INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the original text directly from the copy submitted. Thus, some dissertation copies are in typewriter face, while others may be from a computer printer.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyrighted material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each oversize page is available as one exposure on a standard 35 mm slide or as a 17″ × 23″ black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. 35 mm slides or 6″ × 9″ black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Accessing the World's Information since 1938

300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

Order Number 8821119

Group invariant finite Fourier transforms

Shenefelt, Myoung Hee, Ph.D.

City University of New York, 1988

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

PLEASE NOTE:

In all cases this material has been filmed in the best possible way from the available copy. Problems encountered with this document have been identified here with a check mark __✓__.

1. Glossy photographs or pages _____
2. Colored illustrations, paper or print _____
3. Photographs with dark background _____
4. Illustrations are poor copy _____
5. Pages with black marks, not original copy ___✓___
6. Print shows through as there is text on both sides of page _____
7. Indistinct, broken or small print on several pages ___✓___
8. Print exceeds margin requirements _____
9. Tightly bound copy with print lost in spine _____
10. Computer printout pages with indistinct print _____
11. Page(s) _____ lacking when material received, and not available from school or author.
12. Page(s) _____ seem to be missing in numbering only as text follows.
13. Two pages numbered _____. Text follows.
14. Curling and wrinkled pages _____
15. Dissertation contains pages with print at a slant, filmed as received _____
16. Other _____

_____

_____

GROUP INVARIANT

FINITE FOURIER TRANSFORMS

by

MYOUNG SHENEFELT

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1988

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

4/12/1988
date

Chairman of Examining Committee

4/12/1988
date

Executive Officer

Louis Auslander

Alphonse Vasquez

Alex Heller

Supervisory Committee

Abstract

GROUP INVARIANT

FINITE FOURIER TRANSFORMS

by

Myoung Shenefelt

Adviser : Professor Louis Auslander

The computation of the finite Fourier transform of functions is one of the most used computations in crystallogrphy. Since the Fourier transform involved is 3–dimensional, the size of the computation becomes very large even for relatively few sample points along each edge. In this thesis, there is a family of algorithms that reduce the computation of Fourier transform of functions respecting the symmetries. Some properties of these algorithms are :

1) The algorithms make full use of the group of symmetries of a crystal.

2) The algorithms can be factored and combined according to the prime factorization of the number of points in the sample sapce.

3) The algorithms are orginized into a family using the group structure of the crystallographic groups to make iterative procedures possible.

TABLE OF CONTENTS

Introduction.

One of the most used computations in crystallogrphy is the computation of the finite Fourier transform of a function that satisfies the symmetries of a crystallographic group. Since the Fourier transform involved is 3–dimensional, the size of the computation becomes very large even for relatively few sample points along each edge. For instance a Fourier transform on $60 \times 60 \times 60$ points requires the same arithmetic operations as a 1–dimensional Fourier transform on $60 \times 60 \times 60$ points, or 216,000 points. Since in modern macromolecular work, people use Fourier transform of the size $200 \times 200 \times 200$ points, or 8,000,000 points, it becomes clear that any method that would reduce the computational cost is important.

Lyn Ten Eyk [4] was the first person to propose algorithms that take advantage of crystallographic symmetries to reduce arithmetic cost in Fourier transform computations. This was followed by some work of R. Agarwal and G. Bricogne, but no general program to attack this problem has been undertaken until the recent work at the Center for Large Scale Computation of C.U.N.Y. and collaborative work by J. Cooley at I.B.M. Watson Research Center.

J. Cooley developed a method, called the *orbit exchange method*, for studying this problem for crystallographic group $P3$. This consists of 120° rotations about an axis. The Fourier transform of functions invariant under this group had never been studied before. When J. Cooley programmed his algorithm on an I.B.M. 3090 for a function on $60 \times 60 \times 60$ points he obtained a 5–fold increse in computational speed over the same computation without symmetry.

However the group $P3$, being a simple group, has a particularly "simple" orbit structure. It was not clear how to extend the orbit exchange method to more complicated groups. Further, since there are 230 crystallographic groups, it was particularly pressing to find a method whereby a solution for one group could be used to find solutions for other groups.

Since crystallographic groups are solvable, it was reasonable to choose a large crystallographic group and use its solvable structure and study the orbit exchange method for both the large proup and for its subgroups simultaneously. We choose $P622$, a group of order 12, as our large group. It has 6 crystallographic subgroups, and we should solve the orbit exchange for all of these groups, but in such a way that, once a problem is solved for one group, it helps to solved the orbit exchange method for other groups.

This thesis is organized as follows.

Chapter 1 Review of basic facts and discussion of J. Cooley's orbit exchange method for $P3$ and a general formulation of the method.

Chapter 2 A study of the group $P622$ and its subgroups. Of particular importance for us are the concepts of conjugate subgroups and complementary pairs of subgroups and their structure.

Chapter 3 A study of orbit decomposition and its subgroups. This chapter contains the bulk of the technical work of this thesis. We introduce several new concepts to relate the orbit structure of $P622$ to its subgroups. Theorem 19 and the Main Theorem are the major new technical results of this thesis.

Chapter 4 Computation of Fourier Transform coefficients using the group structure.

Chapter 5 In this chapter we use the Main Theorem to prove that (a) all subgroups of $P622$ have an orbit exchange method, and that (b) the solution for $P622$ can be construction so as to give solutions for the subgroups of $P622$.

List of symbols

ϕ : the empty set.

$A < B$: A is a subgroup of B.

$A \lhd B$: A is a normal subgroup of B.

$ord(A)$: the order of the group (or the set) A.

I : the identity element or the group consisting of the identity element.

I_n : the $n \times n$ identity matrix for a natural number n.

1. Outline of Approach.

Because our work involves many details, we will begin with an overview of our approach to the problem.

For a positive integer n, let $L(n)$ denote the space of functions on $(Z/n)^3$, where Z denotes the integers and $(Z/n)^3 = Z/n \times Z/n \times Z/n$. Define the mapping $\omega_n^{<\cdot,>}$ from $(Z/n)^3 \times (Z/n)^3$ onto the nth roots of unity as follows : For x^*, $x \in (Z/n)^3$,

$$\omega_n^{<x^*,x>} = exp(\tfrac{2\pi i}{n} \cdot k),$$

where k is an integer belonging to the coset $\sum_{i=1}^{3} x_i^* \cdot x_i + nZ$.

Since $exp(\frac{2\pi i}{n} \cdot k) = exp(\frac{2\pi i}{n} \cdot (k+n))$, $\omega_n^{<\cdot,>}$ is well defined.

The *Finite Fourier Transform*, $F(n) : L(n) \longrightarrow L(n)$ is defined for $f \in L(n)$ by

$$F(n)f(x^*) = \sum_{x \in (Z/n)^3} f(x) \cdot \omega_n^{<x^*,x>}. \tag{1}$$

Notation We will denote $F(n)f$ by $\hat{f}$.

A mathematical way of describing a point group $\mathcal{G}$ is as an integer unimodular equivalence class of representations in $SL(3,Z)$ of an abstract finite group. For convenience, we will use G to denote a fixed representation. Considering the elements of $(Z/n)^3$ as column vectors, we may view $SL(3,Z)$ as acting on $(Z/n)^3$, where the action is the matrix multiplication followed by reduction of the entries *modulo n*. In this way, we will view G as acting on $(Z/n)^3$. Throughout this thesis, we will use G to denote a finite group of automorphisms of $(Z/n)^3$, unless otherwise specified.

Definition For $x \in (Z/n)^3$, the set $\{gx \mid g \in G\}$, denoted by $G(x)$, is called the $G-$orbit of x. Also, the subgroup $Iso_G(x) = \{g \in G \mid gx = x\}$ is called the *isotropy subgroup* in G at x.

Notation For a subset X of $(Z/n)^3$, we will denote by $G(X)$ the set $\cup_{x \in X} G(x)$.

Definition A subset X of $(Z/n)^3$ is called a *$G-$fundamental domain* in $(Z/n)^3$ if

$G(X) = (Z/n)^3$, and for any x, $x' \in X$, and $x \neq x'$, $G(x) \cap G(x') = \phi$.

We will denote a $G-$fundamental domain in $(Z/n)^3$ by $G-fd(n)$. We can determine a $G-fd(n)$ by first decomposing $(Z/n)^3$ into $G-$orbits, then choosing one element from each $G-$orbit. Note that $G - fd(n)$ is not unique.

Theorem 1 For $x \in (Z/n)^3$, there is a bijection between $G/Iso_G(x)$ and $G(x)$.

Proof Let $g_1 Iso_G(x)$, $g_2 Iso_G(x)$, ..., $g_k Iso_G(x)$ be the coset decomposition of G by $Iso_G(x)$. We will show that the mapping $\theta : g_j Iso_G(x) \longrightarrow g_j x$, $1 \leq j \leq k$ from the left cosets of $Iso_G(x)$ in G to $G(x)$ is a bijection. If $g_j x = g_l x$, for g_j, $g_l \in G$, then $g_l^{-1} g_j \in Iso_G(x)$ which implies that $g_j Iso_G(x) = g_l Iso_G(x)$ and θ is an injection. On the other hand, any element of $G(x)$ is of the form gx for some $g \in G$. If $g_j Iso_G(x)$ is the coset to which g belongs, then $g = g_j h$, for some $h \in Iso_G(x)$. $gx = ghx = g_j x$. Thus, θ is a surjection.

Let $C_G(x)$ be a set of coset representatives of $Iso_G(x)$. By the bijective correspondence between $G(x)$ and $C_G(x)$, we have that $G(x) = \{c_1 x, c_2 x, \ldots, c_j x\}$, where $\{c_1, c_2, \ldots, c_j\} = C_G(x)$. Let $G(x_1)$, $G(x_2)$, ..., $G(x_k)$ be the $G-$orbit decomposition of $(Z/n)^3$. Then $\{x_1, x_2, \ldots, x_k\}$ is a $G-$fundamental domain in $(Z/n)^3$. Thus, $(Z/n)^3 = \cup_{x_j \in G-fd(n)} C_G(x_j)(x_j)$. We can rewrite (1) as

$$\hat{f}(x^*) = \sum_{x_j \in G-fd(n)} \Big(\sum_{c \in C_G(x_j)} f(cx_j) \cdot \omega_n^{<x^*, cx_j>} \Big). \tag{2}$$

Definition $f \in L(n)$ is said to be *$G-$invariant*, if for $x \in (Z/n)^3$, and $g \in G$, $f(x) = f(gx)$. We will denote the collection of $G-$invariant functions in $L(n)$ by $L_G(n)$.

For a $G-$invariant function f, if we know $f(x)$ for $x \in G - fd(n)$, then we know $f(x)$ for all $x \in (Z/n)^3$. This is because if $x \in (Z/n)^3$, then either x is an element of $G - fd(n)$ or it is a $G-$image of an element in $G - fd$. Since $f(x) = f(cx)$ for $f \in L_G(n)$ and $c \in C_G(x)$, we can rewrite (2) as

$$\hat{f}(x^*) = \sum_{x_j \in G-fd(n)} f(x_j) \Big(\sum_{c \in C_G(x_j)} \omega_n^{<x^*, cx_j>} \Big).$$

Lemma 1 Let $T \in GL(3, Z/n)$, and denote the transpose of T by T^t. Then

$< T(x), y > = < x, T^t(y) >$, for x, $y \in (Z/n)^3$.

Proof Let the coordinates of T be (T_{jk}), j, k = 1, 2, 3. Let $x = (x_1, x_2, x_3)^t$ and $y = (y_1, y_2, y_3)^t$.

$< Tx, y > = \sum_{j=1}^{3}(\sum_{k=1}^{3} T_{jk}x_k)y_j = \sum_{j=1}^{3}(\sum_{k=1}^{3} T_{jk}x_k y_j) = \sum_{k=1}^{3}(\sum_{j=1}^{3} T_{jk}y_j x_k)$.

