A Numerical example. Let $n = 11$ and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 4 & 3 & 1 & 7 & 8 & 10 & 6 & 9 \end{pmatrix}.$$

Then

$$\sigma = (1\ 2\ 5)(3\ 4)(6\ 7\ 8\ 10\ 9).$$

Now,

$$\text{sgn}(\ (1\ 2\ 5)\ ) = 1, \quad \text{sgn}(\ (3\ 4)\ ) = -1, \quad \text{sgn}(\ (6\ 7\ 8\ 10\ 9)\ ) = 1.$$

We conclude that $\text{sgn}(\sigma) = -1$.

Realizing S_n as linear transformations. Let $\mathbb{F}$ be any field. Let $\sigma \in S_n$. There is a unique linear transformation Dummit & Foote p.810

$$T_\sigma : \mathbb{F}^n \longrightarrow \mathbb{F}^n,$$

such that

$$T(e_i) = e_{\sigma(i)}, \quad i = 1, \ldots n,$$

where, as usual, $e_1, \ldots, e_n$ are the standard basis of $\mathbb{F}^n$. Note that

$$T_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}.$$

(For example, because $T_\sigma x_1 e_1 = x_{\sigma^{-1}(1)} e_1$, the $\sigma(1)$ coordinate is x_1, namely, in the $\sigma(1)$ place we have the entry $x_{\sigma^{-1}(\sigma(1))}$.) Since for every i we have $T_\sigma T_\tau(e_i) = T_\sigma e_{\tau(i)} = e_{\sigma\tau(i)} = T_{\sigma\tau} e_i$, we have the relation

$$T_\sigma T_\tau = T_{\sigma\tau}.$$

The matrix representing T_σ is the matrix (a_{ij}) with $a_{ij} = 0$ unless $i = \sigma(j)$. For example, for $n = 4$ the matrices representing the permutations $(12)(34)$ and $(1\ 2\ 3\ 4)$ are, respectively

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Otherwise said,[6]

$$T_\sigma = \left(e_{\sigma(1)} \mid e_{\sigma(2)} \mid \ldots \mid e_{\sigma(n)}\right) = \left(\begin{array}{c} e_{\sigma^{-1}(1)} \\ \hline e_{\sigma^{-1}(2)} \\ \hline \vdots \\ \hline e_{\sigma^{-1}(n)} \end{array}\right).$$

[6]This gives the interesting relation $T_{\sigma^{-1}} = T_\sigma^t$. Because $\sigma \mapsto T_\sigma$ is a group homomorphism we may conclude that $T_\sigma^{-1} = T_\sigma^t$. Of course for a general matrix this doesn't hold.

Exercise 2.4.3. Prove that the set of upper triangular matrices in $\mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F}$ is any field, forms a subgroup of $\mathrm{GL}_n(F)$. It is also called a Borel subgroup.

Prove that the set of upper triangular matrices in $\mathrm{GL}_n(\mathbb{F})$ with 1 on the diagonal, where $\mathbb{F}$ is any field, forms a subgroup of $\mathrm{GL}_n(F)$. It is also called a unipotent subgroup.

Calculate the cardinality of these groups when $\mathbb{F}$ is a finite field of q elements.

end of 3-rd lecture

Consider the case $R = \mathbb{C}$, the complex numbers, and the set of eight matrices

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

One verifies that this is a subgroup of $\mathrm{GL}_2(\mathbb{C})$, called the *Quaternion group*. One can use the notation

$$\pm 1, \pm i, \pm j, \pm k$$

for the matrices, respectively. Then we have

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = i,\ ki = j.$$

2.5. **Groups of small order.** One can show that in a suitable sense (up to isomorphism, see § 8.1) the following is a complete list of groups for the given orders. (In the middle column we give the abelian groups and in the right column the non-abelian groups.)

