Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Abelian Groups

Direct Sums

- It is traditional to write abelian groups in additive notation, writing

$$a+b, 0, -a, na, \quad n \in \mathbb{Z},$$

rather than

$$ab, 1, a^{-1}, a^n.$$

- We shall be concerned here solely with *finite abelian groups*.
- An abelian group A with subgroups $U_1, U_2, \ldots, U_k$ is said to be the **direct sum** of $U_1, U_2, \ldots, U_k$, if every element a of A has a unique expression

$$a = u_1 + u_2 + \cdots + u_k, \quad u_i \in U_i,\ i = 1, 2, \ldots, k.$$

- Clearly, $U_i \cap U_j = \{0\}$, if $i \neq j$.
  If $0 \neq w \in U_i \cap U_j$, we would have distinct expressions $w + 0 = 0 + w$.
- We write $A = U_1 \oplus \cdots \oplus U_k$.

An Equivalent Condition

- It follows from the definition that, for all $u_i \in U_i$, $i = 1, 2, \dots, k$,

$$u_1 + u_2 + \cdots + u_k = 0 \quad \text{implies} \quad u_1 = u_2 = \cdots = u_k = 0.$$

  Otherwise we would have two distinct expressions for the element 0, the other being $0 + 0 + \cdots + 0$.

- This condition is actually equivalent to the uniqueness condition in $a = u_1 + \cdots + u_k$, $u_i \in U_i$, $i = 1, \dots, k$.

  Let $a = u_1 + u_2 + \cdots + u_k = u_1' + u_2' + \cdots + u_k'$, with $u_i, u_i' \in U_i$, for all i. Then

$$(u_1 - u_1') + (u_2 - u_2') + \cdots + (u_k - u_k') = 0.$$

  By the hypothesis, we get $u_i = u_i'$, for all i.

Order a Product of Two Coprimes

Lemma

Let a be an element of a finite abelian group A, and suppose that the order of a is mn, where $\gcd(m,n)=1$. Then a can be written in exactly one way as $b+c$, where $o(b)=m$ and $o(c)=n$.

- Let $b'=na$ and $c'=ma$. Then certainly $o(b')=m$ and $o(c')=n$.
  Since m and n are coprime, there exist s,t in $\mathbb{Z}$, such that $sm+tn=1$.
  Hence, $a=(sm+tn)a=tb'+sc'$.
  Since $sm+tn=1$, we must have $\gcd(t,m)=1$ and $\gcd(s,n)=1$.
  Hence, $o(tb')=m$ and $o(sc')=n$. So $b=tb'$ and $c=sc'$ are such that $a=b+c$, with $o(b)=m$ and $o(c)=n$.
  Let $a=b+c=b_1+c_1$, where $o(b)=o(b_1)=m$ and $o(c)=o(c_1)=n$.
  So $b-b_1=c_1-c=d$ (say). Then $md=mb-mb_1=0$ and $nd=nc_1-nc=0$. So $o(d)$ divides both m and n. Hence, $o(d)=1$.
  So $b-b_1=c_1-c=0$. I.e., $b=b_1$ and $c=c_1$.

Order a Product of Finitely Many Coprimes

Corollary

Let a be an element of a finite abelian group A, and suppose that $o(a) = m_1 m_2 \cdots m_r$, where $\gcd(m_i, m_j) = 1$, whenever $i \neq j$.
Then a can be written in exactly one way as

$$a_1 + a_2 + \cdots + a_r,$$

where $o(a_i) = m_i$, $i = 1, 2, \ldots, r$.

- By hypothesis, $\gcd(m_1 \cdots m_{r-1}, m_r) = 1$.

  By the theorem we can write a uniquely as $a' + a_r$, with $o(a') = m_1 \cdots m_{r-1}$ and $o(a_r) = m_r$.

  The result then follows by induction on r.

Direct Sum Decomposition of Finite Abelian Groups

Theorem

Every finite abelian group is expressible as the direct sum of abelian p-groups.

- Suppose A is an abelian group of order $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$.

  Let U_i be the set of elements of A whose order is a power of p_i.

  Claim: U_i is a subgroup of A.

  Let $x, y \in U_i$, with orders p_i^k, p_i^ℓ, respectively. Then $p_i^{\max\{k,\ell\}}(x - y) = 0$.

  So the order of $x - y$ is a divisor of $p_i^{\max\{k,\ell\}}$. So it is a power of p_i. Thus, $x - y \in U_i$.

  Let a be an element of A. Then the order of a divides n. So a has order $p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$. By the corollary, a can be expressed uniquely as $a_1 + a_2 + \cdots + a_r$, with $o(a_i) = p_i^{d_i}$, $i = 1, 2, \ldots, r$. Thus, we have $A = U_1 \oplus U_2 \oplus \cdots \oplus U_r$.

The Basis Theorem

Theorem (The Basis Theorem)

Every finite abelian group is expressible as a direct sum of cyclic groups.

- In view of the preceding theorem, we need only consider an abelian p-group A, of order p^m.
  Let a_1 be an element of maximal order p^{r_1} in A.
  Let $A_1 = \langle a_1 \rangle$, the cyclic subgroup of A generated by a_1.
  If $r_1 = m$, then $\langle a_1 \rangle = A$. Thus, the group A is cyclic.
  So suppose that $r_1 < m$. We prove the result by induction.
  Suppose that we have found k elements $a_1, a_2, \ldots, a_k$ of orders $p^{r_1}, p^{r_2}, \ldots, p^{r_k}$ (respectively) such that:
  (i) $r_1 \geq r_2 \geq \cdots \geq r_k$;
  (ii) The subgroup $P_k = \langle a_1, a_2, \ldots, a_k \rangle$ is the direct sum
  $$\langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_k \rangle;$$
  (iii) No element of $A \backslash P_k$ has order exceeding p^{r_k}.