Notice now $(\sum_j T_{j1}y_j, \sum_j T_{j2}y_j, \sum_j T_{j3}y_j)^t = T^t(y)$, where the sum is over j = 1, 2, 3. Hence

$$< T(x), y) > = < T^t(y), x > = < x, T^t(y) >.$$

For $g \in SL(3, Z)$, we will use g^* to denote $(g^{-1})^t$. Let $G^* = \{(g^{-1})^t \mid g \in G\}$. G^* is also a group, and it is isomorphic to G. G^* is called the *contragradient representation.*

Theorem 2 $F(n) : L_G(n) \longrightarrow L_{G^*}(n)$.

Proof For $f \in L_G(n)$ and $x^* \in (Z/n)^3$, $\hat{f}(g^*x^*) = \sum_{x \in (Z/n)^3} f(x) \cdot \omega_n^{<g^*x^*, x>}$. By Lemma 1,

$\hat{f}(g^*x^*) = \sum_{x \in (Z/n)^3} f(x) \cdot \omega_n^{<x^*, g^t x>} = \sum_{x \in (Z/n)^3} f(x) \cdot \omega_n^{<x^*, g^{-1}x>}$.

Since g is an automorphism, we may replace x by gx. Also, since $f(x) = f(gx)$,

$\hat{f}(g^*x^*) = \sum_{gx \in (Z/n)^3} f(gx) \cdot \omega_n^{<x^*, x>} = \sum_{gx \in (Z/n)^3} f(x) \cdot \omega_n^{<x^*, x>}$.

As gx ranges over$(Z/n)^3$, x ranges over $(Z/n)^3$, and we have

$$\hat{f}(g^*x^*) = \sum_{x \in (Z/n)^3} f(x) \cdot \omega_n^{<x^*, x>} = \hat{f}(x^*).$$

G^* acting on $(Z/n)^3$ decomposes $(Z/n)^3$ into disjoint G^*−orbits. Again by choosing one element from each distinct G^*−orbit, we find a G^*−fundamental domain $G^* - fd(n)$. If we know $F(n)f(x^*)$ for $x^* \in G^* - fd(n)$, then we know $F(n)f(x^*)$ for all $x^* \in (Z/n)^3$. We now define the *G−invariant Fourier Transform*, $F_G(n) : L_G(n) \longrightarrow L_{G^*}(n)$ as follows. For $x^* \in G^* - fd(n)$,

$$F_G(n)f(x^*) = \sum_{x \in G - fd(n)} f(x)\mathcal{F}_G(x^*, x),$$

where

$$\mathcal{F}_G(x^*, x) = \sum_{c \in C_G(x)} \omega_n^{<x^*, cx>}. \tag{3}$$

By ordering the elements of $G^* - fd(n)$ and $G - fd(n)$, we can by (3) represent $F_G(n)$ as a matrix. A matrix representation of the G-invariant Finite Fourier Transform of functions in $L_G(n)$ will be denoted by $\mathcal{F}_G(n)$. Using the ordering fixed above, let $[X]_G$ and $[X^*]_{G^*}$ be column

vectors of entries $f(x)$, $x \in G - fd(n)$ and $F_G(n)f(x^*)$, $x^* \in G^* - fd(n)$ respectively. Then $[X^*]_{G^*}$ is the matrix product

$$[X^*]_{G^*} = \mathcal{F}_G(n) \cdot [X]_G.$$

Thus, the new information required to formulate an invariant Finite Fourier Transform matrix consists of a fundamental domain of G, a fundamental domain of G^* and coset representatives of the isotropy groups at elements in the fundamental domain of G. Since coset representatives play the role of indices in the programming of the resulting algorithms, we will call $C_G(x)$ an *indexing set* of $G(x)$.

We may summarize the above discussion as follows. $[\mathcal{F}_I(n)(x^*, x)]$ is a matrix representation of $F(n)$. $[X]_G$ and $[X]_{G^*}$ are subvectors of $[X]_I$ and $[X]_{I^*}$. $[\mathcal{F}_G(n)(x^*, x)]$ is obtained from $[\mathcal{F}_I(n)(x^*, x)]$ by crossing out the rows indexed by the elements not belonging to $G^* - fd(n)$ and adding the columns indexed by elements belonging in the same G–orbit.

We will pause briefly to discuss the relation between conjugate groups and the invariant Fourier transforms.

Definition If A is a subgroup of a group K, then we denote by gAg^{-1}, for some $g \in K$, the set of all elements of K of the form gag^{-1} with $a \in A$. gAg^{-1} is also a subgroup of K. Subgroups A and B are said to be *conjugate subgroups* in K and denoted $A \sim_K B$ if $A = gBg^{-1}$ for some $g \in K$.

In the lemmas below, let $G' = \tau G \tau^{-1}$ for some $\tau \in SL(3, Z)$.

Lemma 2 Let $\{x_1, x_2, \ldots, x_k\}$ be a $G - fd(n)$. Then $\{\tau x_1, \tau x_2, \ldots, \tau x_k\}$ is a $G' - fd(n)$.

Proof For $1 \leq j, l \leq k$ and $j \neq l$,

$G'(\tau x_j) \cap G'(\tau x_l) = \tau G \tau^{-1}(\tau x_j) \cap \tau G \tau^{-1}(\tau x_l) = \tau G(x_j) \cap \tau G(x_l) = \tau(G(x_j) \cap G(x_l)) = \phi$,

because $G(x_j) \cap G(x_l) = \phi$. Also, $\cup_{j=1}^{k} \tau G \tau^{-1}(\tau x_j) = \cup_{j=1}^{k} \tau G(x_j) = \tau(Z/n)^3 = (Z/n)^3$.

Lemma 3 $Iso_{G'}(\tau x) = \tau(Iso_G(x))\tau^{-1}$.

Proof For $g \in Iso_G(x)$, $\tau g\tau^{-1}(\tau x) = \tau gx = \tau x$. Thus $\tau g\tau^{-1}$ is an element of $Iso_{G'}(\tau x)$ and $\tau(Iso_G(x))\tau^{-1} \subset Iso_{G'}(\tau x)$. On the other hand suppose $g'(\tau x) = \tau x$. Then $\tau^{-1}g'(\tau x)\tau = \tau^{-1}g'\tau x = x$ which implies $\tau^{-1}g'\tau \in Iso_G(x)$ and $g' \in \tau(Iso_G(x))\tau^{-1}$.

Lemma 4 For a subgroup S of G, let C be a set of coset representatives of the cosets of S in G. Then $\tau C\tau^{-1}$ is a set of coset representatives of the cosets of $\tau S\tau^{-1}$ in G'.

Proof Let $C = \{c_1, c_2, \ldots, c_k\}$. Then

$$\cup_{j=1}^{k} \tau c_j\tau^{-1}\tau S\tau^{-1} = \cup_{j=1}^{k} \tau c_j S\tau^{-1} = \tau(\cup_{j=1}^{k} c_j S)\tau^{-1} = \tau G\tau^{-1} = G',$$

and for $1 \le j, l \le k$ and $j \ne l$, $\tau(c_j S)\tau^{-1} \cap \tau(c_l S)\tau^{-1} = \tau(c_j S \cap c_l S)\tau^{-1} = \phi$.

Lemma 5 $(G')^* = \tau^* G^*(\tau^*)^{-1}$.

Proof Let $h \in G'$. Then $h = \tau g\tau^{-1}$ for some $g \in G$. $h^* = (\tau g\tau^{-1})^* = (\tau g^{-1}\tau^{-1})^t = \tau^* g^*(\tau^*)^{-1}$.

By the lemmas 2 and 5, we have that $\tau^*(G^* - fd(n))$ is a $G'^* - fd(n)$ and $\tau(G - fd(n))$ is a $G' - fd(n)$. Thus, for $f \in L_{G'}(n)$, $x^* \in G^* - fd(n)$,

$$F_{G'}(n)f(\tau^* x^*) = \sum_{x \in G - fd(n)} \left(\sum_{c \in C_G(x)} \omega_n^{<\tau^* x^*, \tau c\tau^{-1} x>}\right).$$

But $< \tau^* x^*, \tau c\tau^{-1} > = < \tau^* x^*, \tau cx > = < x^*, cx >$. Hence

$$F_{G'}(n)f(\tau^* x^*) = \sum_{x \in G - fd(n)} \left(\sum_{c \in C_G(x)} \omega_n^{<x^*, cx>}\right).$$

Denote by $[X]_{\tau G}$ and $[X^*]_{\tau^* G^*}$ the column vectors of entries $f(\tau x)$, $x \in G - fd(n)$ and $F_{G^*}(n)f(\tau^* x^*)$, $x^* \in G^* - fd(n)$. Then

$$[X^*]_{\tau^* G^*} = [\mathcal{F}_G(n)(x^*, x)]_{x \in G - fd(n), x^* \in G^* - fd(n)} \cdot [X]_{\tau G}.$$

With G, G' and τ as above, we have proved the following theorem.

Theorem 3 By choosing $\tau(G - fd(n))$ as a $G' - fd(n)$ and $\tau^*(G^* - fd(n))$ as a $G'^* - fd(n)$, the matrix representation of $F_{G'}(n)$, a G'−invariant Fourier transform is the same as that of $F_G(n)$.

We need the following preliminary results to further describe our work.

For $n = p \cdot q$, where p and q are relatively prime natural numbers, we have by the Chinese Remainder Theorem [7] the decomposition,

$$(Z/n)^3 \approx (Z/p)^3 \times (Z/q)^3.$$

We also have the decompositions [6],

$$L(n) \approx L(p) \otimes L(q), \quad F(n) \approx F(p) \otimes F(q).$$

Let us now see how to relate the group G acting on the rings $(Z/n)^3$ and $(Z/p)^3 \times (Z/q)^3$. For $x \in (Z/n)^3$, consider the ring isomorphism defined by

$$i(x) = (x_p, x_q),$$

where $x_p \equiv x \ (mod\ p)$, $x_q \equiv x \ (mod\ q)$.

For $g \in G$, $i(gx) = \big((gx)_p, (gx)_q\big)$. Since $(gx)_p \equiv g(x_p) \ (mod\ p)$ and $(gx)_q \equiv gx_q \ (mod\ q)$,

$$i(gx) = (gx_p, gx_q).$$

We will denote the group of automorphisms $\{(g,g) \mid g \in G\}$ of $(Z/p)^3 \times (Z/q)^3$ again by G. Similarly, for $g^* \in G^*$, the automorphism of $(Z/p)^3 \times (Z/q)^3$ induced by the ring isomorphism i is (g^*, g^*). We will denote the group of automorphisms $\{(g^*, g^*) \mid g^* \in G^*\}$ again by G^*. Denoting the collection of G and G^*-invariant functions in $L(p) \otimes L(q)$ by $L_G(p,q)$ and $L_{G^*}(p,q)$, we have seen in theorem 2 that

$$F(p) \otimes F(q) : L_G(p,q) \longrightarrow L_{G^*}(p,q).$$

For $f \in L(p) \otimes L(q)$ and $(y^*, z^*) \in (Z/p)^3 \times (Z/q)^3$, define

$$(F(p) \otimes Iq) f(y^*, z^*) = \sum_{y \in (Z/p)^3} f(y, z^*) \cdot \omega_n^{<y^*, y>},$$

$$(Ip \otimes F(q)) f(y^*, z^*) = \sum_{z \in (Z/q)^3} f(y^*, z) \cdot \omega_n^{<z^*, z>}.$$

$Ip \otimes F(q)$ and $F(p) \otimes Iq$ are linear transformations of $L(p) \otimes L(q)$, and

$$F(p) \otimes F(q) = (Ip \otimes F(q)) \circ (F(p) \otimes Iq),$$

where $\circ$ denotes the composition of linear transformations.

Theorem 4 For $f \in L_G(p,q)$ and $(y^*, z) \in (Z/p)^3 \times (Z/q)^3$,

$$(F(p) \otimes Iq) f(g^* y^*, gz) = (F(p) \otimes Iq) f(y^*, z).$$

Proof $(F(p) \otimes Iq) f(g^* y^*, gz) = \sum_{y \in (Z/p)^3} f(y, gz) \cdot \omega_n^{<g^* y^*, y>}$.