order	abelian groups	non-abelian groups
1	$\{1\}$	
2	$\mathbb{Z}/2\mathbb{Z}$	
3	$\mathbb{Z}/3\mathbb{Z}$	
4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$	
5	$\mathbb{Z}/5\mathbb{Z}$	
6	$\mathbb{Z}/6\mathbb{Z}$	S_3
7	$\mathbb{Z}/7\mathbb{Z}$	
8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$	D_8, Q
9	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$	
10	$\mathbb{Z}/10\mathbb{Z}$	D_{10}
11	$\mathbb{Z}/11\mathbb{Z}$	
12	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$	D_{12}, A_4, T

In the following table we list for every n the number $G(n)$ of subgroups of order n (this is taken from J. Rotman/*An introduction to the theory of groups*):

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$G(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1

n	20	21	22	23	24	25	26	27	28	29	30	31	32
$G(n)$	5	2	2	1	15	2	2	5	4	1	4	1	51

2.6. **Direct product.** Let G, H be two groups. Define on the cartesian product $G \times H$ multiplication by Dummit & Foote §1.1

$$m : (G \times H) \times (G \times H) \longrightarrow G \times H, \quad m((a,x),(b,y)) = (ab, xy).$$

This makes $G \times H$ into a group, called the *direct product* (also direct sum) of G and H.

One checks that $G \times H$ is abelian if and only if both G and H are abelian. The following relation among orders hold: $o(a,x) = \mathrm{lcm}(o(a), o(x))$. It follows that if G, H are cyclic groups whose orders are co-prime then $G \times H$ is also a cyclic group.

Example 2.6.1. If $H_1 < H, G_1 < G$ are subgroups then $H_1 \times G_1$ is a subgroup of $H \times G$. However, not every subgroup of $H \times G$ is of this form. For example, the subgroups of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are $\{0\} \times \{0\}, \{0\} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \{0\}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the subgroup $\{(0,0),(1,1)\}$ which is *not* a product of subgroups.

3. Cyclic groups

Let G be a finite cyclic group of order n, $G =< g >$. Dummit & Foote §2.3

Lemma 3.0.2. *We have* $o(g^a) = n/\gcd(a,n)$.

Proof. Note that $g^t = g^{t-n}$ and so $g^t = e$ if and only if $n|t$ (cf. Corollary 1.2.2). Thus, the order of g^a is the minimal r such that ar is divisible by n. Clearly $a \cdot n/\gcd(a,n)$ is divisible by n so the order of g^a is less or equal to $n/\gcd(a,n)$. On the other hand if ar is divisible by n then, because $n = \gcd(a,n) \cdot n/\gcd(a,n)$, r is divisible by $n/\gcd(a,n)$. □

Proposition 3.0.3. *For every $h|n$ the group G has a unique subgroup of order h. This subgroup is cyclic.*

Proof. We first show that every subgroup is cyclic. Let H be a non trivial subgroup. Then there is a minimal $0 < a < n$ such that $g^a \in H$ and hence $H \supseteq < g^a >$. Let $g^r \in H$. We may assume that $r > 0$. Write $r = ka + k'$ for $0 \le k' < a$. Note that $g^{r-ka} \in H$. The choice of a then implies that $k' = 0$. Thus, $H =< g^a >$.

Since $\gcd(a,n) = \alpha a + \beta n$ we have $g^{\gcd(a,n)} = (g^n)^\beta (g^a)^\alpha \in H$. Thus, $g^{a-\gcd(a,n)} \in H$. Therefore, by the choice of a, $a = \gcd(a,n)$; that is, $a|n$. Thus, every subgroup is cyclic and of the form $< g^a >$ for $a|n$. Its order is n/a. We conclude that for every $b|n$ there is a unique subgroup of order b and it is cyclic, generated by $g^{n/b}$. □

Proposition 3.0.4. *Let G be a finite group of order n such that for $h|n$ the group G has at most one subgroup of order h then G is cyclic.* Dummit & Foote P. 316

Proof. We define *Euler's phi function* as

$$\phi(h) = \sharp\{1 \le a \le h : \gcd(a,h) = 1\}.$$

This function has the following properties (that we take as facts):

- If n and m are relatively prime then $\phi(nm) = \phi(n)\phi(m)$.[7]

