Review IV(Slides 226 - 274)

Basic Number Theory& Group Theory

HamHam

University of Michigan-Shanghai Jiao Tong University Joint Institute

January 14, 2022

VE203 - Discrete Mathmatics

Divisibility

Definition

Let $n, d \in \mathbb{Z}$, we say that d divides n if $n = dk$ for some $k \in \mathbb{Z}$. That is

$$d \mid n \Leftrightarrow \exists k \in \mathbb{Z}\ (n = dk)$$

We can see that $\mid$ is a **pre-order** on $\mathbb{Z}$ but $(\mathbb{N}, \mid)$ is a **poset**. (Why?) For simplicity we will discuss divisibility on natural numbers more in number theory. Zero?

Properties:

- $a \mid a$
- $a \mid b \wedge b \mid c \Rightarrow a \mid c$
- $a \mid b \wedge b \mid a \Rightarrow a = \pm b$

Prime Numbers

Definition

A natural number $p \in \mathbb{N}$ is a **prime number** if $p \geq 2$ and is divisible by 1 and itself only. The set of primes is denoted by $\mathbb{P}$.

Unique Factorization

Every positive integer $n \geq 2$ can be **uniquely** expressed in the form

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \ p_i \in \mathbb{P}, \ \alpha_i \in \mathbb{Z}^+$$

Typical Example

Better to memoerize if you can:

- Fermat Primes
- Mersenne Primes

Infinitude of Prime

Theorem

There are *infinitely* many primes.

- Proof of Euclid.
- Proof by contraposition

Theorem (Dirichlet)

There are *infinitely* many primes of the form $an + b$ where a, b are coprime. Speical cases include:

- $2n + 1$
- $3n + 2$ (Consider the product of all primes of such form)
- $4n + 1$ (Slides 235)
- $4n - 1$ (How to construct the product?)

