{G}$ with Kernel K and suppose that $\bar{H}$ is a subgroup of $\bar{G}$ let $H = \{x \in G \mid \phi(x) \in \bar{H}\}$ We assert that H is subgroup of G and that $H \supset K$. That $H \supset K$ is trivial, for if $x \in K$, $\phi(x) = \bar{e}$ is in $\bar{H}$, So that $K \subset H$ follows.

Suppose now that $x, y \in H$, hence $\phi(x) \in \bar{H}$, $\phi(y) \in \bar{H}$ from which we deduce that $\phi(xy) = \phi(x)\phi(y) \in \bar{H}$ Therefore, $xy \in H$ and H is closed under the product in G. Furthermore, if $x \in H$, $\phi(x) \in \bar{H}$ and So $\phi(x^{-1}) = \phi(x)^{-1} \in \bar{H} \Rightarrow x^{-1} \in H$.

Next we prove that $\bar{H}$ is normal in $\bar{G}$.

Let $g \in G$, $h \in H$; then $\phi(h) \in \bar{H}$, whence $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in \bar{H}$ Since $\bar{H}$ is normal in $\bar{G}$. otherwise stated, $ghg^{-1} \in H$, from which it follows that H is normal in G. One other point should be noted, namely, that the homomorphism ϕ from G onto $\bar{G}$, when just considered on elements of H, induces a homomorphism of H onto $\bar{H}$, with kernel exactly K, Since $K \subset H$, by previous theorem, we have that $\bar{H} \approx H/K$.

Suppose, conversely, that L is a subgroup of G and $K \subset L$. Let $\bar{L} = \{\bar{x} \in \bar{G} \mid \bar{x} = \phi(l), l \in L\}$. Now verify that $\bar{L}$ is a subgroup of $\bar{G}$. can we explicitly describe the subgroup $T = \{y \in G \mid \phi(y) \in \bar{L}\}$ clearly $L \subset T$ Is there any element $t \in T$ which is not in L. So suppose $t \in T$; thus $\phi(t) \in \bar{L}$, so by the very definition of $\bar{L}$, $\phi(t) = \phi(l)$ for some $l \in L$.

Thus $\phi(tl^{-1}) = \phi(t)\phi(l)^{-1} = \bar{e}$, whence $tl^{-1} \in K \subset L$, thus t is in $Ll = L$. Equivalently we have proved that $T \subset L$, which, combined with $L \subset T$, yields that $L = T$.

Thus we have set up a one-to-one correspondence between the set of all subgroups of $\bar{G}$ and the set of all subgroups of G which contain K. Moreover, in this correspondence, a normal subgroup of G corresponds to a normal subgroup of $\bar{G}$.

Thus completes the proof.

Theorem: Let ϕ be a homomorphism of G onto $\bar{G}$ with kernel K, and let $\bar{N}$ be a normal subgroup of $\bar{G}$, $N = \{x \in G \mid \phi(x) \in \bar{N}\}$ Then $G/N \approx \bar{G}/\bar{N}$. Equivalently $G/N \approx (G/K)/(N/K)$.

Proof: As we already know, there is a homomorphism θ of $\bar{G}$ onto $\bar{G}/\bar{N}$ defined by $\theta(\bar{g}) = \bar{N}\bar{g}$. We define the mapping $\psi : G \to \bar{G}/\bar{N}$ by $\psi(g) = \bar{N}\phi(g)$ for all $g \in G$. To begin with, ψ is onto, for if $\bar{g} \in \bar{G}$, $\bar{g} = \phi(g)$ for some $g \in G$, Since ϕ is onto, so the typical element $\bar{N}\bar{g}$ in $\bar{G}/\bar{N}$ can be represented as $\bar{N}\phi(g) = \psi(g)$.

If $a, b \in G$, $\psi(ab) = \bar{N}\phi(ab)$ by the definition of the mapping ψ. However, Since ϕ is a homomorphism, $\phi(ab) = \phi(a)\phi(b)$. Thus $\psi(ab) = \bar{N}\phi(a)\phi(b) = \bar{N}\phi(a) \cdot \bar{N}\phi(b) = \psi(a)\psi(b)$ so far we have shown that ψ is a homomorphism of G onto $\bar{G}/\bar{N}$. What is the Kernel, T of ψ? Firstly, if $n \in N$, $\phi(n) \in \bar{N}$, so that $\psi(n) = \bar{N}\phi(n) = \bar{N}$, the identity element of $\bar{G}/\bar{N}$, proving that $N \subset T$.

On the otherhand, if $t \in T$, $\psi(t) =$ identity element of $\bar{G}/\bar{N} = \bar{N}$; but $\psi(t) = \bar{N}\phi(t)$ Comparing these two evaluations of $\psi(t)$, we arrive at $\bar{N} = \bar{N}\phi(t)$, which forces $\phi(t) \in \bar{N}$, but this places t in N by definition of N. (ie) $T \subset N$. The Kernel of ψ has been proved to be equal to N. But then ψ is a homomorphism of G onto $\bar{G}/\bar{N}$ with Kernel N.

By theorem $G/N \approx \bar{G}/\bar{N}$, which is the first part of the theorem. The last statement in the theorem is Immediate from the observation that $\bar{G} \approx G/K$, $\bar{N} \approx N/K$, $\bar{G}/\bar{N} \approx (G/K)/(N/K)$. Thus completes the proof.

AUTOMORPHISMS

Definition: By an automorphism of a group G we shall mean an isomorphism of G onto itself.

Lemma: If G is a group, then $\mathcal{A}(G)$, the set of automorphisms of G, is also a group.

Proof: Let I be the mapping of G which sends every element onto itself, that is, $xI = x$, for all $x \in G$. Trivially I is an automorphism of G. Let $\mathcal{A}(G)$ denote the set of all automorphisms of G, being a subset of $A(G)$, the set of one-to-one mappings of G onto itself, for elements of $\mathcal{A}(G)$ we can use the product of $A(G)$, namely, composition of mappings.

This product then satisfies the associative law in $A(G)$, and so, a fortiori, in $\mathcal{A}(G)$. Also I, the unit element of $A(G)$, is in $\mathcal{A}(G)$, so $\mathcal{A}(G)$ is not empty.

An obvious fact that we should try to establish is that $\mathcal{A}(G)$ is a subgroup of $A(G)$ and so, in its own rights, $\mathcal{A}(G)$ should be a group. If T_1, T_2 are in $\mathcal{A}(G)$ we already know that $T_1T_2 \in A(G)$. We want it to be in the smaller set $\mathcal{A}(G)$.

We proceed to verify this. For all $x, y \in G$,

$$(xy)T_1 = (xT_1)(yT_1)$$
$$(xy)T_2 = (xT_2)(yT_2)$$

therefore

$$(xy)T_1T_2 = ((xy)T_1)T_2 = (xT_1)(yT_1)T_2$$
$$= ((xT_1)T_2)((yT_1)T_2) = (xT_1T_2)(yT_1T_2).$$

That is, $T_1T_2 \in \mathcal{A}(G)$. There is only one other fact that needs verifying in order that $\mathcal{A}(G)$ be a subgroup of $A(G)$, namely, that if $T \in \mathcal{A}(G)$, then $T^{-1} \in \mathcal{A}(G)$.

If $x, y \in G$, then $((xT^{-1})(yT^{-1}))T = ((xT^{-1})T)((yT^{-1})T) = (xI)(yI) = xy$

thus $(xT^{-1})(yT^{-1}) = (xy)T^{-1}$ placing T^{-1} in $\mathcal{A}(G)$.

Hence Completes the proof.

Lemma: $\mathcal{I}(G) \approx G/Z$, where $\mathcal{I}(G)$ is the group of inner automorphisms of G, and Z is the center of G.

Proof: Let G be a group for $g \in G$ define $T_g: G \to G$ by $xT_g = g^{-1}xg$ for all $x \in G$. We claim that T_g is an automorphism of G. First, T_g is onto, for given $y \in G$, let $x = gyg^{-1}$. Then $xT_g = g^{-1}(x)g = g^{-1}(gyg^{-1})g = y$, so T_g is onto.

Now consider, for $x, y \in G$, $(xy)T_g = g^{-1}(xy)g = g^{-1}(xgg^{-1}y)g = (g^{-1}xg)(g^{-1}yg) = (xT_g)(yT_g)$

Consequently T_g is a homomorphism of G onto itself. We further assert that T_g is one-to-one, for if $xT_g = yT_g$, then $g^{-1}xg = g^{-1}yg$, so by the cancellation laws in G, $x = y$. T_g is called the inner automorphism corresponding to g.

If G is non-abelian, there is a pair $a, b \in G$ such that $ab \neq ba$; but then $bT_a = a^{-1}ba \neq b$, so that $T_a \neq I$. Thus for a non-abelian group G there always exist nontrivial automorphisms.

Let $\mathcal{I}(G) = \{T_g \in \mathcal{A}(G) \mid g \in G\}$. The computation of T_{gh} for $g, h \in G$, might be of some interest. So, suppose $x \in G$; by definition

$$xT_{gh} = (gh)^{-1}x(gh) = h^{-1}g^{-1}xgh = (g^{-1}xg)T_h = (xT_g)T_h = xT_gT_h.$$

$\Rightarrow T_{gh} = T_gT_h$. clearly $\mathcal{I}(G)$ is a subgroup of $\mathcal{A}(G)$. usually $\mathcal{I}(G)$ is called the group of inner automorphisms of G

It is suggestive, for if we consider the mapping $\psi: G \to \mathcal{A}(G)$ defined by $\psi(g) = T_g$ for every $g \in G$, then $\psi(gh) = T_{gh} = T_g T_h = \psi(g)\psi(h)$.

(ie) ψ is a homomorphism of G into $\mathcal{A}(G)$ whose image is $\mathcal{J}(G)$.

Suppose we consider the kernel of ψ is K, and suppose $g_0 \in K$. Then $\psi(g_0) = I$, or equivalently, $T_{g_0} = I$. But this says that for any $x \in G$, $x T_{g_0} = x$, however, $x T_{g_0} = g_0^{-1} x g_0$ and so $x = g_0^{-1} x g_0$ for all $x \in G$. Thus $g_0 x = g_0 g_0^{-1} x g_0 = x g_0$, g_0 must commute with all elements of G.