By lemma 1, we have $(F(p) \otimes Iq) f(g^*, gz) = \sum_{y \in (Z/p)^3} f(y, gz) \cdot \omega_n^{<y^*, g^{-1}y>}$.

Replacing y by gy, we have $(F(p) \otimes Iq) f(g^*, gz) = \sum_{gy \in (Z/p)^3} f(gy, gz) \cdot \omega_n^{<y^*, y>}$.

Since $f(gy, gz) = f(y, z)$, we have now

$(F(p) \otimes Iq) f(g^*, gz) = \sum_{gy \in (Z/p)^3} f(y, z) \cdot \omega_n^{<y^*, y>} = (F(p) \otimes Iq) f(y^*, z)$.

Let $\overline{G} = \{(g^*, g) \mid g \in G\}$. $\overline{G}$ is also a group of automorphisms of $(Z/p)^3 \times (Z/q)^3$. Denote the set of $\overline{G}-$invariant functions in $L(p, q)$ by $L_{\overline{G}}(p, q)$. We can then prove the next theorem in exactly the same way as above.

Theorem 5 For $f \in L_{\overline{G}}(p, q)$, $(y^*, z^*) \in (Z/p)^3 \times (Z/q)^3$,

$(Ip \otimes F(q)) f(g^* y, g^* z) = (Ip \otimes F(q)) f(y^*, z^*)$.

Thus we have

$$L_G(p, q) \xrightarrow{F(p) \otimes Iq} L_{\overline{G}}(p, q) \xrightarrow{Ip \otimes F(q)} L_{G^*}(p, q).$$

Notation For a group G of automorphisms of the product ring, $(Z/p)^3 \times (Z/q)^3$, we will denote a $G-$fundamental domain in $(Z/p)^3 \times (Z/q)^3$ by $G - fd(p, q)$.

We will now define the group $P3$ and describe the *$P3-$invariant product construction.*

$P3$ is the group generated by the matrix

$$\alpha = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$\alpha^3 = I$, and $P3$ is a simple group of order 3.

Comment In the set of groups we deal with, any simple group is isomorphic to $Z/2$ or $Z/3$. We have chosen to deal with $P3 \simeq Z/3$.

Definition The *$P3-$invariant product construction* is a collection of procedures that determines a $P3-$invariant Fourier Transform on the product ring $(Z/p)^3 \times (Z/q)^3$ as a tensor product of $F_{P3}(p)$ and $F_{P3}(q)$.

The $P3$−invariant product construction consists of the following three procedures once we have precomputed $P3-fd(p)$, $P3^*-fd(p)$, $P3-fd(q)$, $P3^*-fd(q)$, $\mathcal{F}_{P3}(p)$ and $\mathcal{F}_{P3}(q)$. (Algorithms for computing with $F(n)$, for a natural number n, are abundant.) :

(a) Construct a $P3-fd(p,q)$ and a $\overline{P3}-fd(p,q)_1$ such that for $f \in L_{P3}(p,q)$, $(F(p)\otimes Iq)f$ can be computed in terms of $F_{P3}(p)$ and $F(p)$.

(b) Construct a $\overline{P3}-fd(p,q)_2$ and a $P3^*-fd(p,q)$ such that for $f \in L_{\overline{P3}}(p,q)$, $(Ip\otimes F(q))f$ can be computed in terms of $F_{P3}(q)$ and $F(q)$.

(c) Determine a bijection between the two $\overline{P3}$−fundamental domains $\overline{P3}-fd(p,q)_1$ and $\overline{P3}-fd(p,q)_2$.

The constructions (a), (b) and (c) are easy, because $P3$ is a simple group. For any $x \in (Z/n)^3$, $Iso_{P3}(x)$ is either $P3$ or I. Similarly, $Iso_{P3^*}(x)$ is either $P3^*$ or $I^* = I$. We will show a method for constructing (a). The construction in (b) is achieved in exactly the same way. We will also determine the bijection in (c).

Construction of (a) :

Decompose a $P3-fd(p)$ and a $P3-fd(q)$ by the isotropy subgroups as follows.

$Z(P3:I) = \{z \in P3-fd(q) \mid Iso_{P3}(z) = I\}$,

$Z(P3:P3) = \{z \in P3-fd(q) \mid Iso_{P3}(z) = P3\}$.

$Y(P3:I) = \{y \in P3-fd(p) \mid Iso_{P3}(y) = I\}$,

$Y(P3:P3) = \{y \in P3-fd(p) \mid Iso_{P3}(y) = P3\}$.

Decompose a $P3^*-fd(p)$ and $P3^*-fd(q)$ by the isotropy subgroups in the same way.

$Z(P3^*:I) = \{z \in P3^*-fd(q) \mid Iso_{P3^*}(z) = I\}$,

$Z(P3^*:P3^*) = \{z \in P3^*-fd(q) \mid Iso_{P3^*}(z) = P3^*\}$.

$Y(P3^*:I) = \{y \in P3^*-fd(p) \mid Iso_{P3^*}(y) = I\}$,

$Y(P3^*:P3^*) = \{y \in P3^*-fd(p) \mid Iso_{P3^*}(y) = P3^*\}$.

Then we have

$(Z/q)^3 = Z(P3:P3) \cup Z(P3:I) \cup \alpha Z(P3:I) \cup \alpha^2 Z(P3:I)$,

$(Z/p)^3 = Y(P3:P3) \cup Y(P3:I) \cup \alpha Y(P3:I) \cup \alpha^2 Y(P3:I)$,

where the union is disjoint. Trivially,

$Z(P3:P3) = \alpha Z(P3:P3) = \alpha^2 Z(P3:P3), \quad (Z/q)^3 = \alpha(Z/q)^3 = \alpha^2(Z/q)^3.$

$Y(P3:P3) = \alpha Y(P3:P3) = \alpha^2 Y(P3:P3), \quad (Z/p)^3 = \alpha(Z/p)^3 = \alpha^2(Z/p)^3.$

We may now decompose $(Z/p)^3 \times (Z/q)^3$ as follows:

$$(Z/p)^3 \times (Z/q)^3 = \big((Z/p)^3 \times Z(P3:P3)\big) \cup \big((Z/p)^3 \times Z(P3:P3)\big)$$
$$\cup\big((Z/p)^3 \times \alpha Z(P3:I)\big) \cup \big((Z/p)^3 \times \alpha^2 Z(P3:I)\big)$$

$$= \Big(\big(Y(P3:P3) \cup Y(P3:I) \cup \alpha Y(P3:I) \cup \alpha^2 Y(I)\big) \times Z(P3:P3)\Big)$$
$$\cup\Big((Z/p)^3 \times Z(P3:I)\Big) \cup \Big((Z/p)^3 \times \alpha Z(P3:I)\Big) \cup \Big((Z/p)^3 \times \alpha^2 Z(P3:I)\Big)$$

$$= \Big(\big(Y(P3:P3) \cup Y(P3:I)\big) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big)$$
$$\cup(\alpha,\alpha)\Big(\big(Y(P3:P3) \cup Y(P3:P3)\big) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big)$$
$$\cup(\alpha^2,\alpha^2)\Big(\big(Y(P3:P3) \cup Y(P3:I)\big) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big).$$

$Y(P3:P3) \cup Y(P3:I)$ is a G–fd(p). We have thus shown the following.

Lemma 6 $\Big(G - fd(p) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big)$ is a $G - fd(p,q)$.

Lemma 7 $\Big(G^* - fd(p) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big)$ is a $\overline{G} - fd(p,q)$.

Proof The proof consists of replacing $G - fd(p)$ with $G^* - fd(p)$, $Y(P3:P3)$ with $Y(P3^*:P3^*)$ and $Y(P3:I)$ with $Y(P3^*:I^*)$ in the above construction.

Theorem 6 For $f \in L_{P3}(p,q)$ and an element (y^*,z) of $\Big(G^* - fd(p) \times Z(P3:P3)\Big) \cup \Big((Z/p)^3 \times Z(P3:I)\Big)$,

$(F(p) \otimes Iq)f(y^*,z)$ can be computed in terms of $F_{P3}(p)$ and $F(p)$.

Proof We will prove this by constructing a matrix representation of the linear transformation $F(p) \otimes Iq$ of a function $f \in L_{P3}(p,q)$. To do this, consider the $P3 - fd(p,q)$ and $\overline{P3} - fd(p,q)$ in the lemmas 6 and 7 as lexicographically ordered sets. Let q_I and q_{P3} denote the orders of

the sets $Z(P3 : I)$ and $Z(P3 : P3)$. Then

$$(\mathcal{F}_{P3}(p) \otimes Iq_{P3}) \oplus (\mathcal{F}(p) \otimes Iq_I)$$

is a desired matrix representation, where $\oplus$ denotes the direct product of matrices.

Construction of (b) :

Lemma 8 $\Big(Y(P3^* : P3^*) \times P3 - fd(q)\Big) \cup \Big(Y(P3^* : I^*) \times (Z/q)^3\Big)$ and

$\Big(Y(P3^* : P3^*) \times P3^* - fd(q)\Big) \cup \Big(Y(P3^* : I^*) \times (Z/q)^3\Big)$ are $\overline{P3} - fd(p,q)$ and $P3^* - fd(p,q)$ respectively.

Theorem 7 For $f \in L_{\overline{P3}}(p,q)$ and an element (y^*, z^*) of

$\Big(Y(P3^* : P3^*) \times P3^* - fd(q)\Big) \cup \Big(Y(P3^* : I^*) \times (Z/q)^3\Big)$, $(Ip \otimes F(q))f(y^*, z^*)$ can be computed in terms of $F_{P3}(q)$ and $F(q)$.

To find the matrix representation of $(Ip \otimes F(q))$ of a function $f \in L_{\overline{P3}}(p,q)$, let the orders of $Y(P3^* : P3^*)$ and $Y(P3^* : I^*)$ be p_{P3} and p_I. Consider the $\overline{P3} - fd(p,q)$ and $P3^* - fd(p,q)$ in the lemma above as lexicographically ordered sets. A $P3-$invariant matrix representation of $Ip \otimes F(q)$ is

$$(Ip_{P3} \otimes \mathcal{F}_{P3}(q)) \oplus (Ip_I \otimes \mathcal{F}(q)).$$

Determination of (c) :

Let

$$\overline{P3} - fd(p,q)_1 = \Big(P3 - fd(p) \times Z(P3^* : P3^*)\Big) \cup \Big((Z/p)^3 \times Z(P3 : I)\Big),$$
$$\overline{P3} - fd(p,q)_2 = \Big(Y(P3^* : P3^*) \times P3 - fd(q)\Big) \cup \Big(Y(P3^* : I^*) \times (Z/q)^3\Big).$$

The mapping Π defined below as a union of the mappings of the partition of $\overline{P3} - fd(p,q)_1$ and

$\overline{P3} - fd(p,q)_2$ is a bijection.

$$\begin{array}{ccc}
\overline{P3} - fd(p,q)_1 & & \overline{P3} - fd(p,q)_2 \\
Y(P3^* : P3^*) \times Z(P3 : P3) & \xrightarrow{(I,I)} & Y(P3^* : P3^*) \times Z(P3 : P3) \\
Y(P3^* : I^*) \times Z(P3 : P3) & \xrightarrow{(I,I)} & Y(P3^* : I^*) \times Z(P3 : P3) \\
Y(P3^* : P3^*) \times Z(P3 : I) & \xrightarrow{(I,I)} & Y(P3^* : P3^*) \times Z(P3 : I) \\
Y(P3^* : I^*) \times Z(P3 : I) & \xrightarrow{(I,I)} & Y(P3^* : I^*) \times Z(P3 : I) \\
\alpha^* Y(P3^* : I^*) \times Z(P3 : I) & \xrightarrow{(\alpha^{*2},\alpha^2)} & Y(P3^* : I^*) \times \alpha^2 Z(P3 : I) \\
\alpha^{*2} Y(P3^* : I^*) \times Z(P3 : I) & \xrightarrow{(\alpha^*,\alpha)} & Y(P3^* : I^*) \times \alpha Z(P3 : I)
\end{array}$$

A trivial, yet crucial property of Π is that for $\overline{f} \in L_{\overline{P3}}(p,q)$,

$$\overline{f}(y^*, z) = \overline{f}(\Pi(y^*, z)). \tag{4}$$

If P is the mapping defined for $(y^*, z) \in \overline{P3} - fd(p,q)_1$ by

$$P : (F(p) \otimes Iq) f(y^*, z) \longrightarrow (F(p) \otimes Iq) f(\Pi(y^*, z)),$$

we have

$$P\big((F(p) \otimes Iq) f(y^*, z)\big) = (F(p) \otimes Iq) f(\Pi(y^*, z)) \ .$$

For $f \in L_{P3}(p,q)$, $(F(p) \otimes Iq) f \in L_{\overline{P3}}(p,q)$. Hence by (4), P is a permutation of the set

$$\{(F(p) \otimes Iq) f(y^*, z)\}_{(y^*,z) \in \overline{P3} - fd(p,q)_1}$$

onto the set

$$\{(F(p) \otimes Iq) f(\Pi(y^*, z))\}_{\Pi(y^*,z) \in \overline{P3} - fd(p,q)_2}.$$

Definition We will call a bijection between two $\overline{G}$–fundamental domains satisfying (4) an *orbit exchange* for $\overline{G}$.

