- 书面作业讲解
  - TC第30.1节练习2、4、5
  - TC第30.2节练习1、4、5、7
  - TC第30.3节练习2
  - TC第30章问题1

TC第30.2节练习7

- 多项式可以表示为：
  - $P(x) = \prod_{i=0}^{n-1}(x - z_i)$
  - 利用分治法将问题分为两个问题的乘积：
    - $P(x) = (\prod_{i=0}^{n\backslash 2-1}(x - z_i))\,(\prod_{n/2}^{n-1}(x - z_i))$

$$A(x) \times B(x) \xrightarrow{\text{FFT}} O(n\log n)$$

$$T(n) = 2T(n) + O(nlgn)$$

$$So\ T(n) \in O(nlog^2n)$$

TC第30.3节练习2

- 如果利用DFT的逆来计算FFT(a)，就可以将BIT-REVERSE-COPY放在最后。
  - 将ω_n 修改为$\omega_n{}^{-1}$
  - 令每个y_i = y_i /n
  - 将BIT-REVERSE-COPY放在最后

TC第30章问题1

- a).
  $(ax+b)(cx+d)=$
  $ac\,x^2+\big((a+b)(c+d)\ -ac-bd\big)x+bd$
  - 三次乘法
- b). 当n>2时，将p(x)、q(x)分别划分为两个多项式：
  - $p(x)=p_0(x)+p_1(x)x^{n/2}$
  - $q(x)=q_0(x)+q_1(x)x^{n/2}$

TC第30章问题1

求解、组合改进：

$$p(x)q(x) = p_0(x)q_0(x) + [p_1(x)q_0(x) + p_0(x)q_1(x)]x^{n/2} + p_1(x)q_1(x)x^n$$

$$(p_0(x)+p_1(x))(q_0(x)+q_1(x)) = p_0(x)q_0(x)+p_1(x)q_0(x)+p_0(x)q_1(x)+p_1(x)q_1(x)$$

记：$r_0(x) = p_0(x)q_0(x) \quad r_1(x) = p_1(x)q_1(x)$

$r_2(x) = (p_0(x)+p_1(x))(q_0(x)+q_1(x))$

TC第30章问题1

$$p(x)q(x) = r_0(x) + (r_2(x) - r_0(x) - r_1(x))x^{n/2} + r_1(x)x^n$$

改进后的分治算法乘积次数为三次。

改进分治算法时间复杂度：

$$\begin{cases} T(2) = O(1) & n = 2 \\ T(n) = 3T(n/2) + O(n) & n > 2 \end{cases}$$