But the center of G, Z, was defined to be precisely all elements in G which commute with every element of G. Thus $K \subset Z$. However, if $z \in Z$, then $x T_z = z^{-1} x z = z^{-1}(zx)$ (since $zx = xz$) $= x$, whence $T_z = I$ and so $z \in K$. Therefore, $Z \subset K$. Having proved both $K \subset Z$ & $Z \subset K$ we have that $Z = K$.

Summarizing, ψ is a homomorphism of G into $\mathcal{A}(G)$ with image $\mathcal{J}(G)$ and kernel Z. By theorem $\mathcal{J}(G) \approx G/Z$.

Hence completes the proof.

Lemma: Let G be a group and ϕ an automorphism of G. If $a \in G$ is of order $o(a) > 0$ then $o(\phi(a)) = o(a)$.

Proof: Suppose that ϕ is an automorphisms of a group G and suppose that $a \in G$ has order n (ie) ($a^n = e$ but for no lower positive power).

Then $\phi(a)^n = \phi(a^n) = \phi(e) = e$, hence $\phi(a^n) = e$.

If $\phi(a)^m = e$ for some $0 < m < n$, then $\phi(a^m) = \phi(a)^m = e$, which implies, since ϕ is one-to-one, that $a^m = e$, a contradiction.

Hence the proof.

CAYLEY'S THEOREM

Theorem: Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.

Proof: Let G be a group. For the set S we will use the elements of G; (ie) put $S = G$.
If $g \in G$, define $\tau_g : S(=G) \to S(=G)$ by $x\tau_g = xg$ for every $x \in G$. If $y \in G$, then $y = (yg^{-1})g = (yg^{-1})\tau_g$. So that τ_g maps S onto itself. Moreover, τ_g is one-to-one, for if $x, y \in S$ and $x\tau_g = y\tau_g$ then $xg = yg$, which, by the cancellation property of groups, implies that $x = y$. We have proved that for every $g \in G$, $\tau_g \in A(S)$.

If $g, h \in G$, consider τ_{gh}. For any $x \in S = G$. $x\tau_{gh} = x(gh) = (xg)h = (x\tau_g)\tau_h = x\tau_g\tau_h$

From $x\tau_{gh} = x\tau_g\tau_h$ we deduce that $\tau_{gh} = \tau_g\tau_h$. Therefore, if $\psi : G \to A(S)$ is defined by $\psi(g) = \tau_g$, the relation $\tau_{gh} = \tau_g\tau_h$ tells us that ψ is a homomorphism.

If $g_0 \in K$, then $\psi(g_0) = \tau_{g_0}$ is the identity map on S, so that for $x \in G$, and, in particular, for $e \in G$, $e\tau_{g_0} = e$. But $e\tau_{g_0} = eg_0 = g_0$.

Thus comparing these two expressions for $e\tau_{g_0}$ we conclude that $g_0 = e$, whence $K = (e)$. Thus ψ is an isomorphism of G into $A(S)$.

Hence the proof.

Theorem: If G is a group, H be a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism θ of G into $A(S)$ and the kernel of θ is the largest normal subgroup of G which is contained in H.

Proof: Let G be a group, H be a subgroup of G. Let S be the set whose elements are the right cosets of H in G. That is, $S = \{Hg \mid g \in G\}$. S need not be a group itself, in fact, it would be a group only if H were a normal subgroup of G.

However, we can make our group G act on S in the following natural way: for $g \in G$. Let $t_g : S \to S$ be defined by $(Hx)t_g = Hxg$.

Next we prove (1) $t_g \in A(S)$ for every $g \in G$ (2) $t_{gh} = t_g t_h$

Thus the mapping $\theta : G \to A(S)$ defined by $\theta(g) = t_g$ is a homomorphism of G into $A(S)$.
Suppose that K is the kernel of θ. If $g_0 \in K$, then $\theta(g_0) = t_{g_0}$ is the identity map on S, so that for every $X \in S$, $Xt_{g_0} = X$.

Since every element of S is a right coset of H in G, we must have that $Hat_{g_0} = Ha$ for every $a \in G$, and using the definition of t_{g_0}, namely, $Hat_{g_0} = Hag_0$, we arrive at the identity $Hag_0 = Ha$ for every $a \in G$.

On the other hand, if $b \in G$ is such that $Hxb = Hx$ for every $x \in G$, retracing our argument we could show that $b \in K$. Thus $K = \{b \in G \mid Hxb = Hx \text{ all } x \in G\}$.
We claim that, K must be the largest normal subgroup of G which is contained in H.

We first explain the use of the word largest; by this we mean that if N is a normal subgroup of G which is contained in H, then N must be contained in K.

Decompose G into double ...
we wish to show this is the case. That K is a normal subgroup of G follows from the fact that it is the kernel of a homomorphism of G. Now we assert that $K \subset H$, for if $b \in K$, $Hab = Ha$ for every $a \in G$, so, in particular, $Hb = Heb = He = H$, whence $b \in H$.

Finally, if N is a normal subgroup of G which is contained in H, if $n \in N$, $a \in G$, then $ana^{-1} \in N \subset H$, so that $Hana^{-1} = H$, thus $Han = Ha$ for all $a \in G$. Therefore, $n \in K$ by our characterization of K.

Hence the proof

Lemma: If G is a finite group, and $H \neq G$ is a subgroup of G such that $o(G) \nmid i(H)!$ then H must contain a nontrivial normal subgroup of G. In particular, G cannot be simple.

Proof: Suppose that G has a subgroup H whose index $i(H)$ ((ie) the number of right cosets of H in G) satisfies $i(H)! < o(G)$. Let S be the set of all right cosets of H in G. The mapping, θ, of previous theorem cannot be an isomorphism, for if it were, $\theta(G)$ would have $o(G)$ elements and yet would be a subgroup of $A(S)$ which has $i(H)! < o(G)$ elements.

Therefore the kernel of θ must be larger than (e); this kernel being the largest normal subgroup of G which is contained in H, we can conclude that H contains a nontrivial normal subgroup of G.

However, the argument used above has implications even when $i(H)!$ is not less than $o(G)$. If $o(G)$ does not divide $i(H)!$ then by invoking Lagrange's theorem we know that $A(S)$ can have no subgroup of order $o(G)$, hence no subgroup isomorphic to G. However, $A(S)$ does contain $\theta(G)$, whence $\theta(G)$ cannot be isomorphic to G, (ie) θ cannot be an isomorphism. But then, as above, H must contain a nontrivial normal subgroup of G.

Hence the lemma.

PERMUTATION GROUPS:

Definition: Let A be a finite set. A bijection from A to itself is called a permutation of A.

Example: If $A = \{1,2,3,4\}$, $f : A \to A$ given by $f(1)=2$, $f(2)=1$, $f(3)=4$ and $f(4)=3$ is a permutation of A. We shall write this permutation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

An element in the bottom row is the image of the element just above it in the upper row.

Definition: Let A be a finite set containing n elements. The set of all permutations of A is clearly a group under the composition of functions. This group is called the symmetric group of degree n and is denoted by S_n.

Example: Let $A = \{1,2,3\}$. Then S_3 consist of $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. In this group, e is the identity element. We now compute the product $p_1 p_2$.

$$p_1 p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

and $p_1 p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = p_5$.

...larly we can compute all the other products and the cayley table for this group is given by

	e	p_1	p_2	p_3	p_4	p_5
e	e	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	e	p_4	p_5	p_3
p_2	p_2	e	p_1	p_5	p_3	p_4
p_3	p_3	p_5	p_4	e	p_2	p_1
p_4	p_4	p_3	p_5	p_1	e	p_2
p_5	p_5	p_4	p_3	p_2	p_1	e

Thus S_3 is a group containing $3! = 6$ elements.

Definition: Let G be a finite group. Then the number of elements in G is called the order of G and is denoted by $|G|$ or $o(G)$.

Lemma: Every permutation is the product of its cycles.

Proof: Given the permutation $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$

Next we find the cycles of θ. First find the orbit of 1;
namely, 1, $1\theta = 2$, $1\theta^2 = 2\theta = 3$, $1\theta^3 = 3\theta = 8$, $1\theta^4 = 8\theta = 5$, $1\theta^5 = 5\theta = 6$,
$1\theta^6 = 6\theta = 4$, $1\theta^7 = 4\theta = 1$. (ie) the orbit of 1 is the set $\{1,2,3,8,5,6,4\}$.
The orbits of 7 and 9 can be found to be $\{7\}$, $\{9\}$ respectively. The cycles of θ thus are (7), (9), $(1, 1\theta, 1\theta^2, \ldots 1\theta^6) = (1,2,3,8,5,6,4)$

The product of $(1,2,3,8,5,6,4)$, (7), (9) is θ.
(ie) atleast in this case, θ is the product of its cycles.

Hence the Lemma

Lemma: Every permutation is a product of 2-cycles.

Proof: Let θ be the permutation. Then its cycles are of the form $(s, s\theta, \ldots s\theta^{l-1})$. By the multiplication of cycles, as defined above, and since the cycles of θ are disjoint, the image of $s' \in S$ under θ, which is $s'\theta$, is the same as the image of s' under the Product, ψ, of all the distinct cycles of θ. So θ, ψ have the same effect on every element of S, hence $\theta = \psi$.

Consider the m-cycle $(1,2,\ldots m)$. A simple computation shows that $(1,2,\ldots m) = (1,2)(1,3)\ldots(1,m)$. More generally the m-cycle $(a_1,a_2\ldots a_m) = (a_1,a_2)(a_1,a_3)\ldots(a_1,a_m)$.
This decomposition is not unique, by this we mean that an m-cycle can be written as a product of 2-cycles in more than one way.

For instance $(1,2,3) = (1,2)(1,3) = (3,1)(3,2)$.

Now, since every permutation is a product of disjoint cycles and every cycle is a product of 2-cycles, we have proved.

Definition: A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transpositions.

Lemma: S_n has as a normal subgroup of index 2 the alternating group A_n, consisting of all even permutations.

Proof: Let A_n be the subset of S_n consisting of all even permutations. Since the product of two even permutations is even, A_n must be a subgroup of S_n. We claim it is normal in S_n. Perhaps the best way of seeing this is as follows:

Let W be the group of real numbers 1 and -1 under multiplication. Define $\psi : S_n \to W$ by $\psi(s) = 1$ if s is an even permutation, $\psi(s) = -1$ if s is an odd permutation. By the rules 1,2,3 above ψ is a homomorphism onto W.