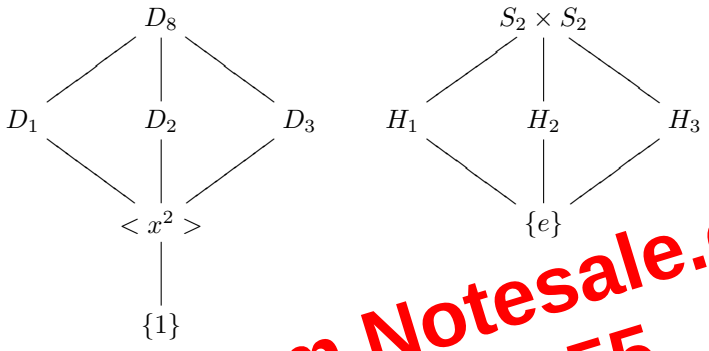
[7] This can be proved as follows. Using the Chinese Remainder Theorem $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings. Now calculate the unit groups of both sides.

Finally, define a function

$$f : G/N \longrightarrow G/K, \qquad f(gN) = gK.$$

First, f is well defined: $f(gnN) = gnK = gK$ for $n \in N$. Next, f is a homomorphism: $f(gNg_1N) = f(gg_1N) = gg_1K = gKg_1K = f(gN)f(g_1N)$. Clearly, f is surjective. The kernel of f are the cosets gN such that $gK = K$, i.e. $g \in K$. That is, the kernel of f is just K/N. We conclude by the First Isomorphism Theorem. □

Example 11.0.8. Consider again the group homomorphism $f : D_8 \longrightarrow S_2 \times S_2$ constructed in Example 9.0.4. Using the third isomorphism theorem we conclude that the graph of the subgroups of D_8 containing $< x^2 >$ is exactly that of $S_2 \times S_2$ (analyzed in Example 2.6.1). Hence we have:



We'll see later that this does not exhaust the list of subgroups of D_8. Here we have
$D_1 =< x >$,
$D_2 =< y, x^2 >$
$D_3 =< xy, x^2 >$
and
$H_1 = f(D_1) = \{(1,1), ((ab), (AB))\}$,
$H_2 = f(D_2) = \{(1,1), (1, (AB))\}$,
$H_3 = f(D_3) = \{(1,1), ((ab), 1)\}$.

end of lecture 9

Example 11.0.9. Let $\mathbb{F}$ be a field and let $N = \{\text{diag}[f, f, \ldots, f] : f \in \mathbb{F}^\times\}$ be the set of diagonal matrices with the same non-zero element in each diagonal entry. We proved in an assignment that $N = Z(\text{GL}_n(\mathbb{F}))$ and is therefore a normal subgroup. The quotient group

$$\text{PGL}_n(\mathbb{F}) := \text{GL}_n(\mathbb{F})/N$$

is called the projective linear group.

Let $\mathbb{P}^{n-1}(\mathbb{F})$ be the set of equivalence classes of non-zero vectors in $\mathbb{F}^n$ under the equivalence $v \sim w$ if there is $f \in \mathbb{F}^*$ such that $fv = w$; that is, the set of lines through the origin. The importance of the group $\text{PGL}_n(\mathbb{F})$ is that it acts as automorphisms on the projective $n-1$-space $\mathbb{P}^{n-1}(\mathbb{F})$.

Let

$$\pi : \text{GL}_n(\mathbb{F}) \longrightarrow \text{PGL}_n(\mathbb{F})$$

be the canonical homomorphism. The function

$$\det : \text{GL}_n(\mathbb{F}) \longrightarrow \mathbb{F}^*$$

Part 3. Group Actions on Sets

13. Basic definitions

Let G be a group and let S be a non-empty set. We say that G *acts on* S if we are given a function Dummit & Foote §4.1

$$G \times S \longrightarrow S, \quad (g, s) \longmapsto g \star s,$$

such that;

(i) $e \star s = s$ for all $s \in S$;

(ii) $(g_1 g_2) \star s = g_1 \star (g_2 \star s)$ for all $g_1, g_2 \in G$ and $s \in S$.