The Basis Theorem (Cont'd)

- If $P_k = A$, then we are done.
  Suppose there exists b in $A \setminus P_k$. By (iii), the order of b is p^β, $\beta \le r_k$.
  The set of multiples of b lying in P_k is non-empty, since $p^\beta b = 0 \in P_k$.
  Let λ be the least positive integer with the property that $\lambda b \in P_k$.
  Thus,
  $$\lambda b = \sum_{i=1}^{k} \mu_i a_i, \quad \lambda \le p^\beta.$$
  Claim: The integer λ must in fact be a power of p.
  We divide p^β by λ to obtain $p^\beta = q\lambda + r$, with $0 \le r < \lambda$.
  Suppose $r \neq 0$. Then $rb = p^\beta b - q\lambda b = -q\lambda b \in P_k$. This contradicts the definition of λ as the least integer with this property. So $r = 0$.
  It follows that λ divides p^β. Thus, λ is a power of p, say $\lambda = p^{r_{k+1}}$.
  By (iii), $r_{k+1} \le r_k$. Certainly, $r_{k+1} \le \beta$.

The Basis Theorem (Cont'd)

Claim: Every coefficient μ_i in $\lambda b = \sum_{i=1}^k \mu_i a_i$ is divisible by λ.

Multiply by $\frac{p^\beta}{\lambda} = p^{\beta - r_{k+1}}$. We get $0 = p^\beta b = \sum_{i=1}^k \frac{\mu_i p^\beta}{\lambda} a_i$.

By (ii), we have $\frac{\mu_i p^\beta}{\lambda} a_i = 0$, for all i.

Hence, $\frac{\mu_i p^\beta}{\lambda} = \mu_i p^{\beta - r_{k+1}}$ is divisible by $o(a_i) = p^{r_i}$, say $\frac{\mu_i p^\beta}{\lambda} = \mu_i' p^{r_i}$.

Now $\beta \leq r_i$, for $i = 1, 2, \ldots, k$.

Hence, $\mu_i = \lambda \mu_i' p^{r_i - \beta} = \lambda \nu_i$, where $\nu_i = \mu_i' p^{r_i - \beta}$ is an integer.

Let

$$a_{k+1} = b - \sum_{i=1}^k \nu_i a_i.$$

Then the order of a_{k+1} is $\lambda = p^{r_{k+1}}$.

We have $\lambda a_{k+1} = \lambda b - \sum_{i=1}^k \lambda \nu_i a_i = 0$.

Assume $\kappa a_{k+1} = 0$, for $\kappa > 0$.

Then $\kappa b = \kappa (a_{k+1} + \sum_{i=1}^k \lambda \nu_i a_i) = \sum_{i=1}^k \kappa \lambda \nu_i a_i \in P_k$. So $\kappa \geq \lambda$.

The Basis Theorem (Conclusion)

- Let $P_{k+1} = \langle a_1, a_2, \ldots, a_k, a_{k+1}\rangle$.
  We must show $P_{k+1} = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_k\rangle \oplus \langle a_{k+1}\rangle$.
  We show that, if $z_1a_1 + z_2a_2 + \cdots + z_{k+1}a_{k+1} = 0$, where $z_1, z_2, \ldots, z_{k+1}$ are integers, then $z_1a_1 = z_2a_2 = \cdots = z_{k+1}a_{k+1} = 0$.
  Let $z_1a_1 + z_2a_2 + \cdots + z_{k+1}a_{k+1} = 0$, with $z_1, z_2, \ldots, z_{k+1}$ integers.
  Then $z_{k+1}a_{k+1}$ belongs to P_k. Since $a_{k+1} = b - \sum_{i=1}^{k} \nu_i a_i$, $z_{k+1}b$ belongs to P_k. By the minimal property of λ, $\lambda \le z_{k+1}$.
  The division algorithm gives $z_{k+1} = q\lambda + r$, with $0 \le r < \lambda$.
  So $rb = z_{k+1}b - q\lambda b \in P_k$, a contradiction unless $r = 0$. Thus, $\lambda \mid z_{k+1}$.
  Let $z_{k+1} = \lambda z'_{k+1} = p^{r_{k+1}} z'_{k+1}$. The order of a_{k+1} is $\lambda = p^{r_{k+1}}$.
  So $z_{k+1}a_{k+1} = 0$. By (ii), $z_ia_i = 0$, for $i = 1, 2, \ldots, k$.
  So $P_{k+1} = \langle a_1, a_2, \ldots, a_{k+1}\rangle = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_{k+1}\rangle$.
  Since A is finite, the process must eventually terminate.
  We find $A = \langle a_1, a_2, \ldots, a_\ell\rangle = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots \oplus \langle a_\ell\rangle$.

Direct Product Representation

- In multiplicative notation, a direct sum is called a **direct product** and written $U_1 \times U_2 \times \cdots \times U_k$. We have subgroups (necessarily normal since A is abelian)
$$\{1\} = V_0 \lhd V_1 \lhd \cdots \lhd V_k = A,$$
where $V_i = U_1 \times U_2 \times \cdots \times U_i$, $i = 1, 2, \ldots, k$.