We will now define a G–invariant product construction for an arbitrary group G. We will assume some results as we describe our approach to the problem. We will devote the remaining chapters of this thesis to proving them.

Given a $G-$fundamental domain $G-fd(q)$ in $(Z/q)^3$, we will see that a $G-$fundamental domain in $(Z/p)^3 \times (Z/q)^3$ is $\cup_{x \in G-fd(q)}(Iso(x) - fd(p) \times \{x\})$. Since any subgroup of G can be the isotropy subgroup at some element, we will need for all subgroups S of G, $S - fd(p)$ to compute a $G-$fundamental domain in the product ring. Yet, as we will see later, for $x \in (Z/n)^3$ and $S < G$, if $Iso(x)$ is conjugate to S, then there exists an element $x' \in G(x)$ such that $Iso(x') = S$. Thus, by choosing a collection Ψ of representatives of conjugacy classes of subgroups of G, we can determine a $G-$fundamental domain with the property that if S is the isotropy subgroup at an element in this fundamental domain, then $S \in \Psi$. We will denote such a $G-$fundamental domain in $(Z/n)^3$ for a given collection Ψ of subgroups of G by $G - FD(n)$. The $G-$invariant product construction for an arbitrary point group G requires the following precomputation: (Recall that for a representation ψ of a point group, we denote the contragradient representation by ψ^*.)

(d) Collections Ψ and Ψ^* of representatives of the conjugacy classes of subgroups of G and G^*.

(e) $\psi - FD(p)$, $\psi^* - FD(p)$, $\psi - FD(q)$ and $\psi^* - FD(q)$, for $\psi \in \Psi$, $\psi^* \in \Psi^*$. (We are reserving the capital letters FD to denote fundamental domains with the property that the isotropy subgroup at an element in this fundamental domain belongs to Ψ or Ψ^* respectively.)

(f) $\mathcal{F}_\psi(p)$ and $\mathcal{F}_\psi(q)$, for $\psi \in \Psi$.

We claim that the information in (d), (e) and (f) is sufficient to formulate the invariant product construction not only for the group G, but also for any of the groups $\psi \in \Psi$, because we can do the following.

(a') Construct a $\psi - fd(p,q)$ and a $\overline{\psi} - fd(p,q)_1$ such that for $f \in L_\psi(p,q)$, $(F(p) \otimes Iq)f$ can be computed in terms of $F_{\psi_j}(p)$, for $\psi_j < \psi$ and $\psi_j \in \Psi$.

(b') Construct a $\overline{\psi} - fd(p,q)_2$ and a $\psi^* - fd(p,q)$ such that for $f \in L_{\overline{\psi}}(p,q)$, $(Ip \otimes F(I)q)f$ can be computed in terms of $F_{\psi_j}(q)$, for $\psi_j < \psi$ and $\psi_j \in \Psi$.

(c') Determine an orbit exchange for $\overline{\psi}$.

Assuming that we have the information (d), (e) and (f), let us see how we can carry out the construction in (a') and (b').

Note that $Iso_\psi(x) = Iso(x) \cap \psi$. For $\psi \in \Psi$, we will use the following notation.

$Y(\psi : \psi_j) = \{y \in \psi - FD(p) \mid Iso_\psi(y) = \psi_j\}$,

$Z(\psi : \psi_j) = \{z \in \psi - FD(q) \mid Iso_\psi(z) = \psi_j\}$,

$Y(\psi^* : \psi_j^*) = \{y^* \in \psi^* - FD(p) \mid Iso_\psi(y^*) = \psi_j^*\}$,

$Z(\psi^* : \psi_j^*) = \{z^* \in \psi^* - FD(q) \mid Iso_\psi(z^*) = \psi_j^*\}$.

Claim (a') $\cup_j(\psi_j - FD(p) \times Z(\psi : \psi_j))$ and $\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j))$ are the desired ψ and $\overline{\psi}$–fundamental domains in $(Z/p)^3 \times (Z/q)^3$, respectively.

Claim (b') $\cup_j(Y(\psi^* : \psi_j^*) \times \psi_j - FD(q))$ and $\cup_j(Y(\psi^* : \psi_j^*) \times \psi_j^* - FD(q))$ are the desired $\overline{\psi}$ and ψ^*–fundamental domains in $(Z/p)^3 \times (Z/q)^3$, resectively.

Claim (c') There exits an orbit exchange for $\overline{\psi}$ between any two $\overline{\psi}$-fundamnetal domains.

We will prove (c) now, because it is simple. (Observe that we claim only the existence here. Later, we will compute the orbit exchange explicitly.)

Proof Let fd_1 and fd_2 be any two $\overline{\psi}$-fundamental domains in $(Z/p)^3 \times (Z/q)^3$. For an element $x_1 \in fd_1$, there is one and only one $x_2 \in fd_2$ with $\overline{\psi}(x_1) = \overline{\psi}(x_2)$. Hence we can define a mapping Π by setting

$$\Pi(x_1) = x_2, \quad \text{if} \quad \overline{\psi}(x_1) = \overline{\psi}(x_2).$$

$x_2 = gx_1$, for some $g \in \overline{\psi}$. For $f \in L_{\overline{\psi}}(p, q)$, $f(x_2) = f(\overline{g}x_1) = f(\Pi x_1)$. Thus, Π is an orbit exchange for $\overline{\psi}$.

Now we turn our attention to obtaining the necessary precomputations. We will begin by showing, in a crude way, how the solvability of the point groups leads us to iterative procedures for computing invariant Finite Fourier Transform matrices. Let G_2 be a point group and $G_1 \triangleleft G_2$. We will show that there exists a $G_1 - fd(n) \supset G_2 - fd(n)$, and that an indexing set $C_{G_2}(x_j)$

exists such that a subset of $C_{G_1}(x_j)$ is an indexing set of $G_1(x_j)$ for the element x_j. Thus, we can determine $\mathcal{F}_{G_2}(n)$ from $\mathcal{F}_{G_1}(n)$ by deleting the rows indexed by the elements not belonging to the $G_2^* - fd(n)$ and summing the columns indexed by the elements belonging to the same G_2−orbit.

We will now compute G_2 and G_1−fundamental domains and indexing subsets. Note that since G_1 is normal in G_2, the action of G_2 is well defined on the space of G_1−orbits in $(Z/n)^3$. Specifically, we can write G_2 as $g_1G_1 \cup g_2G_1 \cup \ldots \cup g_kG_1$, where the union is disjoint. For $x \in (Z/n)^3$,

$$G_2(x) = G_1(g_1x) \cup G_1(g_2x) \cup \ldots \cup G_1(g_kx).$$

Union here need not be disjoint.

We can determine fundamental domains and indexing subgroups by the following bootstrap technique.

1) Let G_2/G_1 be the set $\{g_1, g_2, \ldots, g_k\}$.

2) Decompose $(Z/n)^3$ into G_1−orbits.

3) Determine the G_2−orbits by aggregating the G_1−orbits. For $x \in (Z/n)^3$, let $[G_2/G_1(x)]$ be a subset of G_2/G_1 such that $G_2(x)$ is a disjoint union of $G_1(gx)$ for $g \in [G_2/G_1(x)]$.

4) Construct $G_2 - fd(n)$ by choosing one element from each G_2−orbit.

5) $G_1 - fd(n) = \cup_{x \in G_2 - fd(n)} [G_2/G_1(x)]x$.

6) For $x \in G_2 - fd(n)$, determine $Iso_{G_1}(x)$. Determine $C_{G_1}(x)$, an indexing subset of $G_1(x)$.

7) $Iso_{G_1}(gx) = Ios_{G_1}(x)$, and $C_{G_1}(gx) = C_{G_1}(x)$, for $g \in [G_2/G_1(x)]$.

8) $Iso_{G_2}(x) = Iso_{G_1}(x) \cdot [G_2/G_1(x)]$, and $C_{G_2}(x) = C_{G_1}(x) \cdot [G_2/G_1(x)]$.

Thus we have a method for computing a ψ−invariant module for $\psi \triangleleft G$. On the other hand, if $\psi \triangleleft G$, then ψ is contained in any collection of representatives of the conjugacy classes of subgroups of G.

We will now proceed to work through in detatil the material outlined above. We will require certain basic facts from group theory and module theory.

2. The Group P622.

As an abstract group, $P622 \simeq (Z/3 \oplus Z/2) \leftthreetimes Z/2$, where $\leftthreetimes$ denotes the semidirect product of groups. We will represent $P622$ and list some properties of the group in this chapter. We will then determine a collection of representatives of the subgroups of $P622$. This collection will be called Ψ and will be fixed throughout the rest of this thesis. We also prove properties of Ψ that we will use in the later chapters.

The following two elements in $SL(3,Z)$ along with α, defined before, generate the group $P622$.

$$\beta = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

$\beta^2 = I$ and β commutes with α. Hence β is a representation of $Z/2$. The group generated by β is called $P2$ and the group $P3 \oplus P2$ is called $P6$. Let $Q2$ be the group generated by γ. $\gamma^2 = I$. $\gamma\alpha\gamma^{-1} = \alpha^2$, and γ is an automorphism of $P3$. The group $P3 \leftthreetimes Q2$ is called $P312$, where $\leftthreetimes$ denotes the semidirect product of the two groups. Let $\delta = \beta\gamma$. $\delta = \gamma\beta$, and $\delta^2 = I$. Since $\delta\alpha\delta^{-1} = \alpha^2$, δ is also an automorphism of $P3$. Denote the group generated by δ by $R2$. The group $P3 \leftthreetimes R2$ is called $P321$. Since $Q2$ and $R2$ are automorphisms of $P6$, we can form $P6 \leftthreetimes Q2$ and $P6 \leftthreetimes R2$. $P622 = P2 \oplus P321 = P2 \oplus P312 = P6 \leftthreetimes Q2 = P6 \leftthreetimes R2$.
Let A be the group generated by β and γ. Since $\beta\gamma = \gamma\beta = \delta$, $A = P2 \oplus Q2 = P2 \oplus R2 = Q2 \oplus R2$. As an abstract group $A \simeq Z/2 \oplus Z/2$, and A is abelian.

Lemma 9 $P3$ is the only subgroup of order 3 in $P622$.

Proof Since $ord(P622) = 3 \cdot 2^2$, $P3$ is a Sylow subgroup. But $P3 \triangleleft P622$.

Lemma 10 Any subgroup of $P622$ of order 4 is conjugate to A.

Proof $ord(A) = 4$, and A is a Sylow subgroup.

Lemma 11 $P622$ has 3 subgroups of order 6.

Proof The preimage of a subgroup of $P622/P3$ of order 2 is a subgroup of order 6 in $P622$.