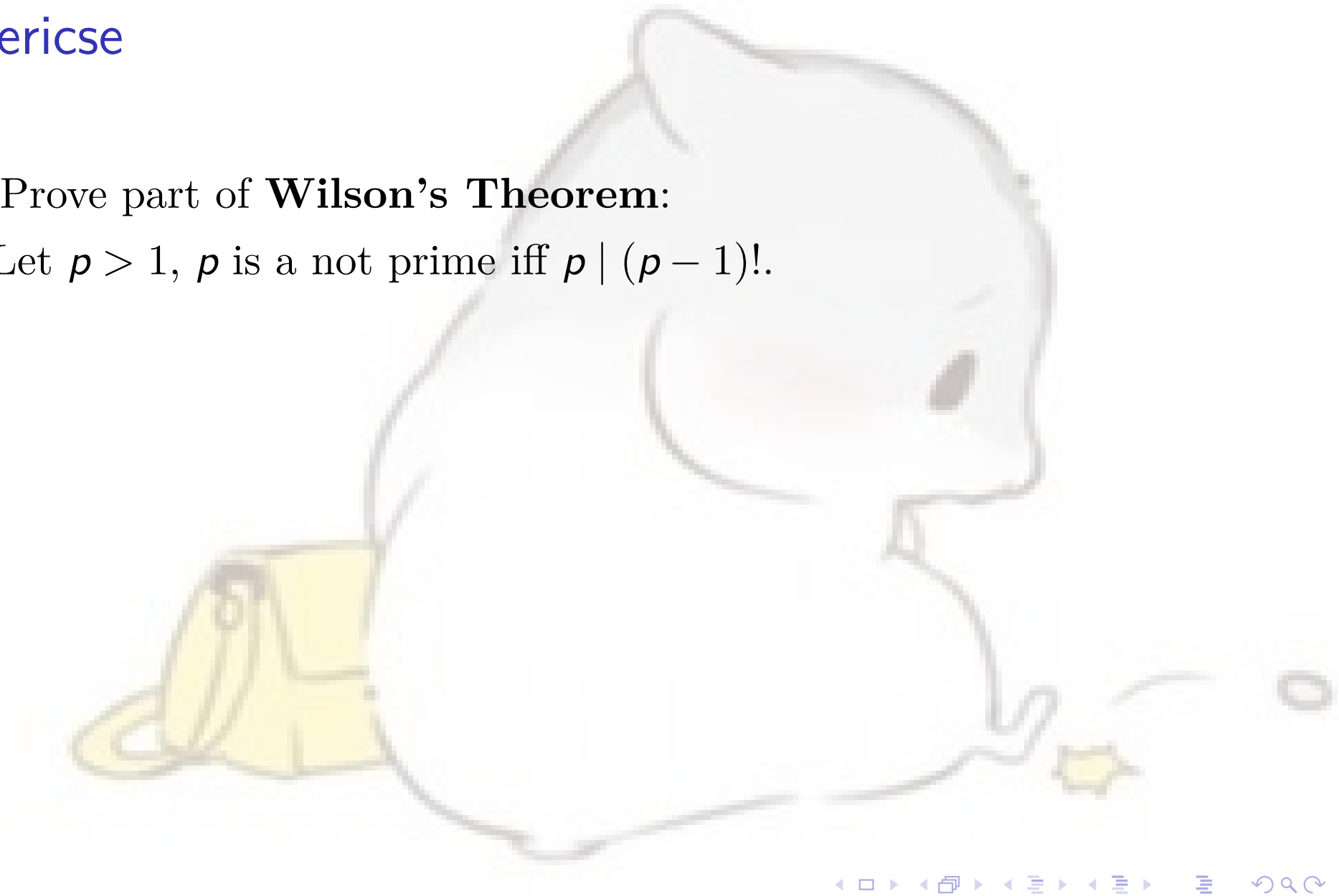
Distance Grows

For any large n, there exists successive n numbers that are not prime.

Exericse

1. Prove part of **Wilson's Theorem**:

   Let $p > 1$, p is a not prime iff $p \mid (p-1)!$.



Exericse

1. Prove part of **Wilson's Theorem**:

   Let $p > 1$, p is a not prime iff $p \mid (p-1)!$.

Solution:

- If p is a prime, then p is not divisible by any number from 1 to $p-1$, so $p \nmid (p-1)!$.
- If p is not prime and is a square, $p = k^2, k > 2$. Since $k < p-1$, $2k < p-1$, we conclude that $k \cdot (2k) \mid (p-1)!$.
- Otherwise, there exists two factors $a, b, a \neq b$, so that $p = ab$. Since $a < p-1$, $b < p-1$, we have $p = ab \mid (p-1)!$.

Division Algorithm

Theorem ((Long) Division Algorithm)

Given $m, n \in \mathbb{N}\backslash\{0\}$, there **exist** *unique* integers q and r with $q \geq 0$ and $0 \leq r < m$ so that $n = qm + r$.

The proof may sounds simple, but it is meaningful!

Uniqueness:

$$m \mid (r_1 - r_2) \wedge |r_1 - r_2| < m \Rightarrow F$$

Existence:

$$k = qm + r \Rightarrow k + 1 = \begin{cases} qm + (r+1), \text{ if } r + 1 < m \\ q(m+1) + 0, \text{ if } r + 1 = m \end{cases}$$

Also pay attention to the case that $1 = 1 \cdot 1 + 0$ or $1 = 0 \cdot m + 1$

Greatest Common Divisor

Definition

Let $a, b \in \mathbb{Z}\backslash\{0\}$, The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the greatest positive integer d such that $d \mid a \wedge d \mid b$.

Notice that

$$(N, |, \wedge := \gcd, \vee := (a, b) \mapsto \frac{ab}{\gcd(a, b)})$$

is a **lattice** where $\top = 0$ and $\bot = 1$.