Theorem

With the above notation, $V_i / V_{i-1} \cong U_i$.

- Let $\varphi : V_i \to U_i$ be given by $\varphi(v_i) = u_i$, where $u_1 u_2 \cdots u_i$ is the unique expression of v_i as a product of elements from $U_1, U_2, \ldots, U_i$.
It is clear that φ maps onto U_i.
φ is a homomorphism. If $v_i' = u_1' u_2' \cdots u_i' \in V_i$, then
$$\varphi(v_i v_i') = \varphi[(u_1 u_1')(u_2 u_2') \cdots (u_i u_i')] = u_i u_i' = \varphi(v_i)\varphi(v_i').$$
The kernel of φ is $\{u_1 u_2 \cdots u_i : u_i = 1\} = V_{i-1}$. So $U_i \cong V_i / V_{i-1}$.

Solvability

- A finite group is called **solvable** if, for some $m \geq 0$, it has a finite series

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$

of subgroups such that, for $i = 0, 1, \ldots, m-1$:
  (i) $G_i \lhd G_{i+1}$;
  (ii) G_{i+1}/G_i is cyclic.
- Solvability is not asserting that the subgroups G_i are all normal in G.
- The representation

$$\{1\} = V_0 \lhd V_1 \lhd \cdots \lhd V_k = A,$$

where $V_i = U_1 \times U_2 \times \cdots \times U_i$, $i = 1, 2, \ldots, k$, yields:

Theorem

Every finite abelian group is solvable.

Solvability: Alternative Formulation

Theorem

A finite group G is solvable if and only if, for some $m \geq 0$, it has a finite series

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$

of subgroups such that, for $i = 0, 1, \ldots, m-1$:

(i) $G_i \lhd G_{i+1}$;

(ii) G_{i+1}/G_i is abelian.

- Since every cyclic group is abelian, the "only if" is clear.
  For the "if", suppose that we have a series as in the statement.
  For all $k = 0, \ldots, m-1$, G_{i+1}/G_i is finite abelian.
  By the preceding theorem, there exists a series

$$\{1\} = \overline{G}_{i,0} \subseteq \overline{G}_{i,1} \subseteq \cdots \subseteq \overline{G}_{i,j_i} = G_{i+1}/G_i,$$

such that $\overline{G}_{i,\ell} \lhd \overline{G}_{i,\ell+1}$ and $\overline{G}_{i,\ell+1}/\overline{G}_{i,\ell}$ is cyclic, for all $0 \leq \ell < j_i$.

Solvability: Alternative Formulation

- Thus, there exist $G_{i,\ell}$, $\ell = 0, \ldots, j_i$, such that

$$G_i = G_{i,0} \subseteq G_{i,1} \subseteq \cdots \subseteq G_{i,j_i} = G_{i+1},$$

and $G_{i,\ell} \lhd G_{i,\ell+1}$ and $G_{i,\ell+1}/G_{i,\ell} \cong \overline{G}_{i,\ell+1}/\overline{G}_{i,\ell}$ is cyclic, for all $0 \leq \ell < j_i$.

The proof is finished by interjecting these series between the G_i's in the series provided by the hypothesis to obtain

$$\begin{aligned}
\{1\} &= G_0 = G_{0,0} \subseteq G_{0,1} \subseteq \cdots \subseteq G_{0,j_0} = G_1 \\
&= G_{1,0} \subseteq G_{1,1} \subseteq \cdots \subseteq G_{1,j_1} = G_2 \\
&= G_{2,0} \subseteq G_{2,1} \subseteq \cdots \subseteq G_{2,j_2} = G_3 \\
&\vdots \\
&= G_{m-1,0} \subseteq G_{m-1,1} \subseteq \cdots \subseteq G_{m-1,j_{m-1}} = G_m.
\end{aligned}$$

Subsection 2

Sylow Subgroups

Join of Groups

- If H and K are subgroups of a group G, then the subgroup $H \vee K$, the smallest subgroup of G containing H and K, consists of all finite products
$$y = h_1 k_1 h_2 k_2 \cdots h_m k_m,$$
where $h_1, h_2, \ldots, h_m \in H$ and $k_1, k_2, \ldots, k_m \in K$.
- If at least one of the subgroups, say H, is normal, then we can rewrite $k_1 h_2$ as $h_2' k_1$, where $h_2' = k_1 h_2 k_1^{-1} \in H$.
- By repeating this argument, we can obtain an expression $h^* k^*$ for y.
- It is then natural to write $H \vee K$ as HK (or equivalently as KH).

Isomorphisms of Groups

Theorem

Let G be a group, let $N \lhd G$ and let H be a subgroup of G.

(i) $N \cap H \lhd H$ and
$$H/(N \cap H) \cong NH/N.$$

(ii) If $N \leq H$ and $H \lhd G$, then $N \lhd H$, $H/N \lhd G/N$, and
$$(G/N)/(H/N) \cong G/N.$$

(i) Let $x \in N \cap H$ and $h \in H$. Then $h^{-1}xh \in N \cap H$. So $N \cap H \lhd H$.
Let $\phi : g \mapsto Ng$ be the natural mapping from G onto G/N.
Let $\iota : H \to G$ be the inclusion mapping.
Consider the homomorphism $\phi \circ \iota : H \to G/N$.