Given an action of G on S we can define the following sets. Let $s \in S$. Define the *orbit* of s

$$\mathrm{Orb}(s) = \{g \star s : g \in G\}.$$

Note that $\mathrm{Orb}(s)$ is a subset of S, equal to all the images of the element s under the action of the elements of the group G. We also define the *stabilizer* of s to be

$$\mathrm{Stab}(s) = \{g \in G : g \star s = s\}.$$

Note that $\mathrm{Stab}(s)$ is a subset of G. In fact, it is a subgroup, as the next Lemma states.

One should think of every element of the group as becoming a symmetry of the set S. We'll make more precise later. For now, we just note that every element $g \in G$ defines a function $S \longrightarrow S$ by $s \mapsto gs$. This function, we'll see later, is bijective.

14. Basic properties

Lemma 14.0.10. (1) *Let $s_1, s_2 \in S$. We say that s_1 is related to s_2, i.e., $s_1 \sim s_2$, if there exists $g \in G$ such that*

$$g \star s_1 = s_2.$$

This is an equivalence relation. The equivalence class of s_1 is its orbit $Orb(s_1)$.

(2) *Let $s \in S$. The set $Stab(s)$ is a subgroup of G.*

(3) *Suppose that both G and S have finitely many elements. Then*

$$|Orb(s)| = \frac{|G|}{|Stab(s)|}.$$

Proof. (1) We need to show reflexive, symmetric and transitive. First, we have $e \star s = s$ and hence $s \sim s$, meaning the relation is reflexive. Second, if $s_1 \sim s_2$ then for a suitable $g \in G$ we

the stabilizer is a subgroup. Apply that for $r = 3, 5, 7$ to see that if x^r fixes a coloring so does x , which is impossible. [11]

Now, x^2 written as a permutation is $(1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. We see that if, say 1 is green so are $3, 5, 7$ and the rest must be red. That is, all the freedom we have is to choose whether the cycle $(1\ 3\ 5\ 7)$ is green or red. This gives us two colorings fixed by x^2. The same rational applies to $x^6 = (8\ 6\ 4\ \ 2)(7\ 5\ 3\ 1)$.

Consider now x^4. It may written in permutation notation as $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$. In any coloring fixed by x^4 each of the cycles $(1\ 5)(2\ 6)(3\ 7)$ and $(4\ 8)$ must be single colored. There are thus $\binom{4}{2} = 6$ possibilities (Choosing which 2 out of the four cycles would be green).

It remains to deal with the elements yx^i. We recall that these are all reflections. There are two kinds of reflections. One may be written using permutation notation as

$$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6)$$

(with the other two vertices being fixed. For example $y = (2\ 8)(3\ 7)(4\ 6)$ is of this form). The other kind is of the form

$$(i_1\ i_2)(i_3\ i_4)(i_5\ i_6)(i_7\ i_8).$$

(For example $yx = (1\ 8)(2\ 7)(3\ 6)(4\ 5)$ is of this sort). Whatever is the case, one uses similar reasoning to deduce that there are 6 colorings preserved by a reflection.

One needs only apply **CFF** to get that there are

$$N = \frac{1}{16}(70 + 2 \cdot 2 + 6 + 8 \cdot 6) = 8$$

distinct necklaces.

17.3. **The game of 16 squares.** Sam Loyd (1841-1911) was America's greatest puzzle expert and invented thousands of ingenious and tremendously popular puzzles.

In this game, we are given a 4×4 box with 15 squares numbered $1, 2, \ldots, 15$ and one free spot. At every step one is allowed to move an adjacent square into the vacant spot. For example

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

$\mapsto$

1	2	3	4
5	6	7	8
9	10	11	12
13	14		15

$\mapsto$

1	2	3	4
5	6	7	8
9	10		12
13	14	11	15

$\mapsto$

1	2	3	4
5	6	7	8
9		10	12
13	14	11	15

$\mapsto$

1	2	3	4
5	6	7	8
9	14	10	12
13		11	15

Can one pass from the original position to the position below?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

It turns out that the answer is no. Can you prove it? Apparently, the puzzle was originally marketed with the tiles in the impossible position with the challenge to rearrange them into the initial position!