The Kernel of ψ is precisely A_n; being the Kernel of a homomorphism A_n is a normal subgroup of S_n. By theorem $S_n/A_n \simeq W$, so, since

$$2 = o(W) = o\left(\frac{S_n}{A_n}\right) = \frac{o(S_n)}{o(A_n)}$$

We see that $o(A_n) = \frac{1}{2} n!$. A_n is called the alternating group of degree n.

ANOTHER COUNTING PRINCIPLE

Definition: If $a, b \in G$, then b is said to be a conjugate of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$.

Lemma: Conjugacy is an equivalence relation on G.

Proof: We must prove that ① $a \sim a$ ② $a \sim b$ implies that $b \sim a$ ③ $a \sim b$, $b \sim c$ implies that $a \sim c$ for all a, b, c in G

1. Since $a = e^{-1}ae$, $a \sim a$, with $c = e$ serving as the c in the definition of conjugacy.
2. If $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$, hence, $a = (x^{-1})^{-1} b (x^{-1})$, and since $y = x^{-1} \in G$ and $a = y^{-1}by$, $b \sim a$ follows.
3. Suppose that $a \sim b$ and $b \sim c$ where $a, b, c \in G$. Then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$, Since $xy \in G$, $a \sim c$ is a consequence.

Defn: For $a \in G$, let $C(a) = \{x \in G \mid a \sim x\}$. $C(a)$, the equivalence class of a in G under our relation, is usually called the conjugate class of a in G, it consists of the set of all distinct elements of the form $y^{-1}ay$ as y ranges over G.

Definition: If $a \in G$, then $N(a)$, the normalizer of a in G, is the set $N(a) = \{x \in G \mid xa = ax\}$

$N(a)$ consists of precisely those elements in G which commute with a.

Lemma $N(a)$ is a subgroup of G

Proof: Suppose that $x, y \in N(a)$. Thus $xa = ax$ and $ya = ay$ Therefore,
$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$ in consequence of which $xy \in N(a)$

From $ax = xa$ it follows that $x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$, so that x^{-1} is also in $N(a)$. But then $N(a)$ has been demonstrated to be a subgroup of G.

Theorem: If G is a finite group, then $c_a = o(G) | o(N(a))$, in otherwords, the number of elements conjugate to a in G is the index of the normalizer of a in G.

Proof: Suppose that $x, y \in G$ are in the same right coset of $N(a)$ in G. Thus $y = nx$, where $n \in N(a)$, and so $na = an$. Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}n^{-1}nax = x^{-1}ax$, whence x and y result in the same conjugate of a.

If, on the other hand, x and y are in different right cosets of $N(a)$ in G we claim that $x^{-1}ax \neq y^{-1}ay$. Were this not the case, from $x^{-1}ax = y^{-1}ay$ we would deduce that $yx^{-1}a = ayx^{-1}$, this in turn would imply that $yx^{-1} \in N(a)$.

However, this declares x and y to be in the same right coset of $N(a)$ in G, contradicting the fact that they are in different cosets.

Hence the proof.

Corollary: $o(G) = \sum o(G) | o(N(a))$
where this sum runs over on element a in each conjugate class.

Proof: Since $o(G) = \sum c_a$ using the theorem the corollary becomes immediate.

SUBLEMMA: $a \in Z$ if and only if $N(a) = G$. If G is finite, $a \in Z$ if and only if $o(N(a)) = o(G)$.

Proof: If $a \in Z$, $xa = ax$ for all $x \in G$, whence $N(a) = G$. If conversely, $N(a) = G$, $xa = ax$ for all $x \in G$, so that $a \in Z$. If G is finite, $o(N(a)) = o(G)$ is equivalent to $N(a) = G$.

Theorem If $o(G) = p^n$ where p is a prime number, then $Z(G) \neq (e)$.

Proof: If $a \in G$, since $N(a)$ is a subgroup of G, $o(N(a))$, being a divisor of $o(G) = p^n$, must be of the form $o(N(a)) = p^{n_a}$; $a \in Z(G)$ if and only if $n_a = n$.

Write out the class equation for this G, letting $z = o(Z(G))$. we get $p^n = o(G) = \sum (p^n | p^{n_a})$, however, since there are exactly z elements such that $n_a = n$, we find that

$$p^n = z + \sum_{n_a < n} \frac{p^n}{p^{n_a}}.$$

Now look at this! p is a divisor of the left-hand side, since $n_a < n$ for each term in the $\sum$ of the right side,

$$p \,\Big|\, \frac{p^n}{p^{n_a}} = p^{n - n_a}$$

So that p is a divisor of each term of this sum, hence a divisor of this sum

Therefore, $$p \,\Big|\, \Big(p^n - \sum_{n_a < n} \frac{p^n}{p^{n_a}}\Big) = z.$$

Since $e \in Z(G)$, $z \neq 0$, thus z is a positive integer divisible by the prime p, $z > 1$. But then there must be an element, besides e, in $Z(G)$!

Hence the proof

Corollary: If $o(G) = p^2$ where p is a prime number, then G is abelian

Proof: Our aim is to show that $Z(G) = G$. We already know that $Z(G) \neq (e)$ is a subgroup of G so that $o(Z(G)) = p$ (or) p^2

If $o(Z(G)) = p^2$, then $Z(G) = G$ and we are done. Suppose that $o(Z(G)) = p$

Let $a \in G$, $a \notin Z(G)$. Thus $N(a)$ is a subgroup of G, $Z(G) \subset N(a)$, $a \in N(a)$.

So that $o(N(a)) > p$, yet by Lagrange's theorem $o(N(a)) \mid o(G) = p^2$

The only way out is for $o(N(a)) = p^2$, implying that $a \in Z(G)$, a contradiction. Thus $o(Z(G)) = p$ is not an actual possibility

Hence the proof

Theorem (cauchy): If p is a prime number and $p \mid o(G)$, then G has an element of order p

Proof: we seek an element $a \neq e \in G$ satisfying $a^p = e$

To prove its existence we proceed by induction on $o(G)$. (ie) we assume the theorem to be true for all groups T such that $o(T) < o(G)$.

We need not worry about starting the induction for the result true for groups of order 1.

If for any subgroup W of G, $W \neq G$, were it to happen, that $p \mid o(W)$, then by our induction hypothesis there would exist an element of order p in W, and thus there would be such an element in G. Thus we may assume that p is not a divisor of the order of any proper subgroup of G

In particular, if $a \notin Z(G)$, since $N(a) \neq G$, $p \nmid o(N(a))$.

Let us write down the class equation $o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$

Since $p \mid o(G)$, $p \nmid o(N(a))$ we have that $p \mid \frac{o(G)}{o(N(a))}$ and so $p \mid \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$

Since we also have that $p \mid o(G)$, we conclude that

$$p \mid \left(o(G) - \sum_{N(a) \neq G} o(G) / o(N(a))\right) = o(Z(G))$$

$Z(G)$ is thus a subgroup of G whose order is divisible by p. But after all we have assumed that p is not a divisor of the order of any proper subgroup of G, so that $Z(G)$ cannot be a proper subgroup of G

We are forced to accept the only possibility left us, namely, that $Z(G) = G$. But then G is abelian now we invoke the result already established for abelian groups to complete the induction

Hence the proof

Theorem (SYLOW) If p is a prime number and $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.

Proof: The number of ways of picking a subset of k elements from a set of n elements can easily be shown to be $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$

If $n = p^\alpha m$ where p is a prime number, and if $p^r \mid m$ but $p^{r+1} \nmid m$, consider

$$\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)!}{(p^\alpha)!\,(p^\alpha m - p^\alpha)!} = \frac{p^\alpha m\,(p^\alpha m-1)\cdots(p^\alpha m - i)\cdots(p^\alpha m - p^\alpha + 1)}{p^\alpha (p^\alpha - 1)\cdots(p^\alpha - i)\cdots(p^\alpha - p^\alpha + 1)}$$

The power of p dividing $(p^\alpha m - i)$ is the same as that dividing $p^\alpha - i$, so all powers of p cancel out except the power which divides m. Thus

$$p^r \,\Big|\, \binom{p^\alpha m}{p^\alpha} \quad \text{but} \quad p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$$

First proof of the theorem

Let $\mathcal{M}$ be the set of all subsets of G which have p^α elements. Thus $\mathcal{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements. Given $M_1, M_2 \in \mathcal{M}$ (M is a subset of G having p^α elements and likewise so is M_2), define $M_1 \sim M_2$ if there exists an element $g \in G$ such that $M_1 = M_2 g$. It is immediate to verify that this defines an equivalence relation on $\mathcal{M}$. We claim that there is atleast one equivalence class of elements in $\mathcal{M}$ such that the number of elements in this class is not a multiple of p^{r+1}, for if p^{r+1} is a divisor of the size of each equivalence class, then p^{r+1} would be a divisor of the number of elements in $\mathcal{M}$. Since $\mathcal{M}$ has $\binom{p^\alpha m}{p^\alpha}$ elements and $p^{r+1} \nmid \binom{p^\alpha m}{p^\alpha}$, this cannot be the case.

Let $\{M_1, M_2 \cdots M_n\}$ be such an equivalence class in $\mathcal{M}$ where $p^{r+1} \nmid n$. By our very definition of equivalence in $\mathcal{M}$, if $g \in G$, for each $i = 1, 2, \cdots n$, $M_i g = M_j$ for some j, $1 \leq j \leq n$.

We let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a subgroup of G, for if $a, b \in H$, then $M_1 a = M_1$, $M_1 b = M_1$ whence $M_1 ab = (M_1 a)b = M_1 b = M_1$.

We shall be vitally concerned with $o(H)$.

We claim that $(n\,o(H)) = o(G)$. We leave the proof to the reader, but suggest the argument used in the counting principle.

Now $n\,o(H) = o(G) = p^\alpha m$. Since $p^{r+1} \nmid n$ and $p^{\alpha+r} \mid p^\alpha m = n\,o(H)$, it must follow that $p^\alpha \mid o(H)$, and so $o(H) \geq p^\alpha$. However, M_1 was a subset of G containing p^α elements. Thus $p^\alpha \geq o(H)$. Combined with $o(H) \geq p^\alpha$ we have that $o(H) = p^\alpha$. But then we have exhibited a subgroup of G having exactly p^α elements, namely H. Hence the proof.