用递推法解，有T(n)=O($n^{\log 3}$)。

根据系数下标奇偶性 分解分析与
上述方法类似。

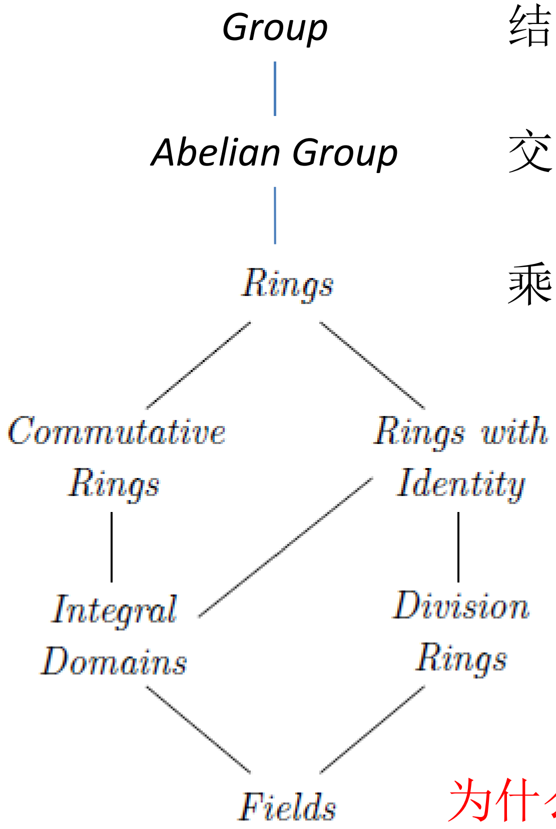
TC第30章问题1

- c). Treat a n – bit integer $b_n, b_{n-1}, \ldots\ldots, b$ as an n – degree polynomial of the form. $b_n x^n + b_{n-1} x^{n-1} + \ldots\ldots + b_1 x + b_0$. Then simply use the multiplication procedure of part (b) to multiply two n – bit integers represented as polynomials in $O\left(n^{\lg 3}\right)$ time.

- 教材讨论
  - TJ第16章第1、2、5节

问题1：环和域

- 你能“增量式”地定义这些概念吗？



结合律、单位元、逆元

交换律

乘法结合律、分配律

乘法交换律

乘法单位元

ab=0 → a=0或b=0

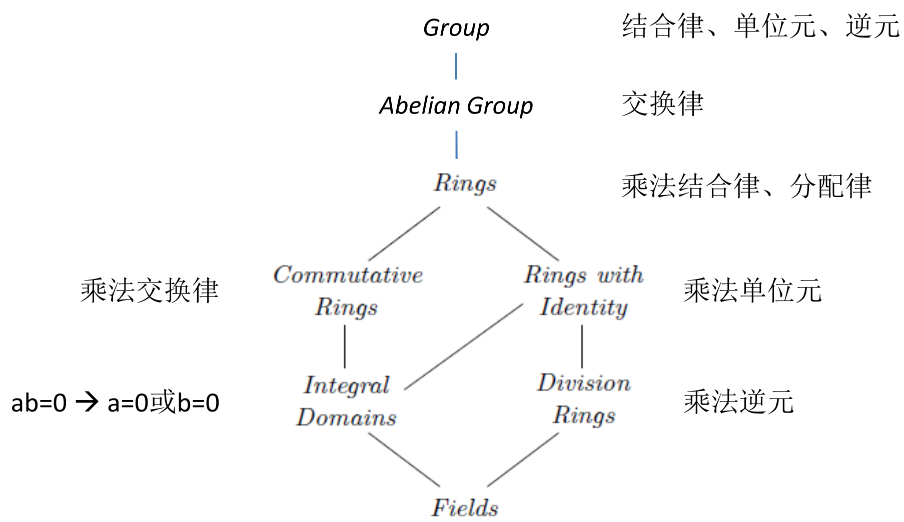
乘法逆元

它关于乘法构成群吗？

为什么Filed是Integral Domain？

问题2：环和域的例子

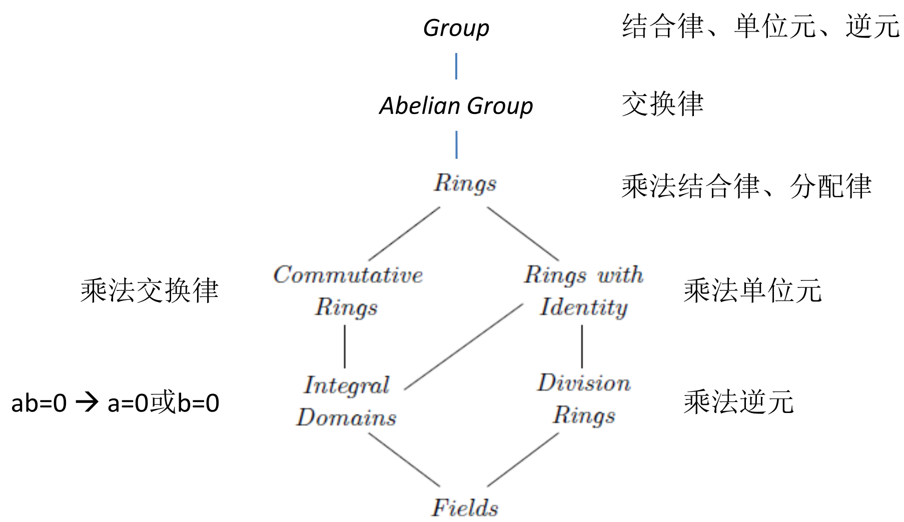
- 自然数？
  - 连Group都不是
- 整数？
  - Integral Domain
- 有理数？
  - Field
- 实数？
  - Field
- 复数？
  - Field