- Its image is NH/N;
- Its kernel is $N \cap H$.

By the Homomorphism Theorem, $H/(N \cap H) \cong NH/N$.

Isomorphisms of Groups Part (ii)

(ii) Let $x \in N$ and $h \in H$. Since $N \lhd G$, $h^{-1}xh \in N$. So $N \lhd H$.
Define a mapping $\theta : G/N \to G/H$ by

$$\theta(Ng) = Hg.$$

- This is well defined: Suppose $Ng_1 = Ng_2$. Then $g_1 g_2^{-1} \in N \subseteq H$. So $Hg_1 = Hg_2$.
- It clearly maps onto G/H.
- It is a homomorphism:

$$\theta((Na)(Nb)) = \theta(N(ab)) = H(ab) = (Ha)(Hb) = [\theta(Na)][\theta(Nb)].$$

- Its kernel is $\{Ng : Hg = H\} = \{Ng : g \in H\} = H/N$.

By the Homomorphism Theorem, $(G/N)/(H/N) \cong G/H$.

Existence of Elements of Prime Divisor Order

Theorem

Let A be a finite abelian group and let p be a prime such that p divides $|A|$. Then A contains an element of order p.

- We use induction on $|A|$. The result is trivial if $|A| = p$.
  Let $|A| = p^k n$, where $k \geq 1$ and $p \nmid n$. Let M be a maximal proper subgroup of A, with order m.
  - Suppose $p \mid m$. By induction, M (and hence, of course, A) contains an element of order p.
  - Suppose $p \nmid m$. Let $v \in A \setminus M$. Suppose that the cyclic subgroup $V = \langle v \rangle$ is of order r. Now MV is a subgroup of A properly containing M. So $MV = A$. By the theorem, $A/M = MV/M \cong V/(M \cap V)$. So

$$p^k n = |A| = \frac{|M||V|}{|M \cap V|} = \frac{mr}{|M \cap V|}.$$

    Hence $p \mid r$. So the element $v^{r/p}$ has order p.

The Class Equation

- Let G be a finite group, and let $a, b \in G$.
- We say that a is **conjugate** to b if there exists x in G such that

$$x^{-1}ax = b.$$

- Conjugacy is an equivalence relation.
- Hence G is partitioned into k equivalence classes C_i, $i = 1, 2, \ldots, k$.
  - Within each C_i, every element is conjugate to every other.
  - The only element conjugate to the identity element e is e itself.
  - We suppose that $C_1 = \{e\}$.
- The **class equation** of G is the arithmetical equality deriving from the partition:

$$|G| = 1 + |C_2| + \cdots + |C_k|.$$

- In an abelian group the notion of conjugacy is not useful, since elements are conjugate only if they are equal.

The Centralizer

- Let G be a group and a an element of G.
- The **centralizer** $Z(a)$ is defined to be the set of all g in G such that

$$ga = ag.$$

Proposition

Let G be a group and $a \in G$. $Z(a)$ is a subgroup of G.

- Let $g, g' \in Z(a)$. By definition, $ga = ag$ and $g'a = ag'$.
  The second gives $g'^{-1}a = ag'^{-1}$. So $g'^{-1} \in Z(a)$.
  Finally, we obtain

$$(gg')a = g(g'a) = g(ag') = (ga)g' = (ag)g' = a(gg').$$

  So $gg' \in Z(a)$. It follows that $Z(a)$ is a subgroup of G.

Conjugacy Classes and the Centralizer

- For $a \in G$, $C(a) = \{x^{-1}ax : x \in G\}$, the conjugacy class of a.

Lemma

Let G be a group and $a \in G$. The number of elements in $C(a)$ is equal to the index of $Z(a)$ in G.

- By definition, $C(a) = \{x^{-1}ax : x \in G\}$. For $x, y \in G$, we have

$$\begin{array}{rll} x^{-1}ax = y^{-1}ay & \text{iff} & axy^{-1} = xy^{-1}a \\ & \text{iff} & xy^{-1} \in Z(a) \\ & \text{iff} & Z(a)x = Z(a)y. \end{array}$$

Thus, the number of distinct elements in $C(a)$ is equal to the number of distinct cosets of $Z(a)$.

Corollary

Let G be a group. Then $|C(a)|$ divides $|G|$, for all $a \in G$.

The Center

- The **center** of a group G is the set

$$Z = Z(G) = \{z \in G : (\forall\ g \in G)\ zg = gz\}.$$

- Alternatively, Z is the set of elements z of G for which $Z(z) = G$.

Proposition

Let G be a group. Every subgroup U of G contained in $Z(G)$ (including $Z(G)$ itself) is normal.

- Suppose $u \in U$ and $g \in G$. Then, since $u \in Z(G)$, we have

$$g^{-1}ug = g^{-1}gu = u \in U.$$

  So U is a normal subgroup of G.
- Note that $a \in Z$ if and only if $C(a) = \{a\}$.

The Center of p-Groups

Theorem

If G is a group of order p^m, where p is prime and m is a positive integer, then $Z(G)$ is non-trivial.

- The class equation gives $p^m = 1 + |C_2| + \cdots + |C_k|$.

  So $1 + |C_2| + \cdots + |C_k|$ is divisible by p.

  But, by a previous corollary, each $|C_i|$ divides p^m.

  So $|C_i| = 1$, for at least $p-1$ values of i in $\{2, \ldots, k\}$.

  Hence, $|Z(G)| \geq p$.