Least Common Multiple

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

Euclidean Algorithm

A recursive algorithm to calculate the greatest common divisor between two integers:

$$\gcd(a,b) = \begin{cases} \gcd(b, r(a,b)) & b \neq 0 \\ a & b = 0 \end{cases}$$

*Interesting names: 辗转相除法、更相减损术

Theorem (Bezout)

The equation $ax + by = c$ of x and y where $a, b, c \in \mathbb{Z}$ has integer solutions iff $\gcd(a,b) \mid c$.

Exercise

2. Let F_n be Fermat Primes, i.e. $F_n = 2^{2^n} + 1$. Prove that they are pairwise coprime, namely $\gcd(F_n, F_m) = 1$.

3. Use the **Euclidean Algorithm** to find a integer pair (x, y) that $111x - 321y = 75$.

Groups

A **group** is a pair $(G, \cdot)$, where G is a set, and $\cdot : G \times G \to G$ is a law of composition that has the following properties:

- Closure: The generalized product is defined as $\cdot : G \times G \to G$
- Associativety: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;
- Identity: G contains an identity element 1, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in G$;
- Inverse: Every element $a \in G$ has an inverse, an element b such that $a \cdot b = b \cdot a = 1$.

An **abelian group** is a group whose law of composition is commutative ($a \cdot b = b \cdot a$).

Properties

Given a group G, $a, b, c \in G$, then

- there exists a **unique** identity element;
  $\rightarrow$ suppose there are two distinct identity i and j, then $i \cdot j = i = j$
- $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$;
  $\rightarrow$ multiply by a^{-1} on both sides, note that a group does not necessarily satisfy the commutative law
- For all $a \in G$, there exists a unique element $b \in G$ such that $ab = ba = 1$;
  $\rightarrow$ prove existence ($b = a^{-1}$) first, then prove uniqueness by contradiction
- $(ab)^{-1} = b^{-1}a^{-1}$.
  $\rightarrow (ab)^{-1}(ab) = 1$; $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = 1$

Subgroup

A subset H of a group G is a subgroup if it has the following properties:

- Closure: If $a, b \in H$, then $ab \in H$;
- Identity: $1 \in H$;
- Inverses: If $a \in H$, then $a^{-1} \in H$.

Look carefully at the identity and inverse axioms for a subgroup:

- In verifying the identity axiom for a subgroup, the issue is not the existence of an identity but **whether the identity for the group is actually contained in the subgroup**.
- Likewise, for subgroups the issue of inverses is not whether inverses exist (every element of a group has an inverse) but **whether the inverse of an element in the subgroup is actually contained in the subgroup**.

Exercise

4. Given a group G and its two distinct subgroups H_1 and H_2. Check whether the following sentences are true or false:

- The identity element in G and H_1 must be the same.
- $H_1 \cup H_2$ is a group.
- $H_1 \cap H_2$ cannot be empty and it is a group.
- A subset in G that is not a subgroup may be a group.

Comment. Compare to the concept of **vector space**. If necessary, take Vv186.

Exercise

5. $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ denotes the set of pairs of integers:

$$\mathbb{Z}^2 = \{(m, n) \mid m, n \in \mathbb{Z}\}.$$

It is a group under "vector addition", that is,

$$(a, b) + (c, d) = (a + c, b + d).$$

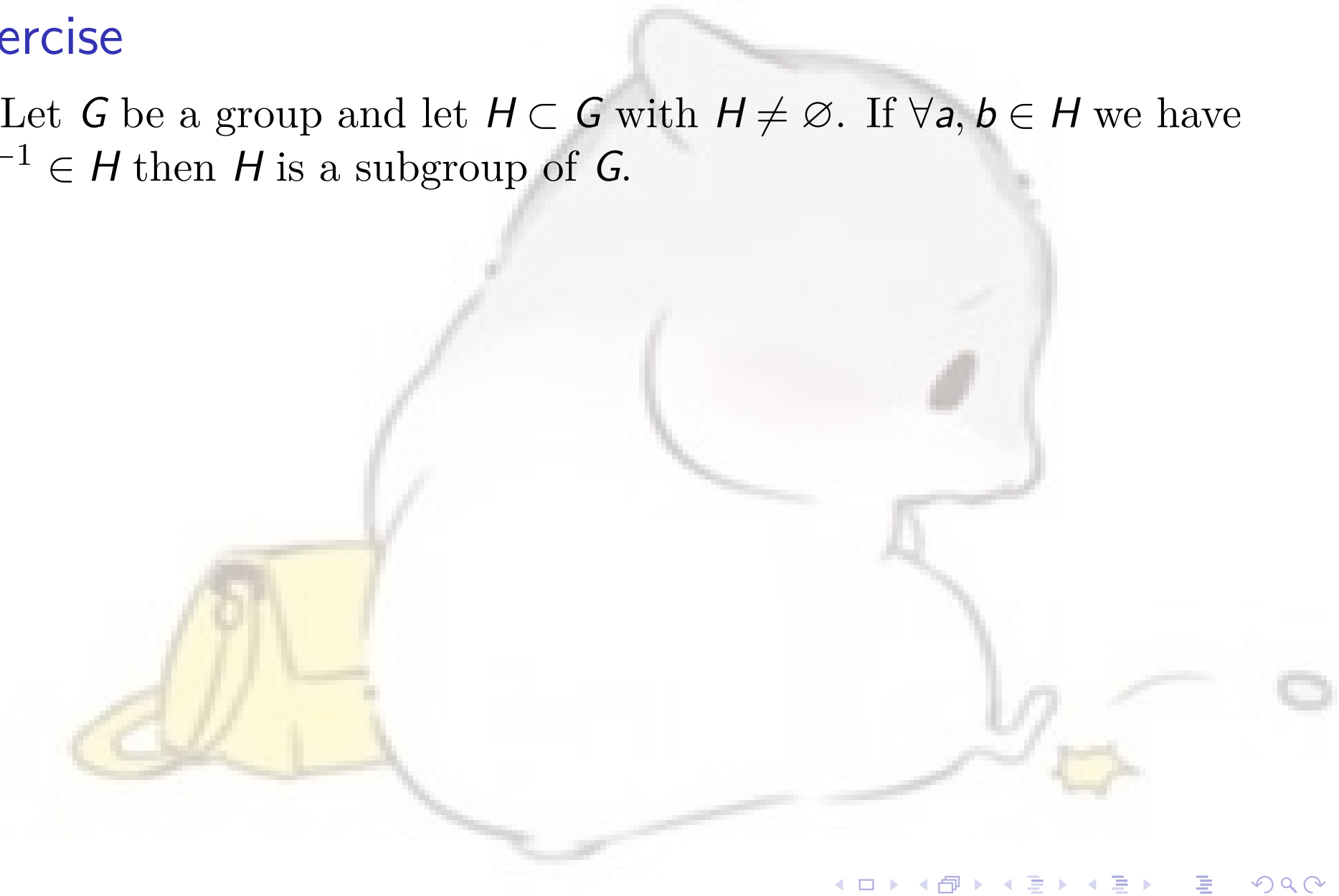
Consider the set

$$H = \{(x, y) \mid x + y \geqslant 0\}.$$

Check if H is a subgroup of $\mathbb{Z}^2$.

Exercise

6. Let G be a group and let $H \subset G$ with $H \neq \varnothing$. If $\forall a, b \in H$ we have $ab^{-1} \in H$ then H is a subgroup of G.



Exercise

6. Let G be a group and let $H \subset G$ with $H \neq \varnothing$. If $\forall a, b \in H$ we have $ab^{-1} \in H$ then H is a subgroup of G.

Solution:

Since $H \subset G$, any operation in H has associativity. Then, we need to verify closure, identity, and inverses requirements but we need to do these in a particular order.

1. Since $H \neq \varnothing$, pick any $a \in H$. Then $aa^{-1} = e \in H$, so H has the identity.
2. Pick any $a \in H$. Since the identity $e \in H$, then $ea^{-1} = a^{-1} \in H$ so we have inverses.
3. Pick any $a, b \in H$. Then $b^{-1} \in H$ and denote as $c \in H$. So, $ac^{-1} \in H$ according to the problem statement. So, $ab = a(b^{-1})^{-1} = ac^{-1} \in H$ and we have closure.