问题2：环和域的例子 (续)

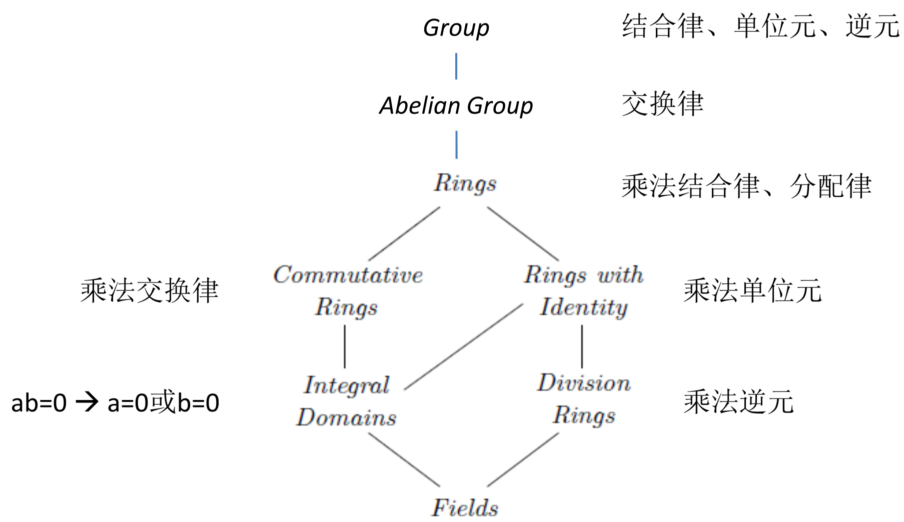
- Gaussian integer?
  - Integral Domain

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \text{ where } i^2 = -1.$$



问题2：环和域的例子 (续)

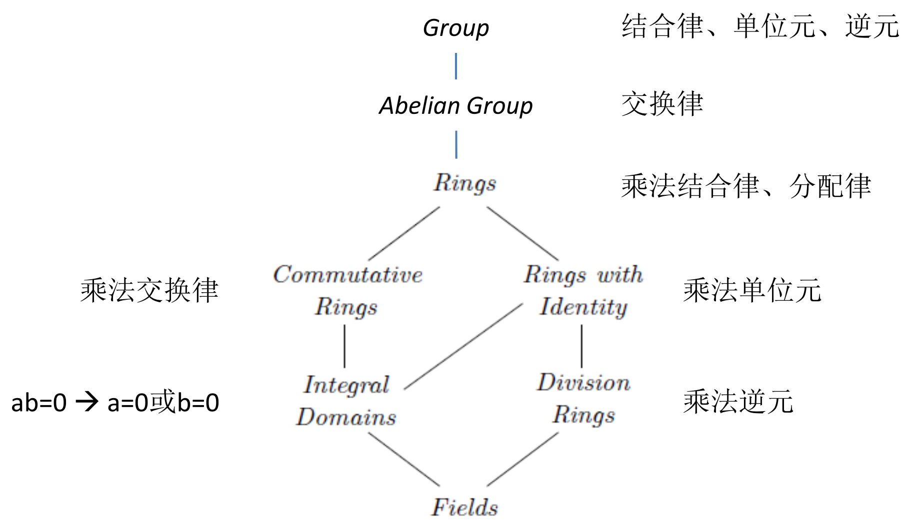
- Z_n?
  - Commutative Ring & Ring with Identity
- 增加什么条件可以成为Field?