[11] $x^{(3^2)} = x^9 = x$ because $x^8 = e$, etc.

It still remains to consider the case where each σ_i is a transposition. Then, if $\sigma = (i_1 i_2)(i_3 i_4)$ then σ moves only 4 elements and thus fixes some element and we are done, else $\sigma = (i_1 i_2)(i_3 i_4)(i_5 i_6)\dots$. Let $\tau = (i_1 i_2)(i_3 i_5)$ then $\tau\sigma\tau^{-1}\sigma = (i_2 i_1)(i_5 i_4)(i_3 i_6)\dots(i_1 i_2)(i_3 i_4)(i_5 i_6)\cdots = (i_3 i_5)(i_4 i_6)\dots$ and so is a permutation of the sort we were seeking.

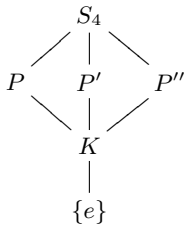
Second step: $N = A_n$.

Consider the subgroups $G_i = \{\sigma \in A_n : \sigma(i) = i\}$. We note that each G_i is isomorphic to A_{n-1} and hence is simple. By the preceding step, for some i we have that $N \cap G_i$ is a non-trivial normal subgroup of G_i, hence equal to G_i.

Next, note that $(12)(34)G_1(12)(34) = G_2$ and, similarly, all the groups G_i are conjugate in A_n to each other. It follows that $N \supseteq < G_1, G_2, \dots, G_n >$. Now, every element in S_n is a product of (usually not disjoint) transpositions and so every element σ in A_n is a product of an even number of transpositions, $\sigma = \lambda_1\mu_1\dots\lambda_r\mu_r$ (λ_i, μ_i transpositions). Since $n > 4$ every product $\lambda_i\mu_i$ belongs to some G_j and we conclude that $< G_1, G_2, \dots, G_n >= A_n$.

□

Call this subgroup K. Then, we see that $|K| = 4$; it is preserved under conjugation hence is a subgroup of all three 2-Sylow subgroups, say P, P', P''. We have the following picture



23.1.5. *Groups of order pq.* Let $p < q$ be primes. Let G be a group of order pq. Then $n_q | p$, $n_q \equiv 1 \pmod q$. Since $p < q$ we have $n_q = 1$ and the q-Sylow subgroup is normal (in particular, G is never simple). Also, $n_p | q$, $n_p \equiv 1 \pmod p$. Thus, either $n_p = 1$, or $n_p = q$ and the last possibility can happen only for $q \equiv 1 \pmod p$.

We conclude that if $p \not| (q-1)$ then both the p-Sylow P subgroup and the q-Sylow subgroup Q are normal. Note that the order of $P \cap Q$ divides both p and q and so is equal to 1. Let $x \in P, y \in Q$ then $[x, y] = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1}) \in P \cap Q = \{1\}$. Thus, PQ, which is equal to G, is abelian.

We shall later see that whenever $p|(q-1)$ there is a non-abelian group of order pq (in fact, unique up to isomorphism). The case of S_3 falls under this.

23.1.6. *Groups of order p^2q.* Let G be a group of order p^2q, where p and q are distinct primes. We prove that G is not simple:

If $q < p$ then $n_p \equiv 1 \pmod p$ and $n_p | q < p$, which implies that $n_p = 1$ and the p-Sylow subgroup is normal.

Suppose that $p < q$, then $n_q \equiv 1 \pmod q$ and $n_q | p^2$, which implies that $n_q = 1$ or p^2. If $n_q = 1$ then the q-Sylow subgroup is normal. Assume that $n_q = p^2$. Each pair of the p^2 q-Sylow subgroups intersect only at the identity (since q is prime). Hence they account for $1 + p^2(q-1)$ elements. Suppose that there were 2 p-Sylow subgroups. They intersect at most at a subgroup of order p. Thus, they contribute at least $2p^2 - p$ new elements. All together we got at least $1 + p^2(q-1) + 2p^2 - p = p^2q + p^2 - p + 1 > p^2q$ elements. That's a contradiction and so $n_p = 1$; the p-Sylow subgroup is normal.