$P622/P3 \simeq Z/2 \oplus Z/2$, and $Z/2 \oplus Z/2$ has 3 subgroups of order 2. Hence there are 3 subgroups of order 6 in $P622$. They are $P6$, $P312$ and $P321$.

Lemma 12 The 3 subgroups of order 6 are normal in $P622$.

Lemma 13 If S is a subgroup of order 2, then S is conjugate to to $P2$, $Q2$, or $R2$.

Proof By Sylow's theorem there exits a Sylow subgroup $B > S$ of order 4. But $B \sim A$.

We have just proved the theorem below.

Theorem 8 The set

$$\Psi = \{I, P2, Q2, R2, P3, A, P6, P312, P321, P622\}.$$

is a collection of representatives of the conjugacy classes of subgroups of $P622$.

Henceforth, we will use ψ or ψ_j, for a natural number j to denote an element of Ψ.

Theorem 9 $P622 \sim_{SL(3,Z)} P622^*$.

Proof Let τ be the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Then $\tau \in SL(3, Z)$, and by a direct computation, we see that $\tau P3\tau^{-1} = P3^*$. Also $\tau A\tau^{-1} = A^* = A$, for $\tau\beta\tau^{-1} = \beta$, $\tau\gamma\tau^{-1} = \delta$, $\tau\delta\tau^{-1} = \gamma$. Thus $\tau P622\tau^{-1} = \tau P3\tau^{-1}\tau A\tau^{-1} = P622^*$.

Thus all the information about $P622^*$ can be obtained from the information about $P622$. In particular, we can obtain a ψ^*−fundamental domain from a ψ'−fundamental domain for $\psi' \in \Psi$ and $\psi' \sim \psi^*$.

Notation For subgroups S_1 and S_2 of a group K, we will denote by $S_1 \cdot S_2$ the set $\{s_1 s_2 \mid s_1 \in S_1,$ and $s_2 \in S_2\}$. In general, $S_1 \cdot S_2$ is not a subgroup of K.

Definition Subgroups S_1 and S_2 of a group K are said to be *complementary in* K, if

$$S_1 \cap S_2 = I \text{ and } S_1 \cdot S_2 = K.$$

Theorem 10 Every subgroup of $P622$ has a complementary subgroup in $P622$.

Proof If S is a subgroup of $P622$, then S is of order 1, 2, 3, 4, 6, or 12. The only non-trivial cases are when $ord(S) = 2$ or 6. If $ord(S) = 2$, then by the Sylow-theorem, there exists a group B in P_{622} of order 4 containing S. Furthermore since $B \simeq Z/2 \oplus Z/2$, $B = S \cdot S'$, for a group S' of order 2.

$P622 = P3 \cdot B = P3 \cdot S' \cdot S$. Thus $P3 \cdot S'$ is a complementary subgroup of S in $P622$.

Suppose now $ord(S) = 6$. $S = P3 \cdot S'$, for a subgroup S' of S. Then again there exists a group B in $P622$ of order 4 such that $B = S' \cdot S''$, for a subgroup S'' of order 2. Thus $P622 = P3 \cdot B$ $= P3 \cdot S' \cdot S = S \cdot S''$, and S'' is a complementary subgroup of S in $P622$.

This implies that we can choose subgroups of $P622$ as indexing subsets of $P622-$orbits. Moreover, this property holds in any subgroup of $P622$.

Notation Henceforth, we will use the phrase *indexing subgroup* in place of indexing subset for an orbit by any subgroup of $P622$.

Theorem 11 For any subgroup of ψ, it or its complementary subgroup in ψ is normal in ψ.

Proof Observe first that if $3 \mid ord(T)$ for a subgroup T of $P622$, then $T \triangleleft P622$. Thus T is normal in any subgroup of $P622$ containing T. Suppose now that $3 \mid ord(\psi)$. For $S < \psi$, either $3 \mid ord(S)$ or 3 divides the order of a complementary subgroup of S in ψ. Hence S or its complement is normal. On the other hand, if 3 does not divide the order of ψ, then ψ is abelian, so there is nothing to prove.

Lemma 14 For a complementary pair S and C of a group G, if either S or C is normal in G, then any subgroup conjugate to C is complementary to S.

Proof If C is normal, there is nothing to prove. Suppose $S \triangleleft G$. $S \cdot gCg^{-1} = gS \cdot Cg^{-1} = G$, for $g \in G$.

Theorem 12 We can choose an indexing subgroup of a $\psi-$orbit in Ψ.

Proof For $x \in (Z/n)^3$, a complementay subgroup of $Iso_{\psi}(x)$ is an indexing subgroup of $\psi(x)$.

Since Ψ is a collection of conjugacy classes of subgroups of $P622$, there is a complementay subgroup of $Iso_\psi(x)$ in Ψ by lemma 14.

Notation We will denote a complementary subgroup of ψ belonging to Ψ by $C(\psi)$. In general $C(\psi)$ is not unique. For $\psi_1 < \psi_2$, we will denote a complementary subgroup of ψ_1 in ψ_2 belonging to Ψ by $C_{\psi_2}(\psi_1)$. Again, $C_{\psi_2}(\psi_1)$ may not be unique.

Theorem 13 The collection Ψ is closed under intersection.

Proof One can prove this by inspection.

Theorem 14 A is contained in the normalizer of ψ.

Proof Any $\psi \in \Psi$ is normal in either A or $P622$.

Lemma 15 $\psi_1 \cdot \psi_2 = \psi_2 \cdot \psi_1$.

Proof If $P3 < \psi_i$, for i = 1 or 2, then $\psi_i \triangleleft P622$. Hence $\psi_1 \cdot \psi_2 = \psi_2 \cdot \psi_1$. On the other hand, if $P3 \not< \psi_i$, for i = 1 and 2 then ψ_1 and ψ_2 belong to A. Thus, again $\psi_1 \cdot \psi_2 = \psi_2 \cdot \psi_1$.

Lemma 16 $\psi_1 \cdot \psi_2 < P622$.

Proof Let $g \in \psi_1 \cdot \psi_2$. Then $g = g_1 g_2$, for some $g_1 \in \psi_i$, i = 1, 2. Then $g_2^{-1} g_1^{-1} = g^{-1} \in \psi_2 \cdot \psi_1$. By the lemma above, $g^{-1} \in \psi_1 \cdot \psi_2$. Let $g_1 g_2$, $h_1 h_2 \in \psi_1 \cdot \psi_2$, where g_i, $h_i \in \psi_i$, i = 1, 2. $(g_1 g_2)(h_1 h_2) = g_1 h_1' g_2' h_2$ for some $h_1' \in \psi_1$ and $g_2' \in \psi_2$, again by the above lemma.

Theorem 15 $\psi_1 \cdot \psi_2 \in \Psi$.

Proof If $P3 < \psi_i$, for i = 1 or 2, then $\psi_1 \cdot \psi_2 \triangleleft P622$. Thus, $\psi_1 \cdot \psi_2 \in \Psi$. On the other hand, if $P3 \not< \psi_i$ for i = 1 and 2, then $\psi_1 \cdot \psi_2 < A$. So, again $\psi_1 \cdot \psi_2 \in \Psi$.

Theorem 16 For $\psi_1 \triangleleft \psi_2$, $C(\psi_2) \cdot C_{\psi_2}(\psi_1)$ is a $C(\psi_1)$.

Proof $C(\psi_2) \cdot C_{\psi_2}(\psi_1) \cdot \psi_1 = C(\psi_2) \cdot \psi_2 = P622$.

3. Orbit Decompositions and Fundamental Domains.

In this chapter, we will compute $\psi - FD(n)$ for all $\psi \in \Psi$.

Since $P622 \sim_{SL(3,Z)} P622^*$ and every subgroup of $P622$ is conjugate to a group in Ψ, we only need to find the ψ–orbit decomposition of $(Z/n)^3$ for $\psi \in \Psi$. On the other hand, we need the orbit decomposition of $(Z/n)^3$ only as a tool for computing fundamental domains and the isotropy subgroups of elements in fundamental doamins. We can obtain an S–fundamental domain and the respective isotropy subgroups for a normal subgroup S of $P622$ from a $P622$–fundamental domain by a bootstap technique. Moreover, we will see that from a $P622 - FD(n)$ for the collection Ψ we have chosen in the previous chapter, we can also obtain an A–fundamental domain and the respective isotropy subgroups. Any $\psi \in \Psi$ is a normal subgroup of either $P622$ or A. Hence we only need to compute the $P622$-orbit decompotion of $(Z/n)^3$. This, as the following lemma implies, is easily achieved by the orbit decomposition by an ascending chain of normal subgroups of $P622$. We will choose the normal series of groups $P622 \triangleright P6 \triangleright P3$.

Lemma 17 Let $S \triangleleft G$, and let C be a set of coset representatives of S–cosets in G. Then for $x \in (Z/n)^3$, $G(x) = \cup_{c \in C} S(cx)$.

Proof $G = \cup_{c \in C} cS$. Since $S \triangleleft G$, $cS = Sc$.

Since $P6 \triangleright P3$ and $P2$ is a set of coset representatives of $P3$–cosets in $P6$, for any $x \in (Z/n)^3$, $P6(x) = P3(x) \cup P3(\beta x)$. $\beta P3(x) = P3(\beta x)$. Thus, β maps the $P3$-orbit determined by x onto the $P3$-orbit determined by βx, and we can determine the $P6$–orbit decomposition of $(Z/n)^3$ by looking at the action of β on the $P3$–orbits in $(Z/n)^3$.

Also since $P622 \triangleright P6$ and $Q2$ is a set of coset representatives of $P6$–cosets in $P622$, for any $x \in (Z/n)^3$, $P622(x) = P6(x) \cup P6(\gamma x)$. $\gamma P6(x) = P6(\gamma x)$. Thus, to determine the $P622$-orbit decomposition of $(Z/n)^3$, we only need to look at the action of γ on the $P6$–orbits in $(Z/n)^3$. For $x \in (Z/n)^3$,

$$P622(x) = P3(x) \cup P3(\beta x) \cup P3(\gamma x) \cup P3(\gamma\beta x) = P3(x) \cup P3(\beta x) \cup P3(\gamma x) \cup P3(\delta x).$$

Therefore, we can find the $P622-$orbits in $(Z/n)^3$ by aggregating the $P3-$orbits in $(Z/n)^3$.

We present here one simplifying method for decomposing $(Z/n)^3$ into $P3-$orbits.
For $x \in (Z/n)^3$, let $x = (x_1, x_2, x_3)^t$ and $x' = (x_1, x_2, x_3')^t$. If $x_3 \neq x_3'$ then $P3(x) \cap P3(x')$ $= \phi$. On the other hand, if $\overline{x} = (\overline{x_1}, \overline{x_2}, x_3)^t \in P3(x)$, then $\overline{x'} = (\overline{x_1}, \overline{x_2}, x_3')^t \in P3(x')$. Thus once we compute one $P3-$orbit, we have n distinct $P3-$orbits by changing the last components of the elements in the $P3-$orbit. This reduces computation of $P3$ acting on n^3 elements to n^2 elements. Depending on the nature of the number n, there are other simplifying methods for computing the actions of $P3$ on the elements of $(Z/n)^3$. (One such method is to employ the structure of the multiplicative group of the units of the ring (Z/n). [3])

From the $P622-$orbit decomposition of $(Z/n)^3$, we can determine a $P622 - fd(n)$ by choosing one element from each $P622-$orbit. To determine a $P622 - FD(n)$ for the collection Ψ, we must first discuss the isotropy subgroups in $P622$ at elements in $P622 - fd(n)$. Henceforth we will denote the isotropy subgroup in $P622$ at $x \in (Z/n)^3$ by $Iso(x)$ in place of $Iso_{P622}(x)$. Once we have $Iso(x)$ for $x \in P622 - fd(n)$, we will show a method for determining $P622 - FD(n)$.

For $x \in (Z/n)^3$, we will determine $Iso(x)$ by extending $Iso_{P3}(x)$. To do this we will use the following theorem and its corollary.