Corollary: If $p^m / o(G)$, $p^{m+1} \nmid o(G)$, then G has a subgroups of order p^m

Proof: A subgroup of G of order p^m, where $p^m / o(G)$ but $p^{m+1} \nmid o(G)$ is called a p-sylow subgroup of G.

Second proof of sylow's Theorem

We prove, by induction on the order of the group G, that for every prime p dividing the order of G, G has a p-sylow subgroup

If the order of the group is 2, the only relevant prime is 2 and the group certainly has a subgroup of order 2, namely itself

So we suppose the result to be correct for all groups of order less than $o(G)$. From this we want to show that the result is valid for G. Suppose, then that $p^m | o(G)$, $p^{m+1} \nmid o(G)$, where p is a prime, $m \geq 1$. If $p^m | o(H)$ for any subgroup H of G, where $H \neq G$, then by the induction hypothesis, H would have a subgroup T of order p^m. However, since T is a subgroup of H, and H is a subgroup of G, T too is a subgroup of G. But then T would be the sought-after subgroup of order p^m.

We therefore may assume that $p^m \nmid o(H)$ for any subgroup H of G, where $H \neq G$. Recall that if $a \in G$ then $N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G, moreover, if $a \notin Z$, the center of G, then $N(a) \neq G$.

The class equation of G states that $o(G) = \sum \frac{o(G)}{o(N(a))}$

Where this sum runs over one element a from each conjugate class. We separate this sum into two pieces, those a which lie in Z, and those which don't. This gives $o(G) = z + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$ where $z = o(Z)$.

Now invoke the reduction we have made, namely, that $p^m \nmid o(H)$ for any subgroup $H \neq G$ of G, to those subgroups $N(a)$ for $a \notin Z$.

Since in this case, $p^m | o(G)$ and $p^m \nmid o(N(a))$, we must have that $p \,\Big|\, \frac{o(G)}{o(N(a))}$ Restating this result $p \,\Big|\, \frac{o(G)}{o(N(a))}$. for every $a \in G$ where $a \notin Z$.

Look at the class equation with this information in hand. Since $p^m | o(G)$, we have that $p | o(G)$, also $p \,\Big|\, \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$

Thus the class equation gives us that $p | z$. Since $p | z = o(Z)$, by cauchy's thm. Z has an element $b \neq e$ of order p. Let $B = (b)$, the subgroup of G generated by b. B is of order p, moreover, since $b \in Z$, B must be normal in G.

Hence we can form the quotient group $\bar{G} = G/B$ whose order is $\bar{G}$. First of all, its order is $o(G)/o(B) = o(G)/p$, hence is certainly less than $o(G)$.
Secondly, we have $p^{m-1} \mid o(\bar{G})$, but $p^m \nmid o(\bar{G})$. Thus by the induction hypothesis, $\bar{G}$ has a subgroup $\bar{P}$ of order p^{m-1}.

Let $P = \{x \in G \mid xB \in \bar{P}\}$. P is a subgroup of G. Moreover, $\bar{P} \cong P/B$.

Thus $p^{m-1} = o(\bar{P}) = o(P)/o(B) = \dfrac{o(P)}{p}$

This results in $o(P) = p^m$. Therefore P is the required p-Sylow subgroup of G.

Hence completes the proof

__Third proof of Sylow's theorem:__

We will first show that the symmetric groups S_{p^r}, p be a prime, all have p-Sylow subgroups. The next step will be to show that if G is contained in M and M has a p-Sylow subgroup, then G has a p-Sylow subgroup.

Finally we will show, via Cayley's theorem, that we can use S_{p^k}, for large enough k, as our M. With this we will have all the pieces and the theorem will drop out.

We will have to know how large a p-Sylow subgroup of S_{p^r} should be. This will necessitate knowing what power of p divides $(p^r)!$. This will be easy. To produce the p-Sylow subgroup of S_{p^r} will be harder.

So we get down to our first task, that of finding what power of a prime p exactly divides $(p^k)!$. Actually, it is quite easy to do this for $n!$ for any integer n. But, for our purposes, it will be clearer and will suffice to do it only for $(p^k)!$. Let $n(k)$ be defined by $p^{n(k)} \mid (p^k)!$ but $p^{n(k)+1} \nmid (p^k)!$

Lemma: $n(k) = 1 + p + p^2 + \cdots + p^{k-1}$

Proof: If $k = 1$ then, since $p! = 1 \cdot 2 \cdot 3 \cdots (p-1)p$, it is clear that $p \mid p!$ but $p^2 \nmid p!$. Hence $n(1) = 1$, as it should be.

Clearly, only the multiples of p in the expansion of $(p^k)!$ (i.e.) $p, 2p, \ldots p^{k-1}p$ which divides $p(2p)(3p)\cdots(p^{k-1}p) =$ $p^{p^{k-1}}(p^{k-1})!$. In other words $n(k)$ must be the power of p which divides $p^{p^{k-1}}(p^{k-1})!$. But then $n(k) = p^{k-1} + n(k-1)$.

Similarly, $n(k-1) = n(k-2) + p^{k-2}$, and so on.

Write these out as

$$n(k) - n(k-1) = p^{k-1}$$
$$n(k-1) - n(k-2) = p^{k-2}$$
$$\vdots$$
$$n(2) - n(1) = p,$$
$$n(1) = 1.$$

Adding these up, with the cross cancellation that we get, we obtain
$n(k) = 1 + p + p^2 + \cdots + p^{k-1}$

Lemma S_{p^k} has a p-Sylow subgroup

Proof We go by induction on k. If $k=1$, then the element $(1,2,\ldots,p)$, in S_p is of order p, so generated a subgroup of order p. Since $n(1)=1$, the result certainly checks out for $k=1$.

Suppose that the result is correct for $k-1$, we want to show that it then must follow for k. Divide the integers $1,2,\ldots p^k$ into p clumps, each with p^{k-1} elements as follows:

$\{1,2 \ldots p^{k-1}\}, \{p^{k-1}+1, p^{k-1}+2, \ldots 2p^{k-1}\}, \ldots \{(p-1)p^{k-1}+1, \ldots p^k\}$.

The permutation σ defined by $\sigma = (1, p^{k-1}+1, 2p^{k-1}+1, \ldots (p-1)p^{k-1}+1) \cdots (j, p^{k-1}+j, 2p^{k-1}+j, \ldots (p-1)p^{k-1}+1+j) \cdots (p^{k-1}, 2p^{k-1}, \ldots (p-1)p^{k-1}, p^k)$ has the following properties.

1. $\sigma^p = e$. 2. If τ is a permutation that leaves all i fixed for $i > p^{k-1}$ (hence, affects only $1,2,\ldots p^{k-1}$), then $\sigma^{-1}\tau\sigma$ moves only elements in $\{p^{k-1}+1, p^{k-1}+2, \ldots 2p^{k-1}\}$ and more generally, $\sigma^{-j}\tau\sigma^{j}$ moves only elements in $\{jp^{k-1}+1, jp^{k-1}+2, \ldots (j+1)p^{k-1}\}$.

Consider $A = \{\tau \in S_{p^k} \mid \tau(i) = i \text{ if } i > p^{k-1}\}$. A is a subgroup of S_{p^k} and elements in A can carry out any permutation on $1,2,\ldots p^{k-1}$. From this it follows easily that $A \approx S_{p^{k-1}}$. By induction, A has a subgroup P_1 of order $p^{n(k-1)}$.

Let $T = P_1(\sigma^{-1}P_1\sigma)(\sigma^{-2}P_1\sigma^{-2}) \cdots (\sigma^{-1(p-1)}P_1\sigma^{p-1}) = P_1P_2 \cdots P_{n-1}$.
where $P_i = \sigma^{-i}P_1\sigma^{-i}$. Each P_i is isomorphic to P_1 so has order $p^{n(k-1)}$. Also elements in distinct P_i's influence nonoverlapping sets of integers, hence commute. Thus T is a subgroup of S_{p^k}.

Since $P_i \cap P_j = (e)$ if $0 \le i \ne j \le p-1$, we see that $o(T) = o(P_1)^p = p^{p\,n(k-1)}$
We are not quite there yet. T is not the p-Sylow subgroup.

Since $\sigma^p = e$ and $\sigma^{-i}P_1\sigma^{i} = P_i$ we have $\sigma^{-1}T\sigma = T$. Let $P = \{\sigma^{j}t \mid t \in T, 0 \le j \le p-1\}$. Since $\sigma \notin T$ and $\sigma^{-1}T\sigma = T$ we have two things, firstly, T is a subgroup of S_{p^k} and, furthermore, $o(P) = p \cdot o(T) = p \cdot p^{n(k-1)p} = p^{n(k-1)p+1}$

Now we are finally there, P is the sought-after p-Sylow subgroup of S_{p^k}.

Definition: Let G be a group, A, B subgroups of G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$, $b \in B$.

The relation defined above is an equivalence relation on G. The equivalence class of $x \in G$ is the set $AxB = \{axb \mid a \in A, b \in B\}$. Here the set AxB is a **double coset** of A, B in G.

Lemma: If A, B are finite subgroups of G, then $o(AxB) = \dfrac{o(A)\,o(B)}{o(A \cap xBx^{-1})}$

Proof: If A, B are finite subgroups of G,

To begin with, the mapping $T : AxB \to AxBx^{-1}$ given by $(axb)T = axbx^{-1}$ is one-to-one and onto (verify).

Thus $o(AxB) = o(AxBx^{-1})$. Since xBx^{-1} is a subgroup of G, of order $o(B)$ by the theorem

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)\,o(xBx^{-1})}{o(A \cap xBx^{-1})} = \frac{o(A)\,o(B)}{o(A \cap xBx^{-1})}$$

Lemma: Let G be a finite group and suppose that G is a subgroup of the finite group M. Suppose further that M has a p-Sylow subgroup Q. Then G has a p-Sylow subgroup P. In fact, $P = G \cap xQx^{-1}$ for some $x \in M$.

Proof: Suppose that $p^m \mid o(M)$, $p^{m+1} \nmid o(M)$, Q is a subgroup of M of order p^m. Let $o(G) = p^n t$ where $p \nmid t$. We want to produce a subgroup P in G of order p^n.