Existence of Sylow Subgroups

Theorem

Let G be a finite group of order $p^\ell r$, where p is prime and $p \nmid r$. Then G has at least one subgroup of order p^ℓ.

- We use induction on $|G|$, the result being clear if $|G| = 1$ or 2.
  Consider the class equation
  $$p^\ell r = |G| = c_1 + c_2 + \cdots + c_k,$$
  where $c_i = |C_i|, i = 1, 2, \ldots, k$.
  By a previous corollary, c_i is equal to $\frac{|G|}{|Z_i|}$, where Z_i is the centralizer in G of a typical element of C_i.
  Writing z_i for the order of Z_i, we get $z_i = \frac{p^\ell r}{c_i}$, $i = 1, 2, \ldots, k$.
  - Suppose, first, that there exists $c_i > 1$ such that $p \nmid c_i$.
    Then $z_i < p^\ell r$ and is divisible by p^ℓ.
    By the induction hypothesis, Z_i contains a subgroup of order p^ℓ.

Existence of Sylow Subgroups (Cont'd)

- Now assume, for all i in $\{1,2,\ldots,k\}$, either $c_i = 1$ or p divides c_i.
  The union of the classes C_i, with $c_i = 1$, is the center Z of G.
  So $p^\ell r = |Z| + vp$, for some integer v.
  Hence Z is non-trivial, with order divisible by p.
  But Z is abelian. So, it contains an element a of order p.
  Since Z is normal, the cyclic subgroup $\langle a\rangle$ is certainly normal.
  Moreover, $|G/\langle a\rangle| = p^{\ell-1}r$.
  By induction, $G/\langle a\rangle$ contains a subgroup $U/\langle a\rangle$ of order $p^{\ell-1}$.
  So G contains a subgroup U of order p^ℓ.
- The subgroup U is called a **Sylow subgroup**.

The Cauchy Theorem

Corollary (Cauchy)

Let G be a finite group and let p be a prime such that p divides $|G|$. Then G contains an element of order p.

- We have seen that G has a subgroup H of order p^ℓ.

  A typical element v of H has order p^k, where $k \leq \ell$.

  It is then clear that $v^{p^{k-1}}$ has order p.
- The preceding theorem is, actually, only part of Sylow's Theorem.

Tower of Normal Subgroups of Power p Order

Theorem

Let G be a group of order p^m, where p is prime and m is a positive integer. Then there exist normal subgroups

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = G$$

of G such that $|H_i| = p^i$, for $i = 0, 1, \ldots, m$.

- G must contain an element of order p. The order of any $a \neq e$ in G is p^r for some r in $\{1, 2, \ldots, m\}$. So $a^{p^{r-1}}$ is of order p.

  For $m = 1$, there is nothing to prove. Let $m \geq 2$. Suppose inductively that the result holds for all $k < m$. Let $|G| = p^m$.

  By a previous theorem, we may suppose that there is a subgroup P of order p contained in the center $Z(G)$.

Tower of Normal Subgroups of Power p Order (Cont'd)

- Consider a subgroup P of order p contained in the center $Z(G)$.

  Then P is normal and we have $|G/P| = p^{m-1}$.

  Every normal subgroup $\overline{N}$ of G/P may be written as N/P, where N is a normal subgroup of G containing P.

  By induction, there exist normal subgroups K_i, all containing P, such that

  $$\{e\} = K_0/P \subset K_1/P \subset \cdots \subset K_{m-1}/P = G/P,$$

  with $|K_i/P| = p^i, i = 1, 2, \ldots, m-1$.

  Define $H_0 = \{e\}$, $H_1 = P$ and $H_i = K_{i-1}$, $i = 2, \ldots, m$.

  We obtain normal subgroups H_i of G, such that

  $$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = G,$$

  with $|H_i| = p^i, i = 0, 1, \ldots, m$.

Subsection 3

Permutation Groups

Symmetric Groups

- Let S_n be the **symmetric group on n symbols**.
  - Its elements are all one-to-one mappings (permutations) of the set $\{1,2,\ldots,n\}$ onto itself;
  - The operation is composition of mappings.
- The composition of two permutations π_1 and π_2 is called their **product**.
- $\pi_1\pi_2$ is interpreted as "first π_1, then π_2".
- A **cycle** of length k, written $\sigma = (a_1\ a_2\ \cdots\ a_k)$ is a permutation such that

$$a_1\sigma = a_2,\ a_2\sigma = a_3,\ \ldots,\ a_{k-1}\sigma = a_k,\ a_k\sigma = a_1$$

and $x\sigma = x$, for each x not in the set $\{a_1, a_2, \ldots, a_k\}$.

The Cycle Decomposition

Theorem

Every π in S_n can be expressed as a product of disjoint cycles. The order of π is the least common multiple of the lengths of the cycles.

- Let x_1 be an arbitrarily chosen element of $\{1,2,\ldots,n\}$. If $x_1\pi = x_1$, then (x_1) is itself a cycle. Otherwise, write $x_1\pi$ as x_2. We continue with a sequence $x_1, x_2 = x_1\pi, x_3 = x_2\pi, \ldots$. Since the set $\{1,2,\ldots,n\}$ is finite, there must eventually be a repetition. Suppose that the first repetition is $x_k\pi = x_j$, with $k > j$. Suppose $j \neq 1$. Then $x_{j-1}\pi = x_k\pi = x_j$. This contradiction gives $j = 1$. So the restriction of π to $\{x_1, x_2, \ldots, x_k\}$ is the cycle $(x_1\ x_2\ \cdots\ x_k)$.