Theorem 17 If x and y are elements belonging to the same $P622-$orbit, then
$Iso_{P3}(x) = Iso_{P3}(y)$.
Proof Since x and y belong in the same $P622-$orbit, $y = gx$, for some $g \in P622$. Observe now that $Iso(y) = gIso(x)g^{-1}$. $Iso_{P3}(y) = Iso(y) \cap P3 = gIso(x)g^{-1} \cap P3$. Because $P3$ is normal, $gIso(x)g^{-1} \cap P3 = g(Iso(x) \cap P3)g^{-1}$. Thus $Iso_{P3}(y) \sim_{P622} Iso_{P3}(x)$. In particular, $ord(Iso_{P3}(y)) = ord(Iso_{P3}(x))$. Since $P3$ is simple, $Iso_{P3}(y) = Iso_{P3}(x)$.

Corollary $Iso_{P3}(x) = Iso_{P3}(\beta x) = Iso_{P3}(\gamma x) = Iso_{P3}(\delta x)$,
and $ord(P3(x)) = ord(P3(\beta x)) = ord(P3(\gamma x)) = ord(P3(\delta x))$.

Suppose $P3(x) = \{x\}$. Then $Iso(x) > P3$. By the above corollary,

$P3(\beta x) = \{\beta x\}$, $P3(\gamma x) = \{\gamma x\}$ and $P3(\delta x) = \{\delta x\}$. If $x = \beta x$, then $Iso(x) > P2 \cdot P3$.

If $x = \gamma x$, then $Iso(x) > Q2 \cdot P3$. If $x = \delta x$, then $Iso(x) > R2 \cdot P3$.

On the other hand, if $ord(P3(x)) = 3$, then $Iso(x) \not> P3$.

If $P3(x) = P3(\beta x)$, then $Iso(x) > P2$. If $P3(x) = P3(\gamma x)$, then $Iso(x) > Q2'$, for some $Q2' \sim_{P622} Q2$.

If $P3(x) = P3(\delta x)$, then $Iso(x) > R2'$, for some $R2' \sim_{P622} R2$.

The two lemmas below now show that we can determine a $P622 - FD(n)$ from a $P622 - fd(n)$ and the isotropy subgroups at the elements of $P622 - fd(n)$.

Lemma 18 For $x, y \in (Z/n)^3$, if $y \in G(x)$, then $Iso(x) \sim_G Iso(y)$.

Proof $y = gx$, for some $g \in G$. Suppose $h \in Iso(y)$. Then $hgx = gx$, so $g^{-1}hg \in Iso(x)$. Hence, $Iso(y) \subset gIso(x)g^{-1}$. By exchanging the roles of x and y, we have the other inclusion.

Lemma 19 For $S < G$ and $x \in (Z/n)^3$, let $S \sim_G Iso(x)$. Then for some element $y \in G(x)$, $S = Iso(y)$.

Proof Let $Iso(x) = gSg^{-1}$, for some $g \in G$. For any $s \in S$, $gsg^{-1}x = x$. Thus, $sg^{-1}x = g^{-1}x$ and $s \in Iso(g^{-1}x)$. Since $Iso(x) \sim_G Iso(g^{-1}x)$, S is the isotropy subgroup at $g^{-1}x$.

Since Ψ is a complete set of representatives of conjugacy classes of subgroups of $P622$, for each $x_i \in P622 - fd(n)$ we can find $y_i \in P622(x_i)$ with $Iso(y_i) \in \Psi$, by the above lemma. Replacing each $x_i \in P622 - fd(n)$ by such y_i, we obtain a $P622 - FD(n)$.

Henceforth, we choose a fixed set for a $P622 - FD(n)$. For $\psi \in \Psi$, let

$$X(\psi) = \{x \in P622 - FD(n) \mid Iso(x) = \psi\}.$$

$P622 - FD(n)$ is the disjoint union of the sets $X(\psi)$. We will use the sets $X(\psi)$ as *building blocks* in computing fundamental domains by the actions of the subgroups of $P622$. We will see later that this gives us *uniqueness* of fundamental domains once we choose a $P622 - FD(n)$.

This property is crucial, as we will see, because we want to express a fundamental domain in more than one way.

Throughout the following discussion, let H be one of the groups $P6$, $P312$ or $P321$. We will now show a way of constructing an $H-FD(n)$ from a $P622-FD(n)$. Since $H \triangleleft P622$, H acting on a $P622-$orbit decomposes the orbit into $H-$orbits. The number of $H-$orbits in a $P622-$orbit is at most two, because there are two $H-$cosets in $P622$.

Lemma 20 For $x \in P622-FD(n)$, if $Iso(x) < H$, then $P622(x)$ is a union of two distinct $H-$orbits.

Proof Let $g \neq I$ be an element of a complementary subgroup of H in $P622$. Thus, $H \cap gH = \phi$. $P622(x) = H(x) \cup gH(x) = H(x) \cup H(gx)$.

Suppose $H(x) \cap H(gx) \neq \phi$. Then for some $h \in H$, $x = hgx$. But this implies that $hg \in Iso(x) < H$, which is a contradiction.

Lemma 21 For $x \in P622-FD(n)$, if $Iso(x) \not< H$, then $P622(x) = H(x)$.

Proof $Iso_H(x) = Iso(x) \cap H \neq Iso(x)$. Thus, $2 \cdot ord(Iso_H(x)) \leq ord(Iso(x))$.

$$ord(P622(x)) = \frac{12}{ord(Iso(x))}, \quad ord(H(x)) = \frac{6}{ord(Iso_H(x))}.$$

Since $P622(x) \supset H(x)$,

$$\frac{12}{ord(Iso(x))} \geq \frac{6}{ord(Iso_H(x))}, \quad \frac{2}{ord(Iso(x)} \geq \frac{1}{ord(Iso_H(x))}.$$

Hence $2 \cdot ord(Iso_H(x)) = ord(Iso(x))$, so $ord(P622(x)) = ord(H(x))$, and $P622(x) = H(x)$.

Theorem 18 $\cup_{\psi \in \Psi} C(H \cdot \psi)X(\psi)$ is an $H-FD(n)$.

Proof If $\psi < H$, then $C(H \cdot \psi) = C(H)$. If $\psi \not< H$, then $H \cdot \psi = P622$, and $C(H \cdot \psi) = I$. Thus, $\cup_{\psi \in \Psi} C(H \cdot \psi)X(\psi)$ contains exactly one element from each $H-$orbit, by the lemmas above. Hence $\cup_{\psi \in \Psi} C(H \cdot \psi)X(\psi)$ is an $H-fd(n)$.

We will now justify the use of the capital letters FD by showing that if $x' \in \cup_{\psi \in \Psi} C(H \cdot \psi)X(\psi)$, then $Iso_\psi(x) \in \Psi$. Note first that $C(H \cdot \psi)$ is a subgroup of a group of order 2. Since $C(H \cdot \psi) \in \Psi$,

$C(H \cdot \psi) < A$. Any $x' \in \cup_{\psi \in \Psi} C(H \cdot \psi)X(\psi)$ is of the form gx for $x \in P622 - FD(n)$ and $g \in C(H \cdot \psi)$. $Iso(gx) = gIso(x)g^{-1}$. Since $x \in P622 - FD(n)$, $Iso(x) \in \Psi$. Since $g \in A$, $gIso(x)g^{-1} = Iso(x)$. $Iso_H(x) = Iso(x) \cap H \in \Psi$, by theorem 13.

We will now decompose an $H - FD(n)$ by the isotropy subgroups in H. To do this, let

$$X(H : \psi') = \{x \in H - FD(n) \mid Iso_H(x) = \psi'\}.$$

We will set $X(H : \psi') = \phi$, for $\psi' \not< H$. Then

$$X(H : \psi') = \cup_{\psi \mid \psi \cap H = \psi'} C(H \cdot \psi)X(\psi).$$

Since $P3 \lhd H$, we can determine a $P3 - FD(n)$ from an $H - FD(n)$ in exactly the same way. For example, we can determine a $P3 - FD(n)$ from a $P6 - FD(n)$. The complementary subgroup of $P3$ in $P6$ is $P2$. $C_{P6}(P3 \cdot P6) = C_{P6}(P3 \cdot P2) = I$, $C_{P6}(P3 \cdot P3) = C_{P6}(P3 \cdot I) = P2$, and the following is a $P3 - FD(n)$.

$$\cup_{\psi \in \Psi} C_{P6}(P3 \cdot \psi)X(P6 : \psi)$$

Thus, once we have a $P622 - FD(n)$, we can construct a $\psi - FD(n)$ for all $\psi \lhd P622$, $\psi \in \Psi$.

We next want to show a method of calculating an A–fundamental domain in $(Z/n)^3$. Since

$$A\Big(P3\big(P622 - FD(n)\big)\Big) = P622\big(P622 - FD(n)\big) = (Z/n)^3,$$

we have that $P3\big(P622 - FD(n)\big)$ spans $(Z/n)^3$ by the action of A. Hence $P3\big(P622 - FD(n)\big)$ contains an A–fundamental domain in $(Z/n)^3$. Now if we can show that the A–orbits of any two distinct elements in $P3\big(P622 - FD(n)\big)$ are disjoint, we will have that $P3\big(P622 - FD(n)\big)$ is an A–fundamental domain in $(Z/n)^3$. So, let x_1 and x_2 be two distinct elements in $P3\big(P622 - FD(n)\big)$. Suppose $A(x_1) \cap A(x_2) \neq \phi$. Then $x_2 = ax_1$ for some $a \in A$. On the other hand, we can write x_1 and x_2 as $\alpha^i x_1'$ and $\alpha^j x_2'$, with x_1', $x_2' \in P622 - FD(n)$ and $\alpha \in P3$. Thus, $\alpha^j x_2'$ $= a\alpha^i x_1'$, $x_2' = \alpha^{-j} a \alpha^i x_1'$. But this implies that $x_2' \in P622(x_1')$ which is a contradiction. Hence $P3\big(P622 - FD(n)\big)$ is an A–fundamental domain in $(Z/n)^3$.

Let us look at the A–fundamental domain $P3\big(P622 - FD(n)\big)$. For $\psi > P3$, $P3\big(X(\psi)\big) =$

$X(\psi)$. Thus,

$$P3\big(P622 - FD(n)\big) = \Big(X(P622) \cup X(P6) \cup X(P312) \cup X(P321) \cup X(P3)\Big)$$
$$\bigcup P3\big(X(A) \cup X(P2) \cup X(Q2) \cup X(R2) \cup X(I)\big).$$

Since $P3$ is the complementary subgroup of A in $P622$, this $A-$fundamental domain can be written as

$$\cup_{\psi \in \Psi} C(A \cdot \psi) X(\psi).$$

Since the isotropy subgroup of any element under the action of A is a subgroup of A, and since every subgroup of A belongs in Ψ, this $A-$fundamental domain in $(Z/n)^3$ is an $A - FD(n)$ for the collection Ψ.

Denote the subset of $A - FD(n)$ consisting of elements whose isotropy subgroup in A is ψ' by $X(A : \psi')$. Then we have $X(A : \psi') = \cup_{\psi | \psi \cap A = \psi'} C(A \cdot \psi) X(\psi)$.

For the rest of this chapter, let J be a subgroup of A of order 2. Replacing $P622$ by A and H by J, we can construct $J - FD(n)$ from an $A - FD(n)$ as before : $C_A(P2)$ is either $Q2$ or $R2$. $C_A(Q2)$ is either $P2$ or $R2$. $C_A(R2)$ is either $P2$ or $Q2$. We will set $C_A(J)$ to be $P2$ or $Q2$.

$$\cup_{\psi \in \Psi} C_A(J \cdot \psi) X(A : \psi) \text{ is a } J - FD(n).$$

Thus, we have obtained a $\psi - FD(n)$, for all $\psi \in \Psi$.

Comment For any $\psi \in \Psi$, we have seen that there is a $\psi' \in \Psi$ such that $\psi^* \sim \psi'$. Hence we can obtain a $\psi^* - fd(n)$ from a $\psi' - FD(n)$ by elementwise multiplication by τ. Setting $\Psi^* = \{\psi^* \mid \psi \in \Psi\}$, a ψ^*-fundamental domain obtained this way has the property that the isotropy subgroup in ψ^* at any element in this fundamental domain belongs in Ψ^*. Since there is no danger of ambiguity, we will denote a $\psi^* - fd(n)$ with this property for the collection Ψ^* by $\psi^* - FD(n)$.

