- 书面作业讲解
  - TJ第3章练习3、6、7、17、28、36、38、41、48、52
  - TJ第4章练习1、12、21、24、32
  - TJ第5章练习3、5、16、27、29
  - TJ第6章练习11、12、16、21
  - [推迟] TJ第9章练习6、7、8、9

TJ第3章练习7

- 阿贝尔群应满足几个条件？
  - 运算封闭
  - 结合律、单位元、逆元
    - 证明单位元和逆元时，左、右运算都要证明
    - 还要证明单位元和逆元也在集合中
  - 交换律

TJ第3章练习36

- 证明子群的几种方法
  - 子集 & 群
  - 命题3.9
  - 命题3.10

TJ第4章练习1(e)

- G中不可能存在阶为无穷的元素a，否则a的每个正次幂都不相等，则存在$<a^1>$、$<a^2>$……无穷多个子群，矛盾。
- 因此，G中每个元素都是有穷阶，而如果G有无穷多个元素，那么必然存在<a>、<b>……无穷多个子群（因为每个都只包含有穷多个元素），矛盾。

TJ第4章练习12

- How about n generators?
  - Z_{2n}行不行？
  - 利用推论4.7

TJ第4章练习24

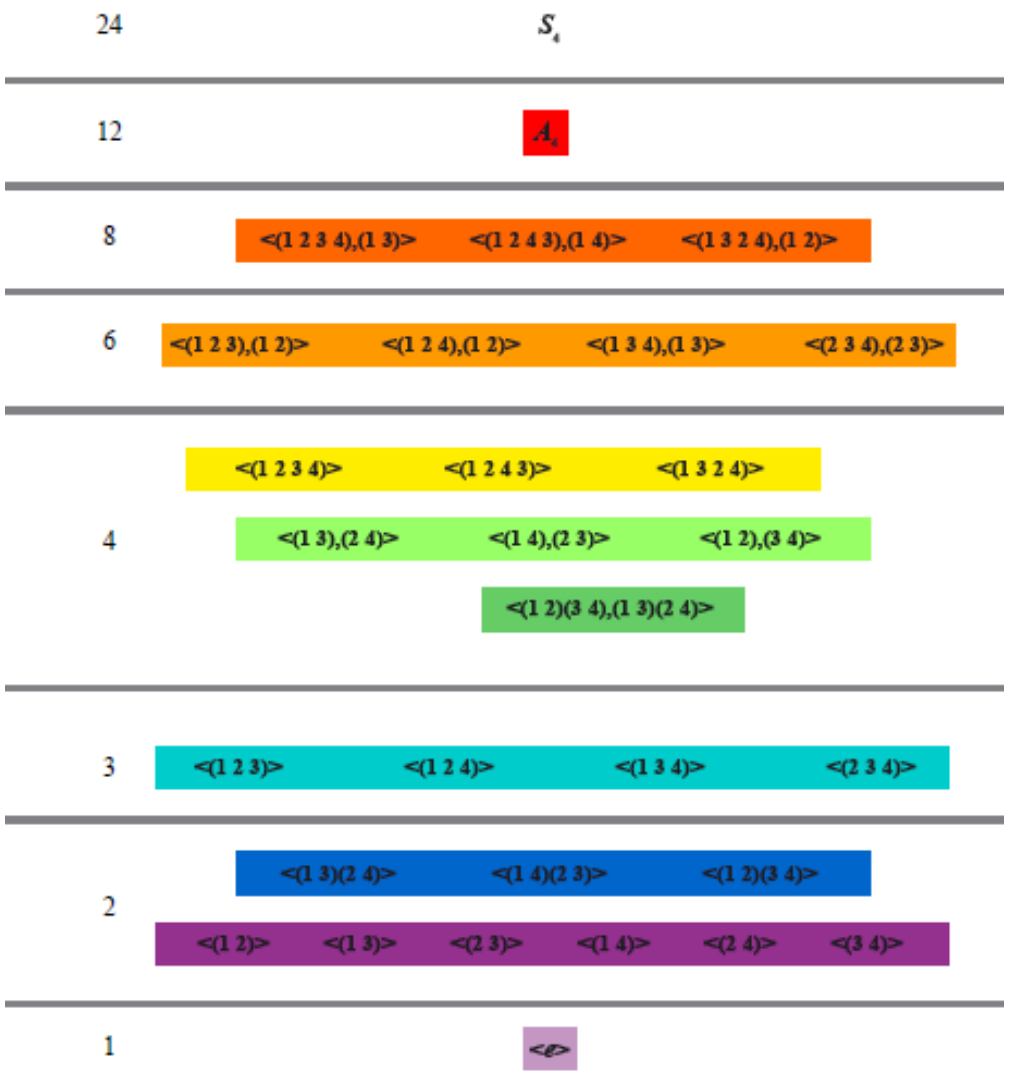
- pq以内与pq互质的数：(p-1)+(q-1)
- 0也不能作为generator