Consider the double coset decomposition of M given by G and Q, $M = \bigcup GxQ$

By Lemma $\quad o(GxQ) = \dfrac{o(G)\,o(Q)}{o(G \cap xQx^{-1})} = \dfrac{p^n t\, p^m}{o(G \cap xQx^{-1})}$

Since $G \cap xQx^{-1}$ is a subgroup of xQx^{-1}, its order is p^{m_x}. We claim that $m_x = n$ for some $x \in M$. If not, then $o(GxQ) = \dfrac{p^n t\, p^m}{p^{m_x}} = t p^{m+n-m_x}$

So is divisible by p^{m+1}. Now, since $M = \bigcup GxQ$, and this is disjoint union, $o(M) = \sum o(GxQ)$, the sum running over one element from each double coset. But $p^{m+1} \mid o(GxQ)$, hence $p^{m+1} \mid o(M)$. This contradicts $p^{m+1} \nmid o(M)$. Thus $m_x = n$ for some $x \in M$.

But then $o(G \cap xQx^{-1}) = p^n$. Since $G \cap xQx^{-1} = P$ is a subgroup of G and has order p^n. Hence the lemma.

Theorem (Second part of Sylow's theorem)

If G is a finite group, p be a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$ then any two subgroups of G of order p^n are conjugate.

Proof: Let A, B be subgroups of G, each of order p^n. We want to show that $A = gBg^{-1}$ for some $g \in G$

Decompose G into double cosets of A and B. $G = \bigcup AxB$. Now by Lemma

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

If $A \neq xBx^{-1}$ for every $x \in G$ then $o(A \cap xBx^{-1}) = p^m$ where $m < n$.

Thus $o(AxB) = \frac{o(A)o(B)}{p^m} = \frac{p^{2n}}{p^m} = p^{2n-m}$ and $2n - m \geq n+1$. Since $p^{n+1} \mid o(AxB)$ for every x and since $o(G) = \sum o(AxB)$, we would get the contradiction $p^{n+1} \mid o(G)$.

Thus $A = gBg^{-1}$ for some $g \in G$.

Hence the proof.

Lemma: The number of p-Sylow subgroups in G equals $o(G)/o(N(P))$, where P is any p-Sylow subgroup of G. In particular, this number is a divisor of $o(G)$

Theorem (THIRD PART OF SYLOW'S THEOREM)

The numbers of p-sylow subgroups in G, for a given prime, is of the form $1+kp$.

Proof: Let P be a p-sylow subgroup of G. We decompose G into double cosets of P and P. Thus $G = \bigcup PxP$.

$$o(PxP) = \frac{o(P)^2}{o(P \cap xPx^{-1})}.$$

Thus, if $P \cap xPx^{-1} \neq P$ then $p^{n+1} \mid o(PxP)$, where $p^n = o(P)$. paraphrasing this: if $x \notin N(P)$ then $p^{n+1} \mid o(PxP)$. Also, if $x \in N(P)$, then $PxP = P(Px) = P^2x = Px$, so $o(PxP) = p^n$ in this case.

$$\text{Now} \quad o(G) = \sum_{x \in N(P)} o(PxP) + \sum_{x \notin N(P)} o(PxP)$$

where each sum runs over one element from each double coset. However, if $x \in N(P)$ since $PxP = Px$, the first sum is merely $\sum_{x \in N(P)} o(Px)$ over the distinct cosets of P in $N(P)$. Thus this first sum is just $o(N(P))$.

we saw that each of its constituent terms is divisible by p^{n+1}, hence $p^{n+1} \mid \sum_{x \notin N(P)} o(PxP)$. we can thus write this second sum as $\sum_{x \notin N(P)} o(PxP) = p^{n+1}u$.

Therefore $o(G) = o(N(P)) + p^{n+1}u$, so $\frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}u}{o(N(P))}$

Now $o(N(P)) \mid o(G)$ since $N(P)$ is a subgroup of G, hence $p^{n+1}u / o(N(P))$ is an integer. Also, since $p^{n+1} \nmid o(G)$, p^{n+1} can't divide $o(N(P))$. But then $p^{n+1}u / o(N(P))$ must be divisible by p, so we can write $p^{n+1}u / o(N(P))$ as kp, where k is an integer.

$$o(G) / o(N(P)) = 1 + kp.$$

Hence the proof.

UNIT III

HOMOMORPHISMS

Definition: A mapping ϕ from the ring R into the ring R' is said to be a homomorphism if (1) $\phi(a+b)=\phi(a)+\phi(b)$, (2) $\phi(ab)=\phi(a)\phi(b)$ for all $a,b\in R$

Lemma: If ϕ is a homomorphism of R into R' then (1) $\phi(0)=0$, (2) $\phi(-a)=-\phi(a)$ for every $a\in R$

~~Proof: Since ϕ is a homomorphism of the Ring R into R'~~

Definition: If ϕ is a homomorphism of R into R' then the Kernel of ϕ, $I(\phi)$, is the set of all elements $a\in R$ such that $\phi(a)=0$, the zero-element of R'.

Lemma: If ϕ is a homomorphism of R into R' with Kernel $I(\phi)$, then (1) $I(\phi)$ is a subgroup of R under addition (2) If $a\in I(\phi)$ and $r\in R$ then both ar and ra are in $I(\phi)$.

Proof: Since ϕ is, in particular, a homomorphism of R, as an additive group, into R' as an additive group, (1) follows directly from our results in group theory.

To see (2), Suppose that $a\in I(\phi)$, $r\in R$. Then $\phi(a)=0$ so that $\phi(ar)=\phi(a)\phi(r) = 0\phi(r)=0$ by lemma. Similarly $\phi(ra)=0$. Thus by defining property of $I(\phi)$ both ar and ra are in $I(\phi)$.

Definition: A homomorphism of R into R' is said to be an isomorphism if it is a one-to-one mapping.

Definition: Two rings are said to be isomorphic if there is an isomorphism of one onto the other.

Lemma The homomorphism ϕ of R into R' is an isomorphism if and only if $I(\phi)=(0)$

IDEALS AND QUOTIENT RINGS

Definition: A nonempty subset U of R is said to be a (two-sided) ideal of R if (1) U is a subgroup of R under addition (2) For every $u\in U$ and $r\in R$, both ur and ru are in U.

Lemma: If U is an ideal of the ring R, then R/U is a ring and is a homomorphic image of R.

Proof: Given an ideal U of a ring R, let R/U be the set of all the distinct cosets of U in R which we obtain by considering U as a subgroup of R under addition. Since R is an abelian group under addition.

To restate what we have just said, R/U consists of all the cosets, $a+U$, where $a\in R$. R/U is automatically a group under addition this is achieved by the composition law $(a+U)+(b+U)=(a+b)+U$. In order to impose a ring structure on R/U we must define, in it, a multiplication. However, we must make sure that this is meaningful.

Otherwise put, we are obliged to show that if $a+U=a'+U$ and $b+U=b'+U$ then under our definition of the multiplication, $(a+U)(b+U)=(a'+U)(b'+U)$

Equivalently, it must be established that $ab+U = a'b'+U$

To this end we first note that since $a+U = a'+U$, $a = a'+u_1$, where $u_1 \in U$. Similarly $b = b'+u_2$ where $u_2 \in U$. Thus $ab = (a'+u_1)(b'+u_2) = a'b' + u_1b' + a'u_2 + u_1u_2$. Since U is an ideal of R, $u_1b' \in U$, $a'u_2 \in U$ and $u_1u_2 \in U$.

Consequently $u_1b' + a'u_2 + u_1u_2 = u_3 \in U$. But then $ab = a'b' + u_3$ from which we deduce that $ab + U = a'b' + u_3 + U$, and since $u_3 \in U$, $u_3 + U = U$. The net consequence of all this is that $ab + U = a'b' + U$.

If $X = a+U$, $Y = b+U$, $Z = c+U$ are three elements of R/U where $a, b, c \in R$ then $(X+Y)Z = ((a+U)+(b+U))(c+U) = ((a+b)+U)(c+U) = (a+b)c + U = ac+bc+U$ $= (ac+U)+(bc+U) = (a+U)(c+U) + (b+U)(c+U) = XZ + YZ$.

R/U has now been made into a ring. Clearly, if R is commutative then so is R/U, for $(a+U)(b+U) = ab+U = ba+U = (b+U)(a+U)$. If R has a unit element 1, then R/U has a unit element $1+U$. There is a homomorphism ϕ of R onto R/U given by $\phi(a) = a+U$ for every $a \in R$, whose kernel is exactly U.

Theorem: Let R, R' be rings and ϕ be a homomorphism of R onto R' with kernel U. Then R' is isomorphic to R/U. Moreover there is a one-to-one correspondence between the set of ideals of R' and the set of ideals of R which contain U. This correspondence can be achieved by associating with an ideal W' in R' the ideal W in R defined by $W = \{x \in R \mid \phi(x) \in W'\}$. With W so defined, R/W is isomorphic to R'/W'.

MORE IDEALS AND QUOTIENT RINGS

Lemma: Let R be a commutative ring with unit element whose only ideals are (0) and R itself. Then R is a field.

Proof: In order to effect a proof of this lemma for any $a \neq 0 \in R$ we must produce an element $b \neq 0 \in R$ such that $ab = 1$.

So, suppose that $a \neq 0$ is in R. Consider the set $Ra = \{xa \mid x \in R\}$. We claim that Ra is an ideal of R. In order to establish this as fact we must show that it is a subgroup of R under addition and that if $u \in Ra$ and $r \in R$ then ru is also in Ra.

Now, if $u, v \in Ra$, then $u = r_1a$, $v = r_2a$ for some $r_1, r_2 \in R$. Thus $u+v = r_1a + r_2a = (r_1+r_2)a \in Ra$; similarly $-u = -r_1a = (-r_1)a \in Ra$. Hence Ra is an additive subgroup of R. Moreover, if $r \in R$, $ru = r(r_1a) = (rr_1)a \in Ra$.

Ra therefore satisfies all the defining conditions for an ideal of R, hence is an ideal of R. By our assumptions on R, $Ra = (0)$ or $Ra = R$. Since $0 \neq a = 1a \in Ra$, $Ra \neq (0)$, thus we are left with the only other possibility, namely that $Ra = R$. This last equation states that every element in R is a multiple of a by some element of R

particular, $1 \in R$ and so it can be realized as a multiple of a (i.e.) there exists an element $b \in R$ such that $ba = 1$

Hence completes the lemma

Definition: An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subset U \subset R$, then either $R = U$ or $M = U$.

