Oct. 13, 2006 (Fri.)

2.6. **symmetry of the plane.** A map from plane itself is called a **rigid motion**, or an **isometry**, if it is distance-preserving. Let S be a subset of the plane. Then the subgroups of rigid motions preserving S is called the **symmetry of** S. It's well-known that:

Example 2.6.1.

Let S be the regular n-gon centered at the origin. Then the symmetry of S id the group D_{2n}. □

In order to build this is a more solid foundation, we need to work a little bit more.

A list of rigid motions consists of:
1. Orientation-preserving motions:
a. Translation.
b. Rotation.
2. Orientation-reversing motions:
a. Reflection.
b. Glide reflection, i.e. reflecting about a line l and then translating by a non-zero vector a parallel to l.

Theorem 2.6.2. *The above list is complete.*

Sketch. We first fix some notations:
t_a: translation by a vector a.
ρ_θ: rotation by an angle θ about the origin.
r: reflection about the x-axis.

Step 1. Orientation preserving motions that fix the origin are $\{\rho_\theta\}$.
Step 2. Let m ne an orientation preserving motion. If $m(o) = a$, then $t_{-a}m = \rho_\theta$ for some θ. by Step 1. Thus $m = t_a\rho_\theta$.
Step 3. If m is not a translation, i.e. $\theta \neq 0$, then m is a rotation about a point p. To see this, first show that m has a fixed point, denoted p, if $\theta \neq 0$. A point on the plane can be written as $p + x$,

$$m(p+x) = t_a\rho_\theta(p+x) = \rho_\theta(p+x)+a = \rho_\theta(p)+\rho_\theta(x)+a = p+\rho_\theta(x).$$

Step 4. Orientation reversing motions that fix the origin are $\{\rho_\theta r\}$. For given such m, it's clear that rm preserves the orientation and fixes the origin. So $rm = \rho_\theta$ for some θ. Thus $m = r\rho_\theta = \rho_{-\theta}r$. Also note that $\rho_\theta r$ is the reflection about l, denoted r_l, which is the line obtained by rotating x-axis by $\frac{1}{2}\theta$.
Step 5. Let m be an orientation reversing motion. Then $m(o) = a$ for some a. Thus $t_{-a}m$ is an orientation reversing motion that fixes origin, hence $t_{-a}m = r_l$. Therefore, $m = t_a r_l$ which is a glide reflection. □

Indeed, let $O(2,\mathbb{R})$ be the subgroup of motions that fix the origin. Then $O(2,\mathbb{R})$ is generated by $\{\rho_\theta, r\}$. Let M be the groups of plane rigid motions, then there is a group action $M \times \mathbb{R}^2 \to \mathbb{R}^2$. The orbit of o is the whole $\mathbb{R}^2$ and the stabilizer of o is $O(2, \mathbb{R})$.

For readers who want to know more about symmetry, we refer [Artin], Chapter 5.

2.7. **abelian groups.** In this section, we are going to study a simple but important category of groups, the abelian groups.

Given an abelian group G, we usually use $+$ to denote the operation. We say that G can be generated by $X \subset G$, denoted $G =< X >$, if every element of G can be written as $\sum n_i x_i$ for some $n_i \in \mathbb{Z}$ and $x_i \in X$. Note that $n_i \neq 0$ for all but finitely many i.

A **basis** of an abelian group G is a *linearly independent* generating subset X. That is for distinct $x_1, ..., x_k \in X$, $\sum n_i x_i = 0$ implies that n_i for all i.

An abelian group with a basis is called a **free abelian group**. And the rank, denoted $rk(F)$, is $|X|$.

It's easy to prove that an abelian group is free if and only if it's a direct sum of $\mathbb{Z}$.

On the other hand, given a set X, we can always construct a free abelian group on the set X by consider the set

$$F := \{\sum n_x x | x \in X, n_x \in \mathbb{Z}, n_x = 0 \text{ for all but finitely many } x\}.$$

The group operation on F is nothing but $\sum n_x x + \sum m_x x := \sum (n_x + m_x)x$. It's clear that X is a basis of F in this construction.

Example 2.7.1.

This construction appeared, for example, in algebraic topology. The groups of 1-chains is the free abelian group on the set of simplicial 1-chains. □

Example 2.7.2.

Let X be a Riemann surface, then the group of divisors, $Div(X)$, is the free abelian group on the set X. □

It has the following universal property:

Proposition 2.7.3. *Let F be a free abelian group with basis X. For any function $f : X \to G$ to an abelian group G. There exist a unique homomorphism $\varphi : F \to G$ extending f.*

Proof. Let $\varphi(\sum n_x x) = \sum n_x f(x)$, then verify it. □

Corollary 2.7.4. *Every abelian group is a quotient of a free abelian group.*

Proof. Let$G$ be an abelian group. Let F be the free abelian group on the set G. Consider $f : G \to G$ the identity map. Then we are done. □

Example 2.7.5.