Remark 23.1.2. A theorem of Burnside states that a group of order $p^a q^b$ with $a + b > 1$ is not simple. You will prove in the assignments that groups of order pqr ($p < q < r$ primes) are not simple. Note that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$ and A_5 is simple. A theorem of Feit and Tompson says that a finite simple group is either of prime order, or of even order.

23.1.7. $\mathrm{GL}_n(\mathbb{F})$. Let $\mathbb{F}$ be a finite field with q elements. The order of $\mathrm{GL}_n(\mathbb{F})$ is $(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{(n-1)n/2}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$. Thus, a p-Sylow has order $q^{(n-1)n/2}$. One such subgroup consists of the upper triangular matrices with 1 on the diagonal (the unipotent group):

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \cdots & * \\ & & \ddots & \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Part 6. Finitely Generated Abelian Groups, Semi-direct Products and Groups of Low Order

24. The structure theorem for finitely generated abelian groups

The structure theorem will proved in the next semester as a corollary of the structure theorem for modules over a principal ideal domain. That same theorem will also yield the Jordan canonical form of a matrix.

Theorem 24.0.3. *Let G be a finitely generated abelian group. Then there exists a unique non-negative integer r and integers $1 < n_1|n_2|\dots|n_t$ $(t \geq 0)$ such that*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}.$$

Remark 24.0.4. The integer r is called the *rank* of G. The subgroup in G that corresponds to $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$ under such an isomorphism is canonical (independent of the isomorphism). It is the subgroup of G of elements of finite order, also called the *torsion subgroup* of G and sometime denoted G_{tor}.

On the other hand, the subgroup corresponding to $\mathbb{Z}^r$ is not canonical and depends very much on the isomorphism.

A group is called *free abelian group* if it is isomorphic to $\mathbb{Z}^r$ for some r (the case $t = 0$ in the theorem above). In this case, elements $x_1, \dots, x_r$ of G that correspond to a basis of $\mathbb{Z}^r$ are called a basis of G; every element of G has the form $a_1x_1 + \cdots + a_rx_r$ for unique integers $a_1, \dots, a_r$.

Remark 24.0.5. The Chinese remainder theorem gives that if $n = p_1^{a_1} \cdots p_s^{a_s}$, p_i distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}.$$

Thus, one could also write an isomorphism $G \cong \mathbb{Z}^r \times \prod_i \mathbb{Z}/p_i^{b_i}\mathbb{Z}$.

We shall also prove the following corollary in greater generality next semester.

Corollary 24.0.6. *Let G, H be two free abelian groups of rank r. Let $f : G \longrightarrow H$ be a homomorphism such that $G/f(H)$ is a finite group. There are bases $x_1, \dots, x_r$ of G and $y_1, \dots, y_r$ of H and integers $1 \leq n_1|\dots|n_r$ such that $f(y_i) = n_ix_i$.*

Example 24.0.7. Let G be a finite abelian p group, $|G| = p^n$. Then $G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{a_s}\mathbb{Z}$ for unique a_i satisfying $1 \leq a_1 \leq \cdots \leq a_s$ and $a_1 + \cdots + a_s = n$. It follows that the number of isomorphism groups of finite abelian groups of order p^n is $p(n)$ (the partition function of n).

25. Semi-direct products

Given two groups B, N we have formed their direct product $G = N \times B$. Identifying B, N with their images $\{1\} \times B, N \times \{1\}$ in G, we find that: (i) $G = NB$, (ii) $N \lhd G, B \lhd G$, (iii) $N \cap B = \{1\}$. Conversely, one can easily prove that if G is a group with subgroups B, N such that: (i) $G = NB$, (ii) $N \lhd G, B \lhd G$, (iii) $N \cap B = \{1\}$, then $G \cong N \times B$. The definition of a semi-direct product relaxes the conditions a little.