Theorem: If R is a commutative ring with unit element and M is an ideal of R then M is a maximal ideal of R if and only if R/M is a field

Proof: Suppose, first, that M is an ideal of R such that R/M is a field since R/M is a field its only ideals are (0) and R/M itself. But by theorem, there is a one to one correspondence between the set of ideals of R/M and the set of ideals of R which contain M. The ideal M of R corresponds to the ideal (0) of R/M whereas the ideal R of R corresponds to the ideal R/M of R/M in this one-to-one mapping.

Thus there is no ideal between M and R other than these two, whence M is a maximal ideal.

On the other hand, if M is a maximal ideal of R, by the correspondence mentioned above R/M has only (0) and itself as ideals. Furthermore R/M is commutative and has a unit element since R enjoys both these properties.

All the conditions of Lemma, are fulfilled for R/M so we can conclude, by the result of that lemma, that R/M is a field.

The Field of Quotients of an Integral Domain

Definition: A ring R can be imbedded in a ring R' if there is an isomorphism of R into R'. R' will be called an over-ring or extension of R if R can be imbedded in R'.

Theorem: Every integral domain can be imbedded in a field

Proof: We define $[a,b] + [c,d] = [ad+bc, bd]$

Since D is an integral domain and both $b \neq 0$ and $d \neq 0$ we have that $bd \neq 0$, this at least, tells us that $[ad+bc, bd] \in F$. We now assert that this addition is well defined, that is, if $[a,b] = [a', b']$ and $[c,d] = [c',d']$, then $[a,b] + [c,d] = [a',b'] + [c',d']$.

To see that this is so, from $[a,b] = [a',b']$ we have that $ab' = ba'$ from $[c,d] = [c',d']$ we have that $cd' = dc'$.

What we need is that these relations force the equality of $[a,b]+[c,d]$ and $[a',b']+[c',d']$. From the definition of addition this boils down to showing that $[ad+bc, bd] = [a'd'+b'c', b'd']$ or in equivalent terms that $(ad+bc)b'd' = bd(a'd'+b'c')$.

Using $ab' = ba'$, $cd' = dc'$ this becomes: $(ad+bc)b'd' = adb'd' + bcb'd' = ab'dd' + bb'cd' = ba'dd' + bb'dc' = bd(a'd'+b'c')$.

Clearly $[0,b]$ acts as a zero-element for this addition and $[-a,b]$ as the negative of $[a,b]$. It is a simple matter to verify that F is an abelian group under this addition.

We now turn to the multiplication in F. Again motivated by our preliminary heuristic discussion we define $[a,b][c,d] = [ac, bd]$. As in the case of addition, since $b \neq 0$, $d \neq 0$, $bd \neq 0$ and so $[ac, bd] \in F$.

A computation, very much in the spirit of the one just carried out, proves that if $[a,b] = [a',b']$ and $[c,d] = [c',d']$ then $[a,b][c,d] = [a',b'][c',d']$. One can now show that the nonzero elements of F form an abelian group under multiplication in which $[d,d]$ acts as the unit element and where

$$[c,d]^{-1} = [d,c] \quad (\text{since } c \neq 0, [d,c] \text{ is in } F).$$

It is a routine computation to see that the distributive law holds in F. F is thus a field. ~~We shall exhibit an ex~~ All that remains is to show that D can be imbedded in F. We shall exhibit an explicit isomorphism of D into F. Before doing so we first notice that for $x \neq 0$, $y \neq 0$ in D, $[ax, x] = [ay, y]$ because $(ax)y = x(ay)$, let us denote $[ax, x]$ by $[a,1]$. Define $\phi: D \to F$ by $\phi(a) = [a,1]$ for every $a \in D$. We leave it to the reader to verify that ϕ is an isomorphism of D into F, and that if D has a unit element 1, then $\phi(1)$ is the unit element of F.

Thus completes the proof.

EUCLIDEAN RINGS:

Definition: An integral domain R is said to be a Euclidean ring if for every $a \neq 0$ in R there is defined a nonnegative integer $d(a)$ such that

1. For all $a, b \in R$, both nonzero, $d(a) \leq d(ab)$.
2. For any $a, b \in R$, both nonzero, there exists $t, r \in R$ such that $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.

Theorem: Let R be a Euclidean ring and let A be an ideal of R. Then there exists an element $a_0 \in A$ such that A consists exactly of all $a_0 x$ as x ranges over R.

Proof: If A just consists of the element 0, put $a_0 = 0$ and the conclusion of the theorem holds.

Thus we may assume that $A \neq (0)$, hence there is an $a \neq 0$ in A. pick an $a_0 \in A$ such that $d(a_0)$ is minimal. suppose that $a \in A$. By the properties of Euclidean rings there exist $r, t \in R$ such that $a = ta_0 + r$ where $r = 0$ or $d(r) < d(a_0)$. Since $a_0 \in A$ and A is an ideal of R, ta_0 is in A. Combined with $a \in A$ this results in $a - ta_0 \in A$ but $r = a - ta_0$ whence $r \in A$. If $r \neq 0$ then $d(r) < d(a_0)$, giving us an element r in A whose d-value is smaller than that of a_0, in contradiction to our choice of a_0 as the element in A of minimal d-value. Consequently $r = 0$ and $a = ta_0$, which proves the theorem.

Definition: An integral domain R with unit element is a principal ideal ring if every ideal A in R is of the form $A = (a)$ for some $a \in R$.

Corollary: A Euclidean ring possesses a unit element.

Proof: Let R be a Euclidean ring, then R is certainly an ideal of R, so that by theorem, we may conclude that $R = (u_0)$ for some $u_0 \in R$. Thus every element in R is a multiple of u_0. Therefore, in particular, $u_0 = u_0 c$ for some $c \in R$. If $a \in R$ then $a = xu_0$ for some $x \in R$, hence $ac = (xu_0)c = x(u_0 c) = xu_0 = a$.

Thus c is seen to be the required unit element.

Definition: If $a \neq 0$ and b are in a commutative ring R then a is said to divide b if there exists a $c \in R$ such that $b = ac$.

Definition: If $a, b \in R$ then $d \in R$ is said to be a greatest common divisor of a & b if ① $d|a$ and $d|b$ ② whenever $c|a$ and $c|b$ then $c|d$.

Lemma: Let R be a Euclidean ring. Then any two elements a and b in R have a greatest common divisor d. Moreover $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Proof: Let A be the set of all elements $ra + sb$ where r, s range over R. We claim that A is an ideal of R. For suppose that $x, y \in A$, therefore $x = r_1 a + s_1 b$, $y = r_2 a + s_2 b$, and so $x \pm y = (r_1 \pm r_2)a + (s_1 \pm s_2)b \in A$. Similarly, for any $u \in R$, $ux = u(r_1 a + s_1 b) = (ur_1)a + (us_1)b \in A$.

Since A is an ideal of R, by theorem there exists an element $d \in A$ such that every element in A is a multiple of d. By dint of the fact that $d \in A$ and that every element of A is of the form $ra + sb$, $d = \lambda a + \mu b$ for some $\lambda, \mu \in R$.

Now by the corollary to theorem, R has a unit element 1, thus $a = 1a + 0b \in A$, $b = 0a + 1b \in A$. Being in A, they are both multiples of d, whence $d|a$ and $d|b$.

Suppose, finally, that $c|a$ and $c|b$, then $c \mid \lambda a$ and $c \mid \mu b$ so that c certainly divides $\lambda a + \mu b = d$. Therefore d has all the requisite conditions for a greatest common divisor and the lemma is proved.

Definition: Let R be a commutative ring with unit element. An element $a \in R$ is a unit in R if there exists an element $b \in R$ such that $ab = 1$.

Lemma: Let R be an integral domain with unit element and suppose that for $a, b \in R$ both $a|b$ and $b|a$ are true. Then $a = ub$, where u is a unit in R.

Proof: Since $a|b$, $b = xa$ for some $x \in R$, Since $b|a$, $a = yb$ for some $y \in R$. Thus $b = x(yb) = (xy)b$, but these are elements of an integral domain so that we can cancel the b and obtain $xy = 1$, y is thus a unit in R and $a = yb$,

Hence the Lemma

Definition: Let R be a commutative ring with unit element. Two elements a and b in R are said to be associates if $b = ua$ for some unit u in R.

Lemma: Let R be a Euclidean ring and $a, b \in R$. If $b \neq 0$ is not a unit in R, then $d(a) < d(ab)$.

Proof: Consider the ideal $A = (a) = \{xa \mid x \in R\}$ of R. By condition 1 for a Euclidean ring, $d(a) \leq d(xa)$ for $x \neq 0$ in R. Thus the d-value of a is the minimum for the d-value of any element in A. Now $ab \in A$, if $d(ab) = d(a)$. Since the d-value of ab is minimal in regard to A, every element in A is a multiple of ab.

In particular, since $a \in A$, a must be a multiple of ab, whence $a = abx$ for some $x \in R$. Since all this is taking place in an integral domain we obtain $bx = 1$.

In this way b is a unit in R, in contradiction to the fact that it was not a unit. The net result of this is that $d(a) < d(ab)$.

Hence the lemma.

Definition: In the Euclidean ring R a non unit π is said to be a prime element of R if whenever $\pi = ab$, where a, b are in R, then one of a (or) b is a unit in R.

Lemma: Let R be a Euclidean ring. Then every element in R is either a unit in R or can be written as the product of a finite number of prime elements of R.

Proof: The proof is by induction on $d(a)$.

If $d(a) = d(1)$ then a is a unit in R, and so in this case, the assertion of the lemma is correct.

... assume that the lemma is true for all elements x in R such that $d(x) < d(a)$. On the basis of this assumption we aim to prove it for a.

By induction proof

If a is a prime element of R there is nothing to prove. So suppose that $a = bc$ where neither b nor c is a unit in R. By lemma, $d(b) < d(bc) = d(a)$ and $d(c) < d(bc) = d(a)$. Thus by our induction hypotheses b and c can be written as a product of a finite number of prime elements of R, $b = \pi_1 \pi_2 \ldots \pi_n$, $c = \pi_1' \pi_2' \ldots \pi_m'$ where the π's and π''s are prime elements of R. Consequently $a = bc = \pi_1 \pi_2 \ldots \pi_n \pi_1' \pi_2' \ldots \pi_m'$ and in this way a has been factored as a product of a finite number of prime elements.