$\mathbb{Q}$ can be describe as following. Let $X = \{x_1, ..., x_n, ...\}$ and F the free abelian group on the set X. Take $f : X \to \mathbb{Q}$ by $f(x_i) = \frac{1}{i}$. Then $\mathbb{Q}$ is a quotient of F. □

We are now ready to state develop to main theorem of this section. We need the following:

Lemma 2.7.6. *If $\{x_1, ..., x_n\}$ is a basis of F, then $\{x_1, ..., x_{j-1}, x_j + ax_i, x_{j+1}, ..., x_n\}$ is also a basis of F for $i \neq j$ and $a \in \mathbb{Z}$.*

Theorem 2.7.7. *Let F be a free abelian group of rank n and G is a non-zero subgroup of F, then there exists a basis $\{x_1, ..., x_n\}$ of F, an integer r $(1 \leq r \leq n)$ and positive integer $d_1, ..., d_r$ such that $d_1|d_2|...|d_r$ and G is free abelian group with basis $\{d_1x_1, ..., d_rx_r\}$.*

Sketch. If $n = 1$, this is easy.

By induction, we assume that the theorem is true for all abelian groups of rank $\leq n - 1$. Let

$$S := \{s \in \mathbb{Z} | sy_1 + ...k_ny_n \in G, \text{ for some basis of } F\ , y_1, ..., y_n\}.$$

Let d_1 be the smallest positive integer in S. By changing basis, we may have $\{x_1, y_2, ..., y_n\}$ basis of F and $d_1x_1 \in G$.

Let $H =< y_2, ..., y_n >$. It's clear that $F = H \oplus \mathbb{Z}x_1$. We claim that $G = (H \cap G) \oplus \mathbb{Z}d_1x_1$.

Apply induction hypothesis to $G \cap H < H$, then we are done. □

Corollary 2.7.8 (fundamental theorem of finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then there exist an integer r and positive integers $d_1|d_2|...|d_t$ such that*

$$G \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t} \oplus \mathbb{Z}^r.$$

Proof. Let X be a finite generating set of G. And let F be the free abelian group on the set X. Then there is a surjective homomorphism $F \to G$. Apply Theorem 2.7.7 to $\ker < F$. □

Now we restrict ourselves to finite abelian groups. Let G be a finite abelian group, by Corollary 2.7.8,

$$G \cong \mathbb{Z}_{d_1} \oplus ... \oplus \mathbb{Z}_{d_t}.$$

These $d_1, ..., d_t$ are called **invariant factors**. We consider the factorization of d_i into prime factors, then we have for all i,

$$d_i = p_1^{a_{i,1}} ... p_k^{a_{i,k}}.$$

By Chinese Remainder Theorem, we have for all i,

$$\mathbb{Z}_{d_i} \cong \mathbb{Z}_{p_1^{a_{i,1}}} \oplus ... \oplus \mathbb{Z}_{p_k^{a_{i,k}}}.$$

Therefore,

$$G \cong \oplus_{j=1}^{k} (\oplus_{i=1}^{t} \mathbb{Z}_{p_j^{a_{i,j}}}).$$

It's clear that $\oplus_{i=1}^{t}\mathbb{Z}_{{p_j}^{a_{i,j}}}$ is the Sylow p_j-subgroup. And these $p_j^{a_{i,j}}$ are called **elementary divisors**.

Example 2.7.9.

Let $G = \mathbb{Z}_{100} \oplus \mathbb{Z}_{40}$. By Chinese Remainder Theorem, $\mathbb{Z}_{100} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$ and $\mathbb{Z}_{40} \cong \mathbb{Z}_8 \oplus \mathbb{Z}_5$. Thus

$$G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{20} \oplus \mathbb{Z}_{200}.$$

So invariant factors are $20, 200$ and elementary divisors are $4, 8, 5, 25$. $\square$

Example 2.7.10.

Let $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Then invariant factors are $(m, n), [m, n]$, the gcd and lcm of m, n. $\square$

Let G be an abelian group, there there is a natural important homomorphism $m : G \to G$ by $m(x) := mx$ for $m \in \mathbb{N}$. The image is denoted mG and kernel is denoted $G[m]$. Let $G(p) = \{u \in G | o(u) = p^n \text{ for some } n \geq 0\}$. One can show that $G(p)$ is the Sylow p-subgroup of G. And G is a direct sum of Sylow subgroups. Thus it remains to study finite abelian p-groups. The only non-trivial part of classical theory is showing that a finite abelian p-group is a direct sum of cyclic p-groups.