  Now choose y_1 not in $\{x_1, x_2, \ldots, x_k\}$ and repeat the process. We obtain a cycle $(y_1\ y_2\ \cdots\ y_1)$. Eventually this process ends.

  We, thus, obtain the decomposition of π into disjoint cycles.

The Cycle Decomposition (Cont'd)

- It is clear that the order of a cycle coincides with its length.

  Moreover, disjoint cycles commute with each other.

  Let π be the product $\sigma_1\sigma_2\cdots\sigma_r$ of disjoint cycles of lengths $\lambda_1,\lambda_2,\ldots,\lambda_r$.

  Then, for each $m \geq 1$,

$$\pi^m = \sigma_1^m\sigma_2^m\cdots\sigma_r^m.$$

  This is equal to the identity permutation if and only if m is a multiple of each of the integers $\lambda_1,\lambda_2,\ldots,\lambda_r$.
- The decomposition into disjoint cycles is in effect unique.
  - The cycles can begin with any one of their entries;
  - The order of the cycles is arbitrary.

Transpositions

- A cycle of length 2 is called a **transposition**.

Corollary

Every permutation can be expressed as a product of transpositions.

- In view of the theorem, we need only show that a cycle is a product of transpositions.

  It is easy to verify that

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

  - $a_1 \xrightarrow{(a_1\ a_2)} a_2$;
  - $a_i \xrightarrow{(a_1\ a_i)} a_1 \xrightarrow{(a_1\ a_{i+1})} a_{i+1}, \quad i \leq 2 \leq k-1$;
  - $a_k \xrightarrow{(a_1\ a_k)} a_1$.

Even and Odd Permutations

- Consider the polynomial

$$\begin{aligned}\Delta(X_1,\ldots,X_n) &= \prod_{1\le i<j\le n}(X_i - X_j) \\ &= (X_1-X_2)(X_1-X_3)\cdots(X_1-X_n) \\ &\qquad (X_2-X_3)\cdots(X_2-X_n) \\ &\qquad\qquad \cdots \\ &\qquad\qquad (X_{n-1}-X_n).\end{aligned}$$

  of degree $(n-1)+(n-2)+\cdots+1=\frac{1}{2}n(n-1)$.
- For each permutation π in the symmetric group S_n, we may define

$$\pi(\Delta)=\prod_{1\le i<j\le n}(X_{\pi(i)}-X_{\pi(j)}).$$

- The factors in $\pi(\Delta)$ are the same as the factors in Δ, except that they are in a different order, and some of them may be reversed.
- A permutation π is **even** or **odd** according as $\pi(\Delta)=\Delta$ or $\pi(\Delta)=-\Delta$.

The Alternating Group

- A permutation π is even [odd] if and only if it is expressible as a composition of an even [odd] number of transpositions.
- It follows that

$$\text{even} \cdot \text{even} = \text{even}, \ \text{even} \cdot \text{odd} = \text{odd} \cdot \text{even} = \text{odd}, \ \text{odd} \cdot \text{odd} = \text{even}.$$

- Consequently the set of all even permutations is a subgroup, indeed a normal subgroup, of S_n, called the **alternating group**, and denoted by A_n.
- For any transposition $(x_1 \ x_2)$, the coset $A_n(x_1 \ x_2)$ is precisely the set of odd permutations.
  - The coset $A_n(x_1 \ x_2)$ consists entirely of odd permutations.
  - Let π be an odd permutation. Then π can be written as $(\pi(x_1 \ x_2))(x_1 \ x_2)$, with $\pi(x_1 \ x_2)$ even. So π is in $A_n(x_1 \ x_2)$.
- So A_n is of index 2 in S_n and of order $\frac{1}{2}n!$.

Solvability of S_3

Theorem

The symmetric group S_3 is solvable.

- S_3 consists of the permutations

$$e = 1,\ a = (1\ 2\ 3),\ b = (1\ 3\ 2),\ x = (2\ 3),\ y = (1\ 3),\ z = (1\ 2).$$

S_3 has a normal subgroup $H = \{e, a, b\}$.

Both H and S/H are cyclic.

Thus S_3 is solvable.

Solubility of S_4

Theorem

The symmetric group S_4 is solvable.

- The alternating group A_4 is a subgroup of index 2 and is normal.
  The quotient S_4/A_4, being a group of order 2, is assuredly cyclic.
  The alternating group consists of the identity, together with:
  $$(1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 2),\ (1\ 3\ 4),\ (1\ 4\ 2),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3),$$
  $$(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3).$$
  The set $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is an abelian subgroup of A_4 (the Klein 4-group). Its right and left cosets are V,
  $V(1\ 2\ 3) = (1\ 2\ 3)V = \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}$,
  $V(1\ 2\ 4) = (1\ 2\ 4)V = \{(1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4)\}$.
  So $V \lhd A_4$. The quotient A_4/V, being of order 3, is cyclic.
  We thus have $1 \lhd V \lhd A_4 \lhd S_4$, with $V/1, A_4/V, S_4/A_4$ cyclic.

Alternating Group and Cycles of Length 3

Lemma

For all $n \geq 3$, the alternating group A_n is generated by the set of all cycles of length 3.