This completes the proof.

Definition: In the Euclidean ring R, a and b in R are said to be relatively prime if their greatest common divisor is a unit of R.

Lemma: Let R be a Euclidean ring. Suppose that for $a, b, c \in R$, $a | bc$ but $(a, b) = 1$. Then $a | c$.

Proof: As we have seen in previous Lemma, the greatest common divisor of a and b can be realized in the form $\lambda a + \mu b$. Thus by our assumptions, $\lambda a + \mu b = 1$.

Multiplying this relation by c we obtain $\lambda ac + \mu bc = c$. Now $a | \lambda ac$, always, and $a | \mu bc$ since $a | bc$ by assumption, therefore $a | (\lambda ac + \mu bc) = c$.

Hence the Lemma.

POLYNOMIAL RINGS:

Definition: If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are in $F[x]$, then $p(x) = q(x)$ if and only if for every integer $i \geq 0$, $a_i = b_i$

Definition: If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $F[x]$, then $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$

Definition: If $p(x) = a_0 + a_1x + \cdots + a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$, then $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t$.

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$ then the degree of $f(x)$, written as $\deg f(x)$, is n.

Lemma: If $f(x)$, $g(x)$ are two non-zero elements of $F[x]$, then

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

Proof: Suppose that $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ and that $a_m \neq 0$ and $b_n \neq 0$. Therefore $\deg f(x) = m$ and $\deg g(x) = n$.

By definition, $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_kx^k$ where $c_t = a_tb_0 + a_{t-1}b_1 + \cdots + a_1b_{t-1} + a_0b_t$. We claim that $c_{m+n} = a_mb_n \neq 0$ and $c_i = 0$ for $i > m+n$.

That $c_{m+n} = a_mb_n$ can be seen at a glance by its definition. c_i is the sum of terms of the form a_jb_{i-j}, Since $i = j + (i-j) > m+n$ then either $j > m$ (or) $(i-j) > n$.

But then one of a_j or b_{i-j} is 0, so that $a_jb_{i-j} = 0$, Since c_i is the sum of a bunch of zeros it itself is 0, and our claim has been established.

Thus the highest nonzero coefficient of $f(x)g(x)$ is c_{m+n}, whence $\deg f(x)g(x) = m+n = \deg f(x) + \deg g(x)$.

Corollary: If $f(x)$, $g(x)$ are nonzero elements in $F[x]$ then $\deg f(x) \leq \deg f(x)g(x)$.

Lemma Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exist polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

Proof: If the degree of $f(x)$ is smaller than that of $g(x)$ there is nothing to prove for merely put $t(x) = 0$, $r(x) = f(x)$ and we certainly have that $f(x) = 0g(x) + f(x)$ where $\deg f(x) < \deg g(x)$ or $f(x) = 0$

So we may assume that $f(x) = a_0 + a_1x + \dots + a_mx^m$ and $g(x) = b_0 + \dots + b_nx^n$ where $a_m \neq 0$, $b_n \neq 0$ and $m \geq n$.

Let $f_1(x) = f(x) - (a_m/b_n)x^{m-n}g(x)$ thus $\deg f_1(x) \leq m-1$, so by induction on the degree of $f(x)$ we may assume that $f_1(x) = t_1(x)g(x) + r(x)$ where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$.

But then $f(x) - (a_m/b_n)x^{m-n}g(x) = t_1(x)g(x) + r(x)$, from which, transposing, we arrive at $f(x) = ((a_m/b_n)x^{m-n} + t_1(x))g(x) + r(x)$.

If we put $t(x) = (a_m/b_n)x^{m-n} + t_1(x)$. we do indeed have that $f(x) = t(x)g(x) + r(x)$ where $t(x), r(x) \in F[x]$. and where $r(x) = 0$ (or) $\deg r(x) < \deg g(x)$. This proves the lemma.

Definition: A polynomial $p(x)$ in $F[x]$ is said to be irreducible over F if whenever $p(x) = a(x)\,b(x)$ with $a(x), b(x) \in F[x]$, then one of $a(x)$ (or) $b(x)$ has degree 0.

Lemma: Any polynomial in $F[x]$ can be written in a unique manner as product of irreducible polynomials in $F[x]$.

Lemma: The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F.

POLYNOMIALS OVER THE RATIONAL FIELD

Definition: The polynomial $f(x) = a_0 + a_1x + \dots + a_nx^n$, where the $a_0, a_1, a_2 \dots a_n$ are integers is said to be primitive if the greatest common divisor of $a_0, a_1, \dots a_n$ is 1.

If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)g(x)$ is a primitive polynomial.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$

Suppose that the Lamma was false, then all the coefficients of $f(x)g(x)$ would be divisible by some integer larger than 1, hence by some prime number p.

Since $f(x)$ is primitive, p does not divide some coefficient a_i.

Let a_j be the first coefficient of $f(x)$ which p does not divide.

Similarly let b_k be the first coefficient of $g(x)$ which p does not divide. In $f(x)g(x)$ the coefficient of x^{j+k}, c_{j+k} is

$$c_{j+k} = a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{j+k}) \rightarrow ①$$

Now by our choice of b_k, $p \mid b_{k-1}, b_{k-2} \cdots$ so that

$p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots a_{j+k}b_0)$.

Similarly, by our choice of a_j, $p \mid a_{j-1}, a_{j-2} \cdots$ so that

$p \mid (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0b_{k+j})$.

By assumption, $p \mid c_{j+k}$. Thus by ①, $p \mid a_jb_k$, which is nonsense since $p \nmid a_j$ and $p \nmid b_k$.

Hence the Lemma.

Definition: The content of the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where the a's are integers, is the greatest common divisor of the integers $a_0, a_1, a_2 \cdots a_n$.

Polynomial rings over Commutative Rings

Lemma If R is an integral domain, then so is $R[x]$

Proof For $0 \neq f(x) = a_0 + a_1 x + \cdots + a_m x^m$, where $a_m \neq 0$, in $R[x]$, we define the degree of $f(x)$ to be m, thus $\deg f(x)$ is the index of the highest nonzero coefficient of $f(x)$.

If R is an integral domain we leave it as an exercise to prove that $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

But then, for $f(x) \neq 0$, $g(x) \neq 0$, it is impossible to have $f(x)g(x) = 0$. That is, $R[x]$ is an integral domain.

Definition:- An integral domain, R, with unit element is a unique factorization domain if.

a. Any nonzero element in R is either a unit or can be written as the product of a finite number of irreducible elements of R.

b. The decomposition in part (a) is unique up to the order and associates of the irreducible elements.

Lemma:- If R is a unique factorization domain and if $p(x)$ is a primitive polynomial in $R[x]$, then it can be factored in a unique way as the product of irreducible elements in $R[x]$.

Proof:- when we consider $p(x)$ as an element in $F[x]$, by Lemma we can factor it as $p(x) = p_1(x)\, p_2(x) \cdots p_k(x)$, where $p_1(x), p_2(x), \ldots p_k(x)$ are irreducible polynomials in $F[x]$.

Each $p_i(x) = (f_i(x)/a_i)$ where $f_i(x) \in R[x]$ and $a_i \in R$, moreover, $f_i(x) = c_i q_i(x)$, where $c_i = c(f_i)$ and where $q_i(x)$ is primitive in $R[x]$. Thus each $p_i(x) = (c_i q_i(x)/a_i)$, where $a_i, c_i \in R$ and where $q_i(x) \in R[x]$ is primitive.

Since $p_i(x)$ is irreducible in $F[x]$, $q_i(x)$ must also be irreducible in $F[x]$. hence by Lemma, it is irreducible in $R[x]$

Now $p(x) = p_1(x) \cdots p_k(x) = \dfrac{c_1 c_2 \cdots c_k}{a_1 a_2 \cdots a_k} q_1(x) \cdots q_k(x)$,

whence $a_1 a_2 \cdots a_k p(x) = c_1 c_2 \cdots c_k q_1(x) \cdots q_k(x)$.

Using the primitivity of $p(x)$ and of $q_1(x) \cdots q_k(x)$, we can read off the content of the left-hand side as $a_1 a_2 \cdots a_k$ and that of the right-hand side as $c_1 c_2 \cdots c_k$.

Thus $a_1 a_2 \cdots a_k = c_1 c_2 \cdots c_k$. hence $p(x) = q_1(x) \cdots q_k(x)$ we have factored $p(x)$, in $R[x]$, as a product of irreducible elements.

<u>Theorem</u>: If R is a unique factorization domain, then so is $R[x]$

<u>Proof</u>: Let $f(x)$ be an arbitrary element in $R[x]$. We can write $f(x)$ in a unique way as $f(x) = cf_1(x)$ where $c = c(f)$ is in R and where $f_1(x)$, in $R[x]$ is primitive.

By Lemma, we can decompose $f_1(x)$ in a unique way as the product of irreducible elements of $R[x]$.

Suppose that $c = a_1(x) a_2(x) \cdots a_m(x)$ in $R[x]$, then $0 = \deg c = \deg(a_1(x)) + \deg(a_2(x)) + \cdots + \deg(a_m(x))$. Therefore, each $a_i(x)$ must be of degree 0, that is, it must be an element of R.

In other words, the only factorizations of c as an element of $R[x]$ are those it had as an element of R. In particular, an irreducible element in R is still irreducible in $R[x]$. Since R is a unique factorization domain, c has a unique factorization as a product of irreducible elements of R, hence of $R[x]$.

Putting together the unique factorization of $f(x)$ in the form $cf_1(x)$ where $f_1(x)$ is primitive and where $c \in R$ with the unique factorization of c and $f_1(x)$ we have proved the theorem.

Inner product spaces:-

The vector space V over F is said to be an inner product space if there is defined for any two vectors $u, v \in V$ an element (u,v) in F such that 1. $(u,v) = (v,u)$

2. $(u,u) \geq 0$ and $(u,u) = 0$ if and only if $u = 0$

3. $(\alpha u + \beta v, w) = \alpha (u,w) + \beta (v,w)$

For any $u, v, w \in V$ and $\alpha, \beta \in F$.