Exercise

7.* Let G be a group. If $\forall x \in G : x^2 = e$, show that G is an abelian group.

Solution:

From $\forall x \in G : x^2 = e$, we obtain $x = x^{-1}$.
Therefore, taking $\forall x, y \in G$, we have

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

This completes the proof.

Cyclic Group

The cyclic subgroup generated by g is

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

In other words, $\langle g \rangle$ consists of all (positive or negative) powers of g.

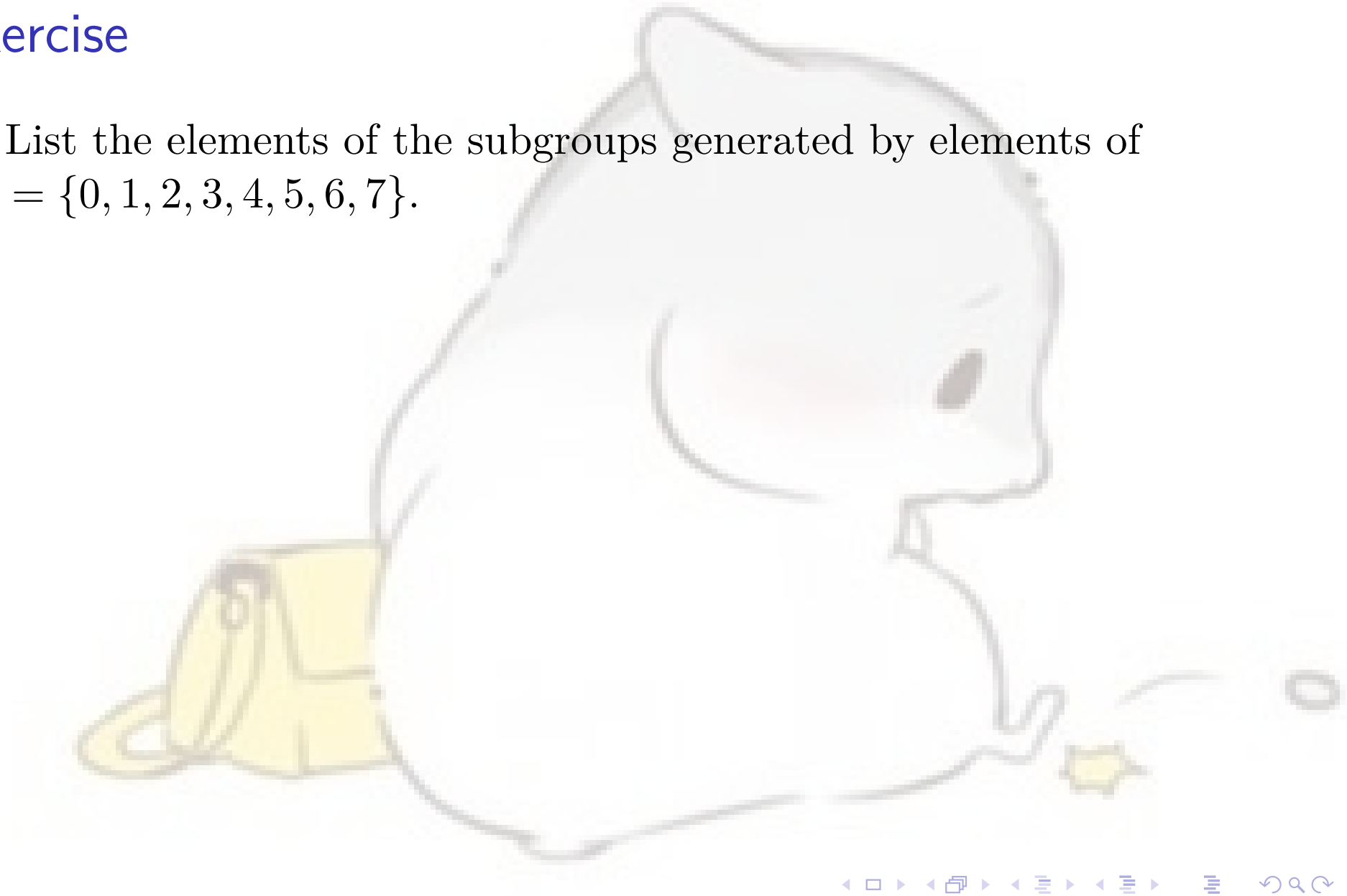
$$\langle g \rangle = \{k \cdot g \mid k \in \mathbb{Z}\}.$$