- generator数量：pq-(p-1)-(q-1)-1=pq-p-q+1

TJ第4章练习32

- 由定理4.6：y的阶是n/1=n
- 而阶为n的元素一定是generator

TJ第5章练习5


24
S_4
12
A_4
8
<(1 2 3 4),(1 3)>
<(1 2 4 3),(1 4)>
<(1 3 2 4),(1 2)>
6
<(1 2 3),(1 2)>
<(1 2 4),(1 2)>
<(1 3 4),(1 3)>
<(2 3 4),(2 3)>
4
<(1 2 3 4)>
<(1 2 4 3)>
<(1 3 2 4)>
<(1 3),(2 4)>
<(1 4),(2 3)>
<(1 2),(3 4)>
<(1 2)(3 4),(1 3)(2 4)>
3
<(1 2 3)>
<(1 2 4)>
<(1 3 4)>
<(2 3 4)>
2
<(1 3)(2 4)>
<(1 4)(2 3)>
<(1 2)(3 4)>
<(1 2)>
<(1 3)>
<(2 3)>
<(1 4)>
<(2 4)>
<(3 4)>
1
<e>

TJ第6章练习16

- g的order为2：gg=e，即g是自己的逆元
- 除了order为2的元素以外，只有e是自己的逆元
- 剩余元素都不是自己的逆元：成对出现
- 而|G|=2n，所以order为2的元素必为奇数个

- 任取一个order为2的元素，与e构成order为2的子群

TJ第6章练习21

- 如果直接用Sylow第一定理，这题就失去意义了

- 任取元素a（非单位元），由推论6.6：a的order为p^k $(1\le k\le n)$
- 取b = a的p^{k-1}次幂：$b^p=e$，因此b的order为p（不可能再小了，因为必须是p的幂）
- 由b可以生成一个p阶循环子群

- 教材讨论
  - TJ第2章
  - CS第2章第2节

问题1：mathematical induction, well ordering

- 什么是良序原理？

- 你有哪些办法来证明“对于任意自然数n，某个命题都成立”？
  - 数学归纳法
  - 良序原理
    - 用反证法：不成立的那些自然数的集合没有最小元

  - 例如，你能证明莱曼引理吗：$8a^4+4b^4+2c^4=d^4$没有正整数解
    - 假设所有解中，(a,b,c,d)使abcd最小
    - 发现d是偶数，将$d=2d'$代入：$4a^4+2b^4+c^4=8d'^4$
    - 发现c是偶数，将$c=2c'$代入：$2a^4+b^4+8c'^4=4d'^4$
    - 发现b是偶数，将$b=2b'$代入：$a^4+8b'^4+4c'^4=2d'^4$
    - 发现a是偶数，将$a=2a'$代入：$8a'^4+4b'^4+2c'^4=d'^4$
    - 找到了新的解(a',b',c',d')且$a'b'c'd'<abcd$，矛盾

问题2： inverse, GCD, prime

- Given an element b in Z_n, what can you say in general about the possible number of elements a such that $a \cdot_n b = 1$ in Z_n?

  – 如果gcd(b,n)>1：找不到a
  – 如果gcd(b,n)=1：有且只有一个a

Lemma 2.8 *The equation*

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1.$$

Lemma 2.11 *Given a and n, if there exist integers x and y such that $ax + ny = 1$ then* $\gcd(a, n) = 1$.

问题2： inverse, GCD, prime (续)

- Either find an equation of the form $a \cdot_n x = b$ in Z_n that has a unique solution even though a and n are not relatively prime, or prove that no such equation exists. In other words, you are either to prove the statement that if $a \cdot_n x = b$ has a unique solution in Z_n, then a and n are relatively prime or to find a counter example.

- 如果gcd(a,n)=g>1
  - 如果g|b
    - $a \cdot_n x = b$有g个解α、α+n/g、α+2n/g……
    - 其中，α是$(a/g) \cdot_{n/g} x = (b/g)$的唯一解
    - （因为$(a/g) \cdot_{n/g} x = (b/g)$的每个解都是原方程的解）
  - 否则
    - 很容易验证无解

问题3： Euclid’s GCD algorithm

- 这个算法利用的基本原理是什么

Lemma 2.13 *If j, k, q, and r are positive integers such that $k = jq + r$ then*

$$\gcd(j, k) = \gcd(r, j)$$

- 递归的base case是什么？
- 计算GCD(210,126)