Before moving onto the next chapter, we will show that indeed the sets $X(\psi)$, $\psi \in \Psi$ play the role of building blocks. Our Main Theorem below follows as a corollary to theorem 19. We use

the properties of the collection Ψ that we proved in the last chapter to prove theorem 19.

Theorem 19 Let $\psi_1 < \psi_2$. Then $C(\psi_1 \cdot \psi)X(\psi) = C(\psi_2 \cdot \psi) \cdot C_{\psi_2}(\psi_1 \cdot \psi)X(\psi)$.

Proof By theorem 23, we can write $C(\psi_1 \cdot \psi) = C(\psi_2 \cdot \psi) \cdot C_{\psi_2 \cdot \psi}(\psi_1 \cdot \psi)$. Note that

$C_{\psi_2}(\psi_1 \cdot \psi) < C_{\psi_2 \cdot \psi}(\psi_1 \cdot \psi) < C_{\psi_2}(\psi_1 \cdot \psi) \cdot \psi$.

Thus, $C(\psi_2 \cdot \psi)C_{\psi_2}(\psi_1 \cdot \psi)X(\psi) \subset C(\psi_1 \cdot \psi)X(\psi) \subset C(\psi_2 \cdot \psi)C_{\psi_2}(\psi_1 \cdot \psi) \cdot \psi X(\psi)$.

But $\psi X(\psi) = X(\psi)$. Therefore, $C(\psi_2 \cdot \psi)C_{\psi_2}(\psi_1 \cdot \psi)X(\psi) = C(\psi_2 \cdot \psi)C_{\psi_2}(\psi_1 \cdot \psi) \cdot \psi X(\psi)$.

We have then $C(\psi_1 \cdot \psi)X(\psi) = C(\psi_2 \cdot \psi) \cdot C_{\psi_2}(\psi_1 \cdot \psi)X(\psi)$.

Main Theorem For ψ_1, $\psi_2 \in \Psi$, and $\psi_1 < \psi_2$ the $\psi_1 - FD(n)$, we computed above can be written as

$$\cup_{\psi \in \Psi} C_{\psi_2}(\psi_1 \cdot \psi)X(\psi_2 : \psi),$$

where $\cup_{\psi \in \Psi} X(\psi_2 : \psi)$ is a $\psi_2 - FD(n)$.

4. Invariant Fourier Transforms.

For $\psi \in \Psi$, let us now look at $F_\psi(n)$, the ψ-invariant Fourier Transform. For $f \in L_\psi(n)$ and $x^* \in \psi^* - FD(n)$,

$$F_\psi(n)f(x^*) = \sum_{x \in \psi - FD(n)} f(x)\mathcal{F}_\psi(x^*, cx), \qquad \mathcal{F}_\psi(x^*, cx) = \sum_{c \in Ind_\psi(x)} \omega_n^{<x^*, cx>},$$

where $Ind_\psi(x)$ is an indexing subgroup of $\psi(x)$. Suppose ψ_1, $\psi_2 \in \Psi$ and $\psi_1 \triangleleft \psi_2$. Then $\psi_2 - FD(n) \subset \psi_1 - FD(n)$. Let us compare $\mathcal{F}_{\psi_1}(x^*, c_1x)$ and $\mathcal{F}_{\psi_2}(x^*, c_2x)$:

$$\mathcal{F}_{\psi_1}(x^*, c_1x) = \sum_{c_1 \in Ind_{\psi_1}(x)} \omega_n^{<x^*, c_1x>}, \tag{5}$$

$$\mathcal{F}_{\psi_2}(x^*, c_2x) = \sum_{c_2 \in Ind_{\psi_2}(x)} \omega_n^{<x^*, c_2x>}. \tag{6}$$

Since $\psi_1(x) \subset \psi_2(x)$, we can choose an indexing subgroup of $\psi_1(x)$ as a subgroup of an indexing subgroup of $\psi_2(x)$. Thus, we can make use of the sum in (5) in evaluating the sum in (6). By the Main Theorem, we can write $\psi_1 - FD(n)$ in the form

$$\cup_{\psi \in \Psi} C_{\psi_2}(\psi_1 \cdot \psi) X(\psi_2 : \psi),$$

where $\cup_{\psi \in \Psi} X(\psi_2 : \psi)$ is a $\psi_2 - FD(n)$.

Thus, for $x \in C_{\psi_2}(\psi_1 \cdot \psi)X(\psi_2 : \psi)$, $\psi_2(x) = C_{\psi_2}(\psi_1 \cdot \psi) \cdot \psi_1(x)$. Now we can rewrite (6) as

$$\sum_{d \in C_{\psi_2}(\psi_1 \cdot \psi)} \Big(\sum_{c_1 \in Ind_{\psi_1}(x)} \omega_n^{<x^*, c_1 dx>} \Big). \tag{7}$$

Since each dx, for $d \in C_{\psi_2}(\psi_1 \cdot \psi)$ and $x \in X(\psi_2 : \psi)$, belongs to $\psi_1 - FD(n)$, the inner sum of (7) occurs as the sum in (5).

Now not only is $\psi_2 - FD(n) \subset \psi_1 - FD(n)$, but also $\psi_2^* - FD(n) \subset \psi_1^* - FD(n)$. $\mathcal{F}_{\psi_2}(n)$ is obtained from $\mathcal{F}_{\psi_1}(n)$ by crossing out the rows indexed by $x^* \notin \psi_2^* - FD(n)$ and summing the columns indexed by dx for $d \in C_{\psi_2}(\psi_1 \cdot Iso_{\psi_2}(x))$.

Thus once we find $\mathcal{F}_{P3}(n)$, we can modify it to compute $\mathcal{F}_H(n)$. From $\mathcal{F}_H(n)$, we can compute $\mathcal{F}_{P622}(n)$. Also from $\mathcal{F}_J(n)$, we can compute $\mathcal{F}_A(n)$.

5. Invariant Product Construction.

Let $n = p \cdot q$, where p and q are relatively prime natural numbers. Using the Chinese Remainder theorem, we can decompose the ring $(Z/n)^3$ into $(Z/p)^3 \times (Z/q)^3$. Using the tensor product presentation, we can decompose the linear transformation $F(n)$ into $F(p) \otimes F(q)$. Moreover, by iterating, we can decompose $(Z/n)^3$ and $F(n)$ in terms of the prime factors of n. In this section, we will be concerned with the task of determining the invariant product construction for the groups $\psi \in \Psi$. We will also show that we can iterate this construction. Thus, we will have a method of computing the ψ–invariant Fourier Transform on $(Z/n)^3$ in terms of invariant Fourier Transforms on the prime factors of n.

For $f \in L(p) \otimes L(q)$ and $(y_o, z_o) \in (Z/p)^3 \times (Z/q)^3$, define

$$(Ip \otimes F(q))f(y_o, z_o) = \sum_{z \in (Z/q)^3} f(y_o, z) \cdot \omega_n^{<z_o, z>},$$

$$(F(p) \otimes Iq)f(y_o, z_o) = \sum_{y \in (Z/p)^3} f(y, z_o) \cdot \omega_n^{<y_o, y>}.$$

$Ip \otimes F(q)$ and $F(p) \otimes Iq$ are linear transformations of $L(p) \otimes L(q)$. Denote the composition of linear tranforms by $\circ$. We have then

$$F(p) \otimes F(q) = (Ip \otimes F(q)) \circ (F(p) \otimes Iq).$$

Let $f \in L_\psi(p, q)$. For $(y_o, z_o) \in (Z/p)^3 \times (Z/q)^3$ and $g \in \psi$, $h = g^*$,

$$(F(p) \otimes Iq)f(hy_o, gz_o) = \sum_{y \in (Z/p)^3} f(y, gz_o) \cdot \omega_n^{<hy_o, y>}.$$

Since $< hy_o, y > = < y_o, h^t y > = < y_o, g^{-1} y >$, we may rewrite

$$(F(p) \otimes Iq)f(hy_o, gz_o) = \sum_{y \in (Z/p)^3} f(y, gz_o) \cdot \omega_n^{<y_o, g^{-1} y>}.$$

Replacing y by gy above,

$$(F(p) \otimes Iq)f(hy_o, gz_o) = \sum_{gy \in (Z/p)^3} f(gy, gz_o) \cdot \omega_n^{<y_o, y>}.$$

Since $f \in L_\psi(p,q)$, $f(gy, gz_0) = f(y, z_0)$. We have now

$$(F(p) \otimes Iq) f(hy_0, gz_0) = \sum_{gy \in (Z/p)^3} f(y, z_0) \cdot \omega_n^{<y_0, y>}.$$

As gy ranges over $(Z/p)^3$, y ranges over $(Z/p)^3$. Thus

$$(F(p) \otimes Iq) f(hy_0, gz_0) = \sum_{y \in (Z/p)^3} f(y, z_0) \cdot \omega_n^{<y_0, y>} = (F(p) \otimes Iq) f(y_0, z_0).$$

i.e., $F(p) \otimes Iq$ maps a (g,g)-invariant function into a (h,g)-invariant function. In exactly the same way we can show that if $f \in L(p) \otimes L(q)$ is (h,g)-invaraiant, then $(Ip \otimes F(q))f$ is (h,h)-invariant.

For $\psi \in \Psi$, we will denote by $\overline{\psi}$ the set of elements (h,g) where $g \in \psi$ and $h = g^*$. Denote the set of $\overline{\psi}$-invariant functions in $(Z/p)^3 \times (Z/q)^3$ by $L_{\overline{\psi}}(p,q)$. We have then

$$L_\psi(p,q) \xrightarrow{F(p) \otimes Iq} L_{\overline{\psi}}(p,q) \xrightarrow{Ip \otimes F(q)} L_{\psi^*}(p,q).$$

For any $\psi \in \Psi$, we have the precomputation required in the ψ–invariant product construction. They are $\psi_j - FD(p)$, $\psi_j^* - FD(p)$, $\psi_j - FD(q)$, $\psi_j^* - FD(q)$ and ψ_j–invariant modules on p and q for $\psi_j < \psi$ and $\psi_j \in \Psi$. The invariant product construction for ψ consists of the following three procedures :

(a′) Construct a $\psi - fd(p,q)$ and a $\overline{\psi} - fd(p,q)_1$ such that for $f \in L_\psi(p,q)$, we can compute $(F(p) \otimes Iq)f$ in terms of $F_{\psi_j}(p)$.

(b′) Construct a $\overline{\psi} - fd(p,q)_2$ and a $\psi^* - fd(p,q)$ such that for $f \in L_{\overline{\psi}}(p,q)$, we can compute $(Ip \otimes F(q))f$ in terms of $F_{\psi_j}(q)$.

(c′) Determine an orbit exchange for the two $\overline{\psi}$–fundamental domains $\overline{\psi} - fd(p,q)_1$ and $\overline{\psi} - fd(p,q)_2$.

To construct the desired fundamental domains, we will prove some preliminary facts.

Definition Let A be a subset of $(Z/n)^3$. A subset B of $(Z/n)^3$ is called a G–fundamental domain in A if $G(B) \supset A$, and for $b, b' \in B$, $G(b) \cap G(b') = \phi$. (This definition is the same as the previous definition in case $A = (Z/n)^3$. This is because $G(B) \subset (Z/n)^3$ for any $B \subset (Z/n)^3$.)

Lemma 22. Let A_1 and A_2 be subsets of $(Z/n)^3$ with $G(A_1) \cap G(A_2) = \phi$. A $G-$fundamental domain in $A_1 \cup A_2$ is the union of fundamental domains of A_1 and A_2.

Proof Let F_1 and F_2 be fundamental domains of A_1 and A_2 respectively.