Be sure you understand that the difference between the two forms is simply notational: It' s the same concept.

Let G be a group, $g \in G$. The order of g is the smallest positive integer n such that $g^n = 1$ $(ng = 0)$. If there is no positive integer n such that $g^n = 1$ $(ng = 0)$, then g has **infinite** order.

Exercise

8. List the elements of the subgroups generated by elements of $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.



Exercise

8. List the elements of the subgroups generated by elements of $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Solution:

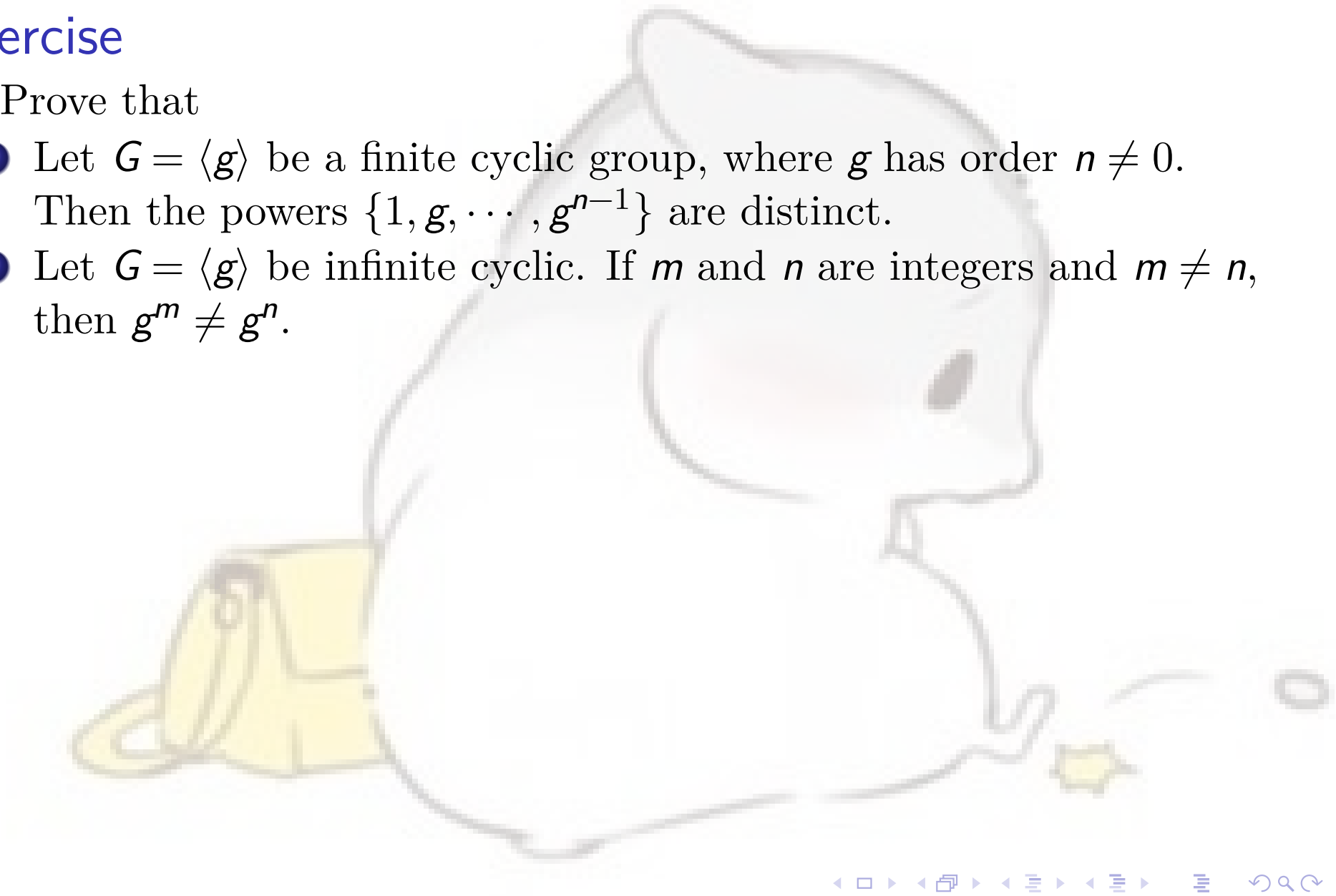
$$\langle 0 \rangle = \{0\}$$
$$\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\}$$
$$\langle 4 \rangle = \{0, 4\}$$
$$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7\} = \mathbb{Z}_8$$