- It is clear that A_n is generated by the set of elements of type $(a\ b)(c\ d)$.
  - If the two transpositions are equal, their product is the identity.
  - If the product is of the form $(a\ b)(a\ c)$, where a, b, c are distinct, then we see that $(a\ b)(a\ c) = (a\ b\ c)$;
  - If a, b, c, d are all distinct, then

$$(a\ b)(c\ d) = [(a\ b)(a\ c)][(c\ a)(c\ d)] = (a\ b\ c)(c\ a\ d).$$

Simplicity of A_n, $n \geq 5$

- A non-abelian group is called **simple** if it has no proper normal subgroups.
- Such a group is certainly not solvable.

Theorem

For all $n \geq 5$, the alternating group A_n is simple.

- Let $N \neq \{1\}$ be a normal subgroup of A_n. We shall show that N contains every cycle of length 3. Then, by the lemma, $N = A_n$.
  Case 1: Suppose that N contains a cycle $(a\ b\ c)$ of length 3.
  Let x, y, z be distinct elements in $\{1, 2, \ldots, n\}$ and $\alpha = \begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix}$.
  Then $\alpha^{-1}(a\ b\ c)\alpha = (x\ y\ z)$.
  - If α is even, this implies that $(x\ y\ z) \in N$.
  - If α is odd, replace it by the even permutation $\beta = (d\ e)\alpha$, where $d, e \notin \{a, b, c\}$ (possible since $n \geq 5$). Observe $\beta^{-1}(a\ b\ c)\beta = (x\ y\ z)$.

  Hence N contains all cycles of length 3. So $N = A_n$.

Simplicity of A_n, $n \geq 5$ (Cont'd)

Case 2: Next, suppose N contains an element π which decomposes into disjoint cycles as $\pi = \kappa_1 \kappa_2 \cdots \kappa_r$. Suppose that one of the cycles, which we may, without loss of generality, take as κ_1, is of length $s \geq 4$: $\kappa_1 = (a_1\ a_2\ \cdots\ a_s)$.

Let $\alpha = (a_1\ a_2\ a_3)$. Then $\alpha^{-1}\pi\alpha = (\alpha^{-1}\kappa_1\alpha)\kappa_2 \cdots \kappa_r$, since only κ_1 is affected by the conjugation. Moreover,

$$\begin{array}{rcl} \alpha^{-1}\kappa_1\alpha & = & (a_1\ a_3\ a_2)(a_1\ a_2\ \cdots\ a_s)(a_1\ a_2\ a_3) \\ & = & (a_2\ a_3\ a_1\ a_4\ a_5\ \cdots\ a_s). \end{array}$$

The element $\pi^{-1}\alpha^{-1}\pi\alpha$ belongs to N. We have

$$\begin{array}{rcl} \pi^{-1}\alpha^{-1}\pi\alpha & = & \kappa_1^{-1}\alpha^{-1}\kappa_1\alpha \\ & = & (a_s\ a_{s-1}\ \cdots\ a_1)(a_2\ a_3\ a_1\ a_4\ a_5\ \cdots\ a_s) \\ & = & (a_1\ a_2\ a_4). \end{array}$$

We are back in Case 1. So $N = A_n$.

Simplicity of A_n, $n \geq 5$ (Cont'd)

- **Case 3**: Suppose all the elements of N have cycle decompositions involving only cycles of length 2 and 3.
  - Suppose π contains only one cycle $(a\ b\ c)$ of length 3 (the other cycles being of length 2). Then $\pi^2 = (a\ c\ b) \in N$. We are back in Case 1.
  - Suppose that π contains at least two disjoint cycles $(a\ b\ c)$ and $(d\ e\ f)$ of length 3. Then N contains

$$\begin{array}{rcl} \pi' & = & (e\ d\ c)\pi(e\ c\ d) \\ & = & (e\ d\ c)(a\ b\ c)(d\ e\ f)(e\ c\ d)\cdots \\ & = & (a\ b\ d)(c\ f\ e)\cdots. \end{array}$$

    So it contains

$$\pi\pi' = (a\ b\ c)(d\ e\ f)\cdots(a\ b\ d)(c\ f\ e)\cdots = (a\ d\ c\ b\ f)\cdots.$$

    We are back in Case 2. So $N = A_n$.

Simplicity of A_n, $n \geq 5$ (Conclusion)

- **Case 3** (Cont'd):
  - The final case is where π is a product of a (necessarily even) number of transpositions.
    - Suppose first that there are just two: $\pi = (a\ b)(c\ d)$. Then there is at least one other symbol e, since we are assuming that $n \geq 5$. So N contains the element

      $$\pi[(a\ b\ e)^{-1}\pi(a\ b\ e)] = (a\ b)(c\ d)(a\ e\ b)(a\ b)(c\ d)(a\ b\ e) = (a\ e\ b).$$

      Again we are back in Case 1.
    - Suppose finally that $\pi = (a\ b)(c\ d)(e\ f)(g\ h)\cdots$. Then N contains

      $$\begin{aligned} \pi[(b\ c)^{-1}(d\ e)^{-1}\pi(d\ e)(b\ c)] &= \pi(b\ c)(d\ e)\pi(d\ e)(b\ c) \\ &= (a\ e\ d)(b\ c\ f)\cdots. \end{aligned}$$

      Once again we are back in a case already considered.

Generation of S_n

Theorem

The symmetric group S_n is generated by the cycles $(1\ 2)$ and $(1\ 2\ \cdots\ n)$.