$G(F_1 \cup F_2) = G(F_1) \cup G(F_2) = A_1 \cup A_2$. Hence $F_1 \cup F_2$ spans $A_1 \cup A - 2$ by the action of G. Since $G(F_1) \cap G(F_2) = \phi$, $G-$orbits of any two distinct elements of $F_1 \cup F_2$ are disjoint.

Lemma 23 Let p and q be relatively natural prime numbers. For a subset $A \subset (Z/p)^3$ and $B \subset (Z/q)^3$, $G(A \times B) = G(A) \times G(B)$, if $G(A) = A$ or $G(B) = B$.

Proof $G(A \times B) = \{(ga, gb) \mid g \in G, (a, b) \in A \times B\}$.

$G(A) \times G(B) = \{(ga, g'b) \mid g, g' \in G, (a, b) \in A \times B\}$. Hence $G(A) \times G(B) \supset G(A \times B)$. Suppose $G(A) = A$ and let $(ga, g'b) \in G(A) \times G(B)$. Since $G(A) = A$, $ga = g'a'$ for some $a' \in A$. Thus $(ga, g'b) = (g'a', g'b) \in G(A \times B)$.

Notation $Z(\psi : \psi_j) = \{z \in \psi - FD(q) \mid Iso_\psi(z) = \psi_j\}$.

$Y(\psi : \psi_j) = \{y \in \psi - FD(p) \mid Iso_\psi(y) = \psi_j\}$.

Construction of (a') :

Theorem 20 $\cup_j(\psi_j - FD(p) \times Z(\psi : \psi_j))$ is a $\psi-$fundamental domain in $(Z/p)^3 \times (Z/q)^3$.

Proof We will first show that for $z \in Z(\psi : \psi_j)$, $\psi_j - FD(n) \times \{z\}$ is a $\psi-$fundamental domain in $(Z/p)^3 \times \psi(z)$. Then, by the repeated application of Lemma 22, we will have the desired result.

Let $z \in Z(\psi : \psi_j)$. Then $\psi_j(z) = \{z\}$. By Lemma 23, $\psi(\psi_j - FD(p) \times \{z\}) = \psi\Big(\psi_j(\psi_j - FD(p) \times \{z\})\Big) = \psi\big((Z/p)^3 \times \{z\}\big) = (Z/p)^3 \times \psi(z)$. Suppose for y_1 and $y_2 \in \psi_j - FD(p)$ and $y_1 \neq y_2$, $\psi(y_1, z) \cap \psi(y_2, z) \neq \phi$. Then $(y_1, z) = (gy_2, gz)$, for some $g \in \psi$. This implies that $g \in Iso_\psi(z) = \psi_j$ and $y_2 \in \psi_j(y_1)$ which is a contradiction.

In exactly the same way we can prove the following theorem.

Theorem 21 $\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j))$ is a $\overline{\psi} - fd(p,q)$.

For $f \in L_\psi(p,q)$, $z \in Z(\psi : \psi_j)$, $y \in \psi_j - FD(p)$ and $g \in \psi_j$, $f(g(y,z)) = f(gy, gz) = f(gy, z)$. Also for such f, $(F(p) \otimes Iq)f \in L_{\overline{\psi}}(p,q)$. Thus for $z \in Z(\psi, \psi_j)$ and $y^* \in (\psi)^* - FD(p)$, $\overline{g} \in \overline{\psi_j}$,

$$(F(p) \otimes Iq)f(\overline{g}(y^*, z)) = (F(p) \otimes Iq)f(g^*y^*, gz) = (F(p) \otimes Iq)f(g^*y, z).$$

For $z \in Z(\psi : \psi_j)$, $y^* \in \psi_j^* - FD(p)$,

$$(F(p) \otimes Iq)f(y^*, z) = (F_{\psi_j}(p) \otimes Iq)f(y^*, z).$$

Construction of (b') :

$\cup_j(Y(\psi^*, \psi_j^*) \times \psi_j - FD(q))$ and $\cup_j(Y(\psi^*, \psi_j^*) \times \psi_j^* - FD(q))$ are $\overline{\psi} - fd(p,q)$ and $\psi^* - fd(p,q)$ respectively.

For $f \in L_{\overline{\psi}}(p,q)$, $y \in Y(\psi^* : \psi_j^*)$, $z \in \psi - FD(q)$, and $g \in \psi_j$,

$$f(\overline{g}(y^*, z)) = f(g^*y^*, gz) = f(y^*, gz).$$

For $f \in L_{\overline{\psi}}(p,q)$, $(Ip \otimes F(q))f \in L_{\psi^*}(p,q)$. Thus for $y^* \in Y(\psi^* : \psi_j^*)$ and $z^* \in \psi_j^* - FD(q)$, $g^* \in \psi_j^*$,

$$(Ip \otimes F(q))f(g^*(y^*, z^*)) = (Ip \otimes F(q))f(y^*, g^*z^*).$$

For $y^* \in Y(\psi_j^* : \psi^*)$, and $z^* \in \psi_j^* - FD(q)$,

$$(Ip \otimes F(q))f(y^*, z^*) = (Ip \otimes F_{\psi_j}(q))f(y^*, z^*).$$

Determination of (c') :

We can write the two $\overline{\psi} - FD(p,q)$ as follows :

$$\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j)) = \cup_j\big(\cup_k C_{\psi^*}(\psi_j^* \cdot \psi_k^*)Y(\psi^* : \psi_k^*)) \times Z(\psi : \psi_j)\big)$$

$$\cup_j(Y(\psi^* : \psi_j^*) \times \psi_j - FD(q)) = \cup_j\big(Y(\psi^* : \psi_j^*) \times \cup_k C_\psi(\psi_j \cdot \psi_k)Z(\psi : \psi_k)\big).$$

Any element belonging in $\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j))$ is of the form (c^*y^*, z), where $c^* \in C_{\psi^*}(\psi_j^* \cdot \psi_k^*)$, $y^* \in Y(\psi^* : \psi_k^*)$ and $z \in Z(\psi : \psi_j)$. Define the mapping Π on $\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j))$ by

$$\Pi : (c^*y^*, z) \mapsto (y^*, c^{-1}z).$$

Theorem 22 The mapping Π defined above is an orbit exchange for $\overline{\psi}$.

Proof $\Pi\big(C_{\psi^*}(\psi_j^* \cdot \psi_k^*)Y(\psi^* : \psi_k^*)) \times Z(\psi : \psi_j)\big) = \big(Y(\psi^* : \psi_k^*) \times C_\psi(\psi_j \cdot \psi_k)Z(\psi : \psi_j)\big)$.

$\Pi\big(\cup_j(\psi_j^* - FD(p) \times Z(\psi : \psi_j))\big)$

$=\Pi\big(\cup_j\big(\cup_k(C_{\psi^*}(\psi_j^* \cdot \psi_k^*)Y(\psi^* : \psi_k^*) \times Z(\psi : \psi_j))\big)\big)$

$= \cup_j\big(\cup_k Y(\psi^* : \psi_k^*) \times (C_\psi(\psi_j \cdot \psi_k)Z(\psi : \psi_j))\big)$

$= \cup_j\big(\cup_k Y(\psi^* : \psi_k^*) \times C_\psi(\psi_k \cdot \psi_j)Z(\psi : \psi_j)\big)$

$= \cup_k\big(Y(\psi^* : \psi_k^*) \times \cup_j\big(C_\psi(\psi_k \cdot \psi_j)Z(\psi : \psi_j)\big)\big)$

$= \cup_k(Y(\psi^* : \psi_k^*) \times \psi_k - FD(q)).$

We will summarize the results of this section in terms of matrices. To this end, we will consider the fundamental domains on the product space $(Z/p)^3 \times (Z/q)^3$ as lexicographically ordered sets. Let $f \in L_\psi(p, q)$. Denote by $[YZ]_\psi$, a column vector of entries $f(y, z)$ indexed by $(y, z) \in \cup_j(\psi_j - FD(p) \times Z(\psi : \psi_j)$. Denote by $[Y^*Z]_\psi$ a column vector of entries $(F(p) \otimes Iq)f(y^*, z)$ indexed by $(y^*, z) \in \cup_j(\psi_j{}^* - FD(p) \times Z(\psi : \psi_j)$. Let q_j be the order of the set $Z(\psi : \psi_j)$. Matrix representation of $\psi-$invariant linear transformation $F(p) \otimes Iq$ is

$$\oplus_j(\mathcal{F}_{\psi_j}(p) \otimes Iq_j).$$

Denote by $[\Pi X^*Y]_\psi$ a column vector of entries $(F(p) \otimes Iq)f)(y^*, z)$ indexed by $(y^*, z) \in \cup_j(Y(\psi^* : \psi_j{}^*) \times \psi - FD(q))$. Denote by $[Y^*Z^*]_\psi$ a column vector of entries $(F(p) \otimes F(q))f(y^*, z^*)$ indexed by $(y^*, z^*) \in \cup_k(Y(\psi^* : \psi_k{}^*) \times \psi_k{}^* - FD(q)$. Let p_k be the order of the set $Y(\psi^* : \psi_k{}^*)$. Matrix representation of the $\psi-$invariant linear transformation $Ip \otimes F(q)$ is

$$\oplus_k(Ip_k \otimes \mathcal{F}_{\psi_k}(q)).$$

The vector $[Y^*Z^*]_\psi$ is the matrix product

$$\oplus_k(Im_k \otimes \mathcal{F}_{\psi_k}(n_2)) \cdot P \cdot \oplus_j(\mathcal{F}_{\psi_j}(n_1) \otimes In_j) \cdot [YZ]_\psi,$$

where P is the matrix of the permutation induced by Π.

Theorem 23 We can iterate the invariant product construction.

Proof To prove this, we will show that the $\psi - fd(p,q)$ that we computed has the following property : We can find a collection Ψ' having the same properties as Ψ such that the isotropy subgroup of an element in $\psi - fd(p,q)$ is contained in Ψ' :

For $(y,z) \in (Z/p)^3 \times (Z/q)^3$, $Iso(y,z) = (Iso(y) \cap Iso(z), Iso(y) \cap Iso(z))$.

We computed $\psi - fd(p,q)$ from $\psi - FD(p)$ and $\psi - FD(q)$. Since Ψ is closed under intersection of its elements, if $(y,z) \in \psi - fd(p,q)$, then $Iso(y,z) = (\psi_j, \psi_j)$, for some $\psi_j \in \Psi$. Considr the following collecction

$$\{(\psi,\psi) \mid \psi \in \Psi\}$$

of representatives of the conjugacy classes of the automorphism groups on the product ring. It is easy to show that the collection has the same properties as those of the collection Ψ. Thus we have

$$\Psi' = \{(\psi,\psi) \mid \psi \in \Psi\},$$

and we can iterate the product construction.

BIBLIOGRAPHY

[1] L.Auslander, *An Account of the Theorey of Crystallographic Groups*, PAMS 16 (1965), 1230–1236.

[2] L.Auslander and M.Shenefelt, *Fourier Transforms That Respect Crystallographic Symmetries*, IBM Journal of Research and Development, V 31, No 2 (1987).

[3] D.Bantz and M.Zwick, *The Use of Symmetry with the Fast Fourier Algorithm*, Acta Crystallogrphica, A30 (1974), 257–260.

[4] L.Ten Eyck, *Crystallographic Fast Fourier Transforms*, Acta Crystallographica, A29 (1973), 183–191

[5] D.R.Farkas, *Crystallographic Groups and Their Mathematics*, Rocky Mountain Journal of Mathematics, V 11 (1981), 511–551.

[6] P.R.Halmos, *Finite–Dimensional Vector Space*, Springer–Verlag, 1974

[7] T.W.Hungerford, *Algebra*, Springer–Verlag, 1974

[8] C.M.Radar, Discrete Fourier Transforms When the number of Data Samples is Prime, Proc. IEEE, 56(1968), 1107–1108.

[9] Ramachandran and Srinivasan, *Fourier Methods in Crystallograhy*, Wiley Monograms in Crystallography, Wiley Interscience, 1970.

[10] S.Winograd, On Computing the Discrete Fourier Trnsform, Mathematics of Computation, 32, 175–199.