问题2：环和域的例子 (续)

- 2x2实数矩阵？
  - Ring with Identity

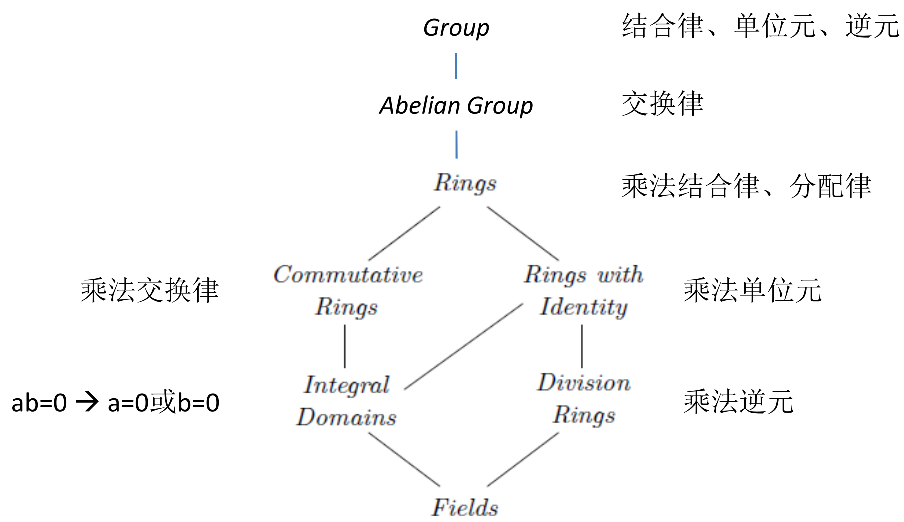
$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$$



问题2：环和域的例子 (续)

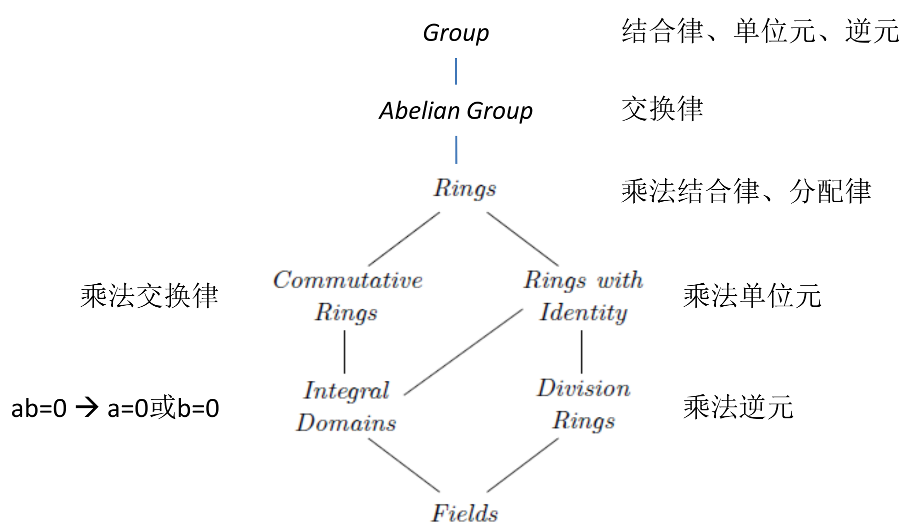
- 实数多项式？
  - Integral Domain

$$p = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m,$$



问题2：环和域的例子 (续)

- 分组讨论：怎样基于S的幂集构造一个Ring？
  - 加法：对称差
  - 乘法：交集
- 它是Commutative Ring吗？
- 它是Ring with Identity吗？
- 它是Integral Domain吗？
- 它是Division Ring吗？



问题3：子环

- 你能找出以下环的子环吗？
  - 整数
  - Gaussian integer $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \text{ where } i^2 = -1.$
  - Z_n
  - 2x2实数矩阵 $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \right\}$
  - 实数多项式 $p = p_0 + p_1 X + p_2 X^2 + \cdots + p_{m-1} X^{m-1} + p_m X^m,$
  - S的幂集