- Let $\tau = (1\ 2)$ and $\zeta = (1\ 2\ \cdots\ n)$.
  Then $\zeta^{-1} = \zeta^{n-1} = (n\ n-1\ \cdots\ 2\ 1)$.
  So $\zeta^{-1}\tau\zeta = (n\ n-1\ \cdots\ 1)(1\ 2)(1\ 2\ \cdots\ n) = (2\ 3)$.
  Claim: For all $i = 1, \ldots, n-1$, $\zeta^{-i+1}\tau\zeta^{i-1} = (i\ i+1)$.
  Suppose $j \notin \{i, i+1\}$. Then we have, modulo n,

  $$j\zeta^{-i+1}\tau\zeta^{i-1} = (j-i+1)\tau\zeta^{i-1} = (j-i+1)\zeta^{i-1} = j.$$

  On the other hand,

  $$\begin{array}{rcl} i\zeta^{-i+1}\tau\zeta^{i-1} & = & 1\tau\zeta^{i-1} = 2\zeta^{i-1} = i+1; \\ (i+1)\zeta^{-i+1}\tau\zeta^{i-1} & = & 2\tau\zeta^{i-1} = 1\zeta^{i-1} = i. \end{array}$$

Generation of S_n (Cont'd)

Claim: For $j = 2, 3, \ldots, n-1$,

$$(j\ j+1)(j-1\ j)\cdots(2\ 3)(1\ 2)(2\ 3)\cdots(j\ j+1) = (1\ j+1).$$

Claim: For $i = 1, 2, \ldots, n-1$ and $j = 1, 2, \ldots, n-i$,

$$\zeta^{-i+1}(1\ j+1)\zeta^{i-1} = (i\ \ i+j).$$

We have

$$\begin{array}{rcl} i\zeta^{-i+1}(1\ j+1)\zeta^{i-1} & = & 1(1\ j+1)\zeta^{i-1} = (j+1)\zeta^{i-1} = i+j; \\ (i+j)\zeta^{-i+1}(1\ j+1)\zeta^{i-1} & = & (j+1)(1\ j+1)\zeta^{i-1} = 1\zeta^{i-1} = i. \end{array}$$

All other members of $\{1, 2, \ldots, n\}$ map to themselves.

We have shown that τ and ζ generate all transpositions in S_n.

By a previous corollary, they generate the whole of S_n.

Subsection 4

Properties of Solvable Groups

Properties of Solvable Groups

- Recall that a group G is **solvable** if, for some $m \geq 0$, it has a finite series
$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m = G$$
of subgroups such that, for $i = 0, 1, \ldots, m-1$,
  (i) $G_i \lhd G_{i+1}$;
  (ii) G_{i+1}/G_i is cyclic.

Theorem

Let G be a group.

(i) If G is solvable, then every subgroup of G is solvable.

(ii) If G is solvable and N is a normal subgroup of G, then G/N is solvable.

(iii) Let $N \lhd G$. Then G is solvable if and only if both N and G/N are solvable.

Proof of Property (i)

(i) Suppose that

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_m = G,$$

and that G_{i+1}/G_i is cyclic for $i = 1, 2, \ldots, m-1$.
Let H be a subgroup of G. For each i, let $K_i = H \cap G_i$. Then

$$K_i = H \cap (G_{i+1} \cap G_i) = (H \cap G_{i+1}) \cap G_i = K_{i+1} \cap G_i.$$

By a preceding theorem, $K_i \lhd K_{i+1}$. We have

$$K_{i+1}/K_i = K_{i+1}/(K_{i+1} \cap G_i) \cong K_{i+1}G_i/G_i.$$

Since $K_{i+1}G_i/G_i$ is a subgroup of the cyclic group G_{i+1}/G_i, it is cyclic (or trivial). So the sequence

$$\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_m = H$$

has the required properties.

Proof of Property (ii)

(ii) With G defined as before, it is clear that G/N has a series

$$N/N = G_0N/N \lhd G_1N/N \lhd \cdots \lhd G_mN/N = G/N.$$

There may be coincidences in this series - for example, if $G_1 \subseteq N$, then $G_1N/N = N/N$ - but this causes no problem.

Using a previous theorem, we can transform a typical quotient:

$$\frac{G_{i+1}N/N}{G_iN/N} \cong \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}.$$

The quotient, being isomorphic to a factor group of the cyclic group G_{i+1}/G_i is certainly cyclic.

Proof of Property (iii)

(iii) From Parts (i) and (ii), if G is soluble, N and G/N are soluble.
Suppose, conversely, that N and G/N are solvable.
Then there are:

- A series
$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_p = N,$$
in which N_{i+1}/N_i is cyclic for $i = 0, 1, \ldots, p-1$;
- A series
$$\{1\} = N/N = G_0/N \lhd G_1/N \lhd \cdots \lhd G_m/N = G/N,$$
such that $G_i \lhd G_{i+1}$ and $G_{i+1}/G_i \cong (G_{i+1}/N)/(G_i/N)$ is cyclic, for $i = 0, 1, \ldots, m-1$.

Hence, there is a series
$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_p = N = G_0 \lhd G_1 \lhd \cdots \lhd G_p = G.$$
So G is solvable.

Non-Solvability of S_n, $n \geq 5$

Corollary

For all $n \geq 5$, the symmetric group S_n is not solvable.

- If S_n were solvable, then all its subgroups would be solvable.
  We know that A_n is simple.
  So it is certainly not solvable.