Question

What is the identity? Order?

Exercise

9. Prove that
   1. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order $n \neq 0$. Then the powers $\{1, g, \cdots, g^{n-1}\}$ are distinct.
   2. Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.



Exercise

9. Prove that

1. Let $G = \langle g \rangle$ be a finite cyclic group, where g has order $n \neq 0$. Then the powers $\{1, g, \cdots, g^{n-1}\}$ are distinct.
2. Let $G = \langle g \rangle$ be infinite cyclic. If m and n are integers and $m \neq n$, then $g^m \neq g^n$.

Solution:

1. Since g has order n, $g, g^2, \cdots, g^{n-1}$ are all different from 1. Suppose $g^i = g^j$ where $0 \leqslant j < i < n$. Then $0 < i-j < n$ and $g^{i-j} = 1$, contrary to the preceding observation.
   Therefore, the powers $\{1, g, \cdots, g^{n-1}\}$ are distinct.
2. Suppose without loss of generality that $m > n$. We want to show that $g^m \neq g^n$.
   Suppose this is false, so $g^m = g^n$. Then $g^{m-n} = 1$, so g has finite order $m - n$. This contradicts the fact that a generator of an infinite cyclic group has infinite order. Therefore, $g^m \neq g^n$.

Divide & Conquer

This is just standby. If we really have time.

Recall Manuel's h5 ex6:

1. Detail Karatsuba algorithm in the README file (search it on internet).
2. Add comments to the code to describe what is done, line by line.
3. Explain in the README file what specific adjustments were made to the algorithm in order to improve the efficiency.
4. Search online what is a divide an conquer strategy.
5. Using a divide and conquer approach, together with the operators &, |, « and » , write an efficient function to replace the for loops marked as "not optimal".

Link: `https://www.bilibili.com/video/BV1jS4y197PV`

Probelm

```
1   unsigned long int mult(unsigned long int a, unsigned long int b) {
2       int i, n, N;
3       unsigned long int x0,y0,z0,z1=1;
4       if(a<b) SWAP(a,b);
5       if(b==0) return 0;
6       for(n=-1, i = 1; i <= b; i<<=1, n++); /* not optimal */
7       for(N=n; i <= a; i<<=1, N++);
8
9       y0=b&((1<<n)-1);
10      x0=a&((1<<N)-1);
11      z0=mult(x0,y0);
12      i=N+n;
13      return ((z1<<i)+(x0<<n)+(y0<<N)+z0);
14  }
```

Reference

- Problem from Vg101 Manuel Homework 5.
- Examples from Dr. Cai Runze's Sildes.
- Exercises from 2021-Fall-Ve203 TA Zhao Jiayuan
- Contents from 2021-Fall-Ve203 Mid_2 RC by Xue Runze