环的定义，例子，基本性质.

回顾：称代数结构 $(R;+;\cdot)$ 为环，如果

1° $(R;+)$ 为Abel群.

2° $(R;\cdot)$ 为幺半群.

3° $\forall a,b,c\in R$，有 $a\cdot(b+c)=ab+ac$. $(a+b)c=ac+bc$.

特别地，若 R 在 $\cdot$ 下满足交换律，则称 $(R,\cdot,\cdot)$ 为交换环.

例子.

1、 $(\mathbb{Z}_2;\overset{\text{模2}}{\oplus};\underset{\text{模2}}{\cdot})$. 交换环.

2、 对 $n\in\mathbb{Z}^+$，考虑 $\mathbb{Z}_2^n=\{(i_1,i_2,\dots,i_n)\mid i_j\in\{0,1\},j=1,\dots,n\}$

定义 $\mathbb{Z}_2^n$ 上的 $\oplus$ 为各分量的模2加法；$\cdot$ 为各分量上的模2乘法.

则 $(\mathbb{Z}_2^n;\oplus;\cdot)$ 也是交换环.

3、 回顾：集合的对称差：$A\oplus B=(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$

（得到在且仅在 A,B 中的一个的元素）

给定集合 X，记 X 的幂集为 $P(X)$. 则 $(P(X);\oplus;\cap)$ 是环.

验证： $(P(X);\oplus)$ 为Abel群：结合、交换律，

幺元为 ϕ. $A^{-1}=A$.

$(P(X);\cap)$ 为幺半群. 幺元为 X.

分配律： $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$ （只验证一边即可）

事实上，例2和例3是有联系的：

对 $n\in\mathbb{Z}$. 考虑 $\mathbb{Z}_2^n$ 与 $X=\{1,2,\dots,n\}$.

作映射 $\varphi:\mathbb{Z}_2^n\to P(X)$. $\forall(a_1,a_2,\dots,a_n)\in\mathbb{Z}_2^n$，$\varphi(a_1,\dots,a_n)=\{i\mid a_i=1,1\le i\le n\}$ 支撑集

显然 φ 是双射. 更进一步，φ 还有某种"保持运算"的性质！

我们有：$\varphi(\alpha\oplus\beta)=\varphi(\alpha)\oplus\varphi(\beta)$. $\forall\alpha,\beta\in\mathbb{Z}_2^n$.

pf: $\alpha_i+\beta_i=1\Leftrightarrow\alpha_i=0,\beta_i=1$ 或 $\alpha_i=1,\beta_i=0$

$\Leftrightarrow i\in B-A$ 或 $i\in A-B$ $(A=\varphi(\alpha),B=\varphi(\beta))$

$\Leftrightarrow i\in A\oplus B$

还有：$\varphi(\alpha\beta)=\varphi(\alpha)\cap\varphi(\beta)$

pf: $\alpha_i\beta_i=1\Leftrightarrow\alpha_i=\beta_i=1\Leftrightarrow i\in A\cap B$.

因此，虽然还没有正式给出定义，但 φ 就是个环同构.

4. 群环.

设 G 为有限群，$\mathbb{C}$ 为复数域. 定义 $\mathbb{C}^G:=\{f\mid f:G\to\mathbb{C}\}$

考虑 $\mathbb{C}^G$ 上的加法：$\forall f,g\in\mathbb{C}^G$，$(f+g)(a):=f(a)+f(g)$，$\forall a\in\mathbb{C}$

乘法：$(f*g)(a)=\sum_{\substack{b,c\in G^2\\ bc=a}}f(b)g(c)=\sum_{b\in G}f(b)g(b^{-1}a)$

则 $(\mathbb{C}^G;+)$ 为交换群. $(\mathbb{C}^G;*)$ 为幺半群. 保持分配律. $(\mathbb{C}^G;+;*)$ 构成环

这个结构是在十九、二十世纪之交提出的. 它将数域上的性质引入了群中.

事实上，有很多关于群的性质是通过过渡到这样的群环上，利用环论性质间接完成的.

5. 四元数环.

考虑 $R:=\left\{\begin{pmatrix}\alpha&\beta\\-\bar\beta&\bar\alpha\end{pmatrix}\middle|\,\alpha,\beta\in\mathbb{C}\right\}$

由于 $M_2(\mathbb{C})$ 本身就成环，因此只需验证封闭性.

$$\begin{pmatrix}\alpha&\beta\\-\bar\beta&\bar\alpha\end{pmatrix}+\begin{pmatrix}\gamma&\theta\\-\bar\theta&\bar\gamma\end{pmatrix}=\begin{pmatrix}\alpha+\gamma&\beta+\theta\\-\overline{(\beta+\theta)}&\overline{\alpha+\gamma}\end{pmatrix}$$

$$\begin{pmatrix}\alpha&\beta\\-\bar\beta&\bar\alpha\end{pmatrix}\begin{pmatrix}\gamma&\theta\\-\bar\theta&\bar\gamma\end{pmatrix}=\begin{pmatrix}\alpha\gamma-\beta\bar\theta&\alpha\theta+\beta\bar\gamma\\-\bar\beta\gamma-\bar\alpha\bar\theta&-\bar\beta\theta+\bar\alpha\bar\gamma\end{pmatrix}=\begin{pmatrix}\alpha\gamma-\beta\bar\theta&\alpha\theta+\beta\bar\gamma\\-\overline{(\alpha\theta+\beta\bar\gamma)}&\overline{\alpha\gamma-\beta\bar\theta}\end{pmatrix}$$

事实上，$(R;+;\cdot)$ 就是 $(M_2(\mathbb{C});+;\cdot)$ 的子环.