Corollary:- If V is a finite-dimensional inner product space and W is a subspace of V then $(W^{\perp})^{\perp} = W$.

Proof:- If $w \in W$ then for any $u \in W^{\perp}$, $(w,u) = 0$, whence $W \subset (W^{\perp})^{\perp}$

Now $V = W + W^{\perp}$ and $V = W^{\perp} + (W^{\perp})^{\perp}$, from these we get, since the sums are direct, $\dim(W) = \dim((W^{\perp})^{\perp})$.

Since $W \subset (W^{\perp})^{\perp}$ and is of the same dimension as $(W^{\perp})^{\perp}$ it follows that $W = (W^{\perp})^{\perp}$.

Unit - V

Extension Fields:

Definition: The degree of K over F is the dimension of K as a vector space over F.

Theorem: If L is a finite extension of K and if K is a finite extension of F, then L is a finite extension of F. Moreover $[L:F] = [L:K][K:F]$

Proof: Suppose, then, that $[L:K] = m$ and that $[K:F] = n$. Let $v_1, v_2 \cdots v_m$ be a basis of L over K and let $\omega_1, \omega_2 \cdots \omega_n$ be a basis of K over F.

We now proceed to show that they do in fact form a basis of L over F. First we must show that every element in L is a linear combination of them with coefficients in F, and then we must demonstrate that these mn elements are linearly independent over F.

Let t be any element in L, since every element in L is a linear combination of $v_1, v_2 \cdots v_m$ with coefficients in K, in particular, t must be of this form.

Thus $t = k_1v_1 + k_2v_2 + \cdots + k_mv_m$, where the elements $k_1, k_2 \cdots k_m$ are all in K.

However, every element in K is a linear combination of $\omega_1, \omega_2 \cdots \omega_n$ with coefficients in F.

Thus $k_1 = f_{11}\omega_1 + f_{12}\omega_2 + \cdots + f_{1n}\omega_n, \cdots k_i = f_{i1}\omega_1 + \cdots + f_{in}\omega_n, \cdots$

$k_m = f_{m1}\omega_1 + f_{m2}\omega_2 + \cdots + f_{mn}\omega_n$, where every f_{ij} is in F.

Substituting these expressions for $k_1, \cdots k_m$ into $t = k_1v_1 + \cdots + k_mv_m$

we obtain $t = (f_{11}\omega_1 + \cdots + f_{1n}\omega_n)v_1 + \cdots + (f_{m1}\omega_1 + \cdots + f_{mn}\omega_n)v_m$.

Multiplying this out, using the distributive and associative laws,

we finally arrive at $t = f_{11}v_1\omega_1 + \cdots + f_{1n}v_1\omega_n + \cdots + f_{ij}v_i\omega_j + \cdots + f_{mn}v_m\omega_n$.

Since the f_{ij} are in F, we have realized t as a linear combination over F of the elements $v_i\omega_j$

Therefore, the elements $v_i w_j$ do indeed span all of L over and so they fulfill the first requisite property of a basis.

Suppose that $f_{11}v_1w_1 + \cdots + f_{1n}v_1w_n + \cdots + f_{ij}v_iw_j + \cdots + f_{mn}v_mw_n = 0$, where the f_{ij} are in F. Our objective is to prove that each $f_{ij} = 0$. Regrouping the above expression yields $(f_{11}w_1 + \cdots + f_{1n}w_n)v_1 + \cdots + (f_{i1}w_1 + \cdots + f_{in}w_n)v_i + \cdots + (f_{m1}w_1 + \cdots + f_{mn}w_n)v_m = 0$.

Since the w_i are in K, and since $K \supset F$, all the elements $k_i = f_{i1}w_1 + \cdots + f_{in}w_n$ are in K. Now $k_1v_1 + \cdots k_mv_m = 0$ with $k_1, k_2 \cdots k_m \in K$. But, by assumption $v_1, v_2 \cdots v_m$ form a basis of L over K. So, in particular they must be linearly independent over K.

The net result of this is that $k_1 = k_2 = \cdots = k_m = 0$. Using the explicit values of the k_i, we get

$$f_{i1}w_1 + \cdots + f_{in}w_n = 0 \text{ for } i = 1, 2 \cdots m$$

But now we invoke the fact that the w_i are linearly independent over F, this yields that each $f_{ij} = 0$. In other words, we have proved that the v_iw_j are linearly independent over F.

We have now succeeded in proving that the mn elements v_iw_j form a basis of L over F. Thus $[L:F] = mn$; Since $m = [L:K]$ and $n = [K:F]$.

we have obtained the desired result $[L:F] = [L:K][K:F]$

Thus Completes the proof.

Definition: An element $a \in K$ is said to be algebraic over F if there exists elements $\alpha_0, \alpha_1 \cdots \alpha_n$ in F, not all 0, such that $\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.

...nition: The extension K of F is called an algebraic extension of F ...very element in K is algebraic over F.

Theorem: If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.

Proof: Let u be any arbitrary element of L, our objective is to show that u satisfies some nontrivial polynomial with coefficients in F.

We certainly do know that u satisfies some polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$, where $\sigma_1, \ldots \sigma_n$ are in K. But K is algebraic over F, therefore, by several uses of Theorem, $M = F(\sigma_1, \sigma_2 \ldots \sigma_n)$ is a finite extension of F.

Since u satisfies the polynomial $x^n + \sigma_1 x^{n-1} + \cdots + \sigma_n$ whose coefficients are in M, u is algebraic over M.

Invoking theorem yields that $M(u)$ is a finite extension of M. However, by theorem $[M(u):F] = [M(u):M][M:F]$ whence $M(u)$ is a finite extension of F.

But this implies that u is algebraic over F, Completing proof of the theorem.

Roots of polynomials:

Definition: If $p(x) \in F[x]$, then an element a lying in some extension field of F is called a root of $p(x)$ if $p(a) = 0$.

Lemma: If $p(x) \in F[x]$ and if K is an extension of F, then for any element $b \in K$, $p(x) = (x-b)q(x) + p(b)$ where $q(x) \in K[x]$ and where $\deg q(x) = \deg p(x) - 1$.

Proof: Since $F \subset K$, $F[x]$ is contained in $K[x]$, whence we can consider $p(x)$ to be lying in $K[x]$.

By the division algorithm for polynomials in $K[x]$,

$p(x) = (x-b)q(x) + r$, where $q(x) \in K[x]$ and where $r = 0$ (or) $\deg r < \deg(x-b) = 1$.

Thus either $r = 0$ (or) $\deg r = 0$ in either case r must be an element of K. But exactly what element of K is it?

Since $p(x) = (x-b)q(x) + r$, $p(b) = (b-b)q(b) + r = r$.

Therefore $p(x) = (x-b)q(x) + p(b)$. That the degree of $q(x)$ is one less than that of $p(x)$ is easy to verify and is left to the reader.

Corrollary: If $a \in K$ is a root of $p(x) \in F[x]$, where $F \subset K$, then in $K[x]$, $(x-a) \mid p(x)$.

More about Roots

Definition: If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots \alpha_i x^{n-i} + \cdots + \alpha_{n-1} x + \alpha_n$ in $F[x]$, then the derivative of $f(x)$, written as $f'(x)$, is the polynomial

$f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$ in $F[x]$.

Definition: The extension K of F is a simple extension of F if $K = F(\alpha)$ for some α in K.

Theorem: If F is of characteristic 0 and if a, b are algebraic over F, then there exists an element $c \in F(a,b)$ such that $F(a,b) = F(c)$.

Proof: Let $f(x)$ and $g(x)$ of degrees m and n, be the irreducible polynomials over F satisfied by a and b, respectively.

Let K be an extension of F in which both $f(x)$ and $g(x)$ split completely. Since the characteristic of F is 0, all the roots of $f(x)$ are distinct, as are all those of $g(x)$.

Let the roots of $f(x)$ be $a = a_1, a_2, \ldots, a_n$ and those of $g(x)$, $b = b_1, b_2, \ldots, b_m$.

If $j \neq 1$, then $b_j \neq b_1 = b$. hence the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K, namely

$$\lambda = \frac{a_i - a}{b - b_j}$$

Since F is of characteristic 0 it has an infinite number of elements, So we can find an element $\gamma \in F$ such that $a_i + \gamma b_j \neq a + \gamma b$ for all i and for all $j \neq 1$.

Let $c = a + \gamma b$, our contention is that $F(c) = F(a, b)$ since $c \in F(a, b)$, we certainly do have that $F(c) \subset F(a, b)$

we will now show that both a and b are in $F(c)$ from which it will follow that $F(a, b) \subset F(c)$

Now b satisfies the polynomial $g(x)$ over F, hence satisfies $g(x)$ considered as a polynomial over $K = F(c)$. Moreover, if $h(x) = f(c - \gamma x)$ then $h(x) \in K[x]$ and $h(b) = f(c - \gamma b) = f(a) = 0$, since $a = c - \gamma b$.

Thus in some extension of K, $h(x)$ and $g(x)$ have $x - b$ as a common factor. We assert that $x - b$ is in fact their greatest common divisor. For, if $b_j \neq b$ is another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$ since by our choice of γ, $c - \gamma b_j$ for $j \neq 1$ avoids all roots a_i of $f(x)$.

Also, since $(x-b)^2 \nmid g(x)$, $(x-b)^2$ cannot divide the greatest common divisor of $h(x)$ and $g(x)$. Thus $(x-b)$ is the greatest common divisor of $h(x)$ and $g(x)$ over some extension of K.

But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$.

Since the degree of $x-b$ is 1, we see that the greatest common divisor of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x-b$.

Thus $x-b \in K[x]$, whence $b \in K$, remembering that $K = F(c)$, we obtain that $b \in F(c)$.

Since $a = c - \gamma b$, and since $b, c \in F(c)$, $\gamma \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a,b) \subset F(c)$. The two opposite containing relations combine to yield $F(a,b) = F(c)$.

A simple induction argument extends the result from 2 elements to any finite number, that is, if $\alpha_1, \alpha_2 \cdots \alpha_n$ are algebraic over F, then there is an element $c \in F(\alpha_1, \alpha_2 \cdots \alpha_n)$ such that $F(c) = F(\alpha_1, \alpha_2 \cdots \alpha_n)$. Thus the

---

Corollary: Any finite extension of a field of characteristic 0 is a simple extension.