我们知道，$\mathbb{C}$ 是将 i 添加到 $\mathbb{R}$ 中得到的. 那么能否向 $\mathbb{C}$ 中添加更多的东西得到更大的系统？这个问题引导了四元数的提出. (Hamilton, 1843)

很明显，当 $\beta=0$ 时，四元数与复数一一对应，因此前者确实是后者的扩充.

考虑 $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$i=\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix}$，$j=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，$k=\begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix}$

可以看出 (I_2,i,j,k) 为 R 的一组基.

$I_2=i^2=j^2=k^2$；$ij=k$，$ji=-k$.

从这里就可以看出它与通常数域的不同.（二次方程有3个根！）

当矩阵被引入后，人们意识到四元数不过是矩阵的一部分.

6. 模 n 的剩余类环.

考虑 $n\in\mathbb{Z}^+,n\ge2$，结构 $(\mathbb{Z}_n;\overset{\text{模n加法}}{\oplus};\underset{\text{模n乘法}}{\otimes})$.

则有 $(\mathbb{Z}_n;\oplus)$ 为循环群（那当然是Abel群）

$(\mathbb{Z}_n;\otimes)$ 为交换幺半群. 结合律：$(a\otimes b)\otimes c=a\otimes(b\otimes c)=(abc)\bmod n$.

因为 $(a\otimes b)\otimes c\equiv(a\otimes b)c\equiv(ab)c=abc\pmod n$

同理有另一式. 故结合律成立.

分配律的验证是类似的（利用同余式的性质）

Thm. 设 $(R;+;\cdot)$ 为环，$a,b\in R$. 则有：

(1) $a0=0a=0$

(2) $-(ab)=(-a)b=b(-a)$

pf: (1) $a0=a(0+0)=a0+a0$ （分配律）

又由 $(R;+)$ 的消去律，有 $a0=0$

另一边是类似的.

(2) $0=a0=a(b+(-b))=ab+a(-b)$

$\Rightarrow a(-b)=-(ab)$

另一边也是类似的

域的概念与例子.

$(F;+;\cdot)$ 是域，指

(1) $(F;+;\cdot)$ 是交换环

(2) $\forall a\in F$，$a\neq0_F$，$\exists b\in F$，使 $ab=ba=1_F$.

或者等价地，

(1) $(F;+)$ 为交换群

(2) $(F;\cdot)$ 是交换幺半群，$(F-\{0\};\cdot)$ 是群

(3) 满足左右分配律.

例子：$(\mathbb{Q};+;\cdot)$，$(\mathbb{R};+;\cdot)$，$(\mathbb{C};+;\cdot)$ 是域

$(\mathbb{Z};+;\cdot)$ 不是（不满足乘法逆元性质）

$K=\{a+b\sqrt2\mid a,b\in\mathbb{Q}\}$，$(K;+;\cdot)$ 是域.

只需验证封闭性：

$(a_1+b_1\sqrt2)+(a_2+b_2\sqrt2)=(a_1+a_2)+(b_1+b_2)\sqrt2\in K$

$(a_1+b_1\sqrt2)\cdot(a_2+b_2\sqrt2)=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt2\in K$

$$\frac{1}{a+b\sqrt2}=\frac{a-b\sqrt2}{(a+b\sqrt2)(a-b\sqrt2)}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt2\in K$$

这个域叫作 $\mathbb{Q}(\sqrt2)$，表示将 $\sqrt2$ 加入 $\mathbb{Q}$ 后的最小域，这个过程叫作"扩域".

在Week 14, 15 中，我们将系统地研究这一主题.

类似地，$K:=\{a+b\cdot\sqrt[3]{2}+c\cdot\sqrt[3]{4}\mid a,b,c\in\mathbb{Q}\}$，$(K;+;\cdot)$ 也是域.

$=\mathbb{Q}(\sqrt[3]{2})$

不是域的例子：

$\mathbb{Z}_n:=\{0,1,\dots,n-1\}$. $(\mathbb{Z}_n;\underset{\text{模n加}}{\oplus};\underset{\text{模n乘}}{\otimes})$ 为交换环.

可以验证 $(\mathbb{Z}_6;\oplus;\otimes)$ 不是域. 因为有元素没有逆元（例如2）

假设2在 $(\mathbb{Z}_6;\oplus;\otimes)$ 中有逆元 x，则 $2\otimes x=1$. 即 $2x\equiv1\pmod 6$

则 $2x$ 为奇数，矛盾！故2无逆元.

事实上，若 n 为合数，则 $(\mathbb{Z}_n;\oplus;\otimes)$ 都不可能为域. 原因是，我们后面会证明域的一个重要基本性质：域中两元素积 $pq=0\Rightarrow p=0$ 或 $q=0$. 而当 n 为合数，$n=pq$ 时，$(\mathbb{Z}_n;\oplus;\otimes)$ 中就有两个非零元 p,q 乘积为零，因此不可能为域.

但是反过来，若 n 为素数，则 $(\mathbb{Z}_n;\oplus;\otimes)$ 一定为域. 这背后是一个数论性质：非零整数模素数一定有数论倒数（用代数的语言，即为乘法逆元）

总结下来即 $(\mathbb{Z}_n;\oplus;\otimes)$ 构成域 $\Leftrightarrow$ n 为素数.