Week 2 摘要

注："摘要"是对笔记内容的总结、思路的引导、学习的建议。我们强烈建议读者在阅读正文前、阅读正文时和阅读正文后随时参阅，以期获得最好的效果。

在 Week 1 中，我们引入了群的概念及相关简单性质。在本周，我们按照代数研究的一般规律——对于复杂结构，去研究其更简单的、同时保持性质的子结构。在群论中，就是去研究子群。我们的思路如下：

① 引入带余除法，这在后续若干定理的证明中都将起到作用；并基于此引入两个不借助群论语言描述，但在本质上是对群 $(\mathbb{Z};+)$ 的子群的刻画，以及其应用。建议读者体会其与抽象的子群定义的联系，以及这种群的抽象性质应用于具体事例的做法。

② 引入严格的子群的抽象定义。我们建议读者体会其与"线性空间的子空间"的概念比较，以认识到这种保持性质的子结构的研究在数学中是普遍存在的一般思路。事实上，后面在环论、域论中也会有类似的处理。

③ 阐述了子群的若干简单性质。在我们刚刚引入的定义中，并没有说明"子群是群"，此处阐明了。此外，子群的幺元、逆元与"母群"的一致性证明中有些许细节，需要认真体会。

④ 子群之间的若干运算。同②中阐述的观点类似，这也是常见的处理。

⑤ 从同余关系引入陪集分解。此处的抽象过程略不易懂，需要仔细体会。该部分内容留待 Week 3 详述。

带余除法的唯一性

设有 $b=qa+r=q'a+r'$ 下证 $q=q'$，$r=r'$

$q'a+r'=qa+r$

$\Rightarrow r-r'=a(q'-q)$

$\Rightarrow |r-r'|=a|q-q'|$

$0\le r,r'\le a-1 \Rightarrow 1\le |r-r'|\le a-1<a$

$\Rightarrow |q-q'|<1 \Rightarrow q=q'$

命题：设 $A\subseteq\mathbb{Z}^+$，$A\neq\phi$，满足：

(1) $\forall a,b\in A$，$a+b\in A$

(2) $\forall a,b\in A$，$a<b$，$b-a\in A$

则 $\exists c\in\mathbb{Z}^+$，使 $A=\{cq\mid q\in\mathbb{Z}^+\}$

pf：取 c 为 A 中的最小数。下证 $A=\{cq\mid q\in\mathbb{Z}^+\}=:A'$

先证 $A'\subseteq A$。由 A 对加法的封闭性显然成立。

再证 $A\subseteq A'$。任取 $b\in A$。作带余除法 $b=qc+r$，$0\le r\le c-1$，$q\in\mathbb{Z}^+$

假设 $r\neq 0$，由 $A'\subseteq A$ 知 $qc\in A$，从而 $r=b-qc\in A$，这与 c 的最小性矛盾！

故 $r=0$，即 $b=qc$

上述命题的一个应用：

例. 设 X 为 n 元有限集，σ 是 X 到 X 的双射。$y\in X$。

$A:=\{l\in\mathbb{Z}^+\mid\sigma^l(y)=y\}$

首先说明 $A\neq\phi$。考虑 $y,\sigma(y),\sigma^2(y),\dots,\sigma^n(y)\in X$，$n=|X|$

这 $(n+1)$ 个数中，由鸽笼原理知存在 $0\le i<j\le n$ 使 $\sigma^i(y)=\sigma^j(y)=\sigma^i(\sigma^{j-i}(y))$

σ^i 双射 $\Rightarrow y=\sigma^{j-i}(y)$。又 $1\le j-i\le n\Rightarrow j-i\in A$。故 $A\neq\phi$。

验证两条性质：设 $a,b\in A$。则有 $\sigma^{a+b}(y)=\sigma^a(\sigma^b(y))=\sigma^a(y)=y$

$\Rightarrow a+b\in A$

设 $a,b\in A$，$b>a$。则有 $\sigma^{b-a}(y)=\sigma^{b-a}(\sigma^a(y))=\sigma^b(y)=y$.

$\Rightarrow b-a\in A$.

则由上述命题可知：$c=\min A$ 满足 $A=\{cq\mid q\in\mathbb{Z}^+\}$

$y,\sigma(y),\sigma^2(y),\dots,\sigma^{c-1}(y)$ 两两不同。继续复合则周期循环。

例. 设 X 为有限集。$(a_1,a_2,\dots,a_n)$ 是 X 上的序列。

$$\text{"旋转" } k \text{ 次}\left\{\begin{array}{l}(a_1,a_2,\dots,a_n)\\ \downarrow\\ (a_n,a_1,\dots,a_{n-1})\\ \downarrow\\ (a_{n-1},a_n,\dots,a_{n-2})\\ \downarrow\\ \vdots\\ (a_{n-k+1},a_{n-k+2},\dots,a_{n-k})\end{array}\right.$$

考虑类似的"旋转"操作。

显然，旋转 n 次后序列回到自己。那么最少需重复多少次？

固定 $(a_1,\dots,a_n)$。设 $A:=\{l\in\mathbb{Z}^+\mid(a_1,\dots,a_n)$ 在 l 次操作后返回 $(a_1,\dots,a_n)\}$

易知 $n\in A\neq\phi$。且 A 满足命题中的两个条件。

则有 $A=\{cq\mid q\in\mathbb{Z}\}$。$c=\min A$

又有 $n\in A$。则有 $c\mid n$。

那么 $(a_1,\dots,a_n)$ 形如 $(\underbrace{a_1,\dots,a_c,a_1,\dots,a_c,\dots,a_1,\dots,a_c}_{\frac{n}{c}\text{个 } a_1,\dots,a_c})$.

以上是若干对 $(\mathbb{Z};+)$ 子群性质的刻画及应用。

定理（对 $(\mathbb{Z};+)$ 的子群的刻画）

(1) 设 $H\subseteq\mathbb{Z}$，$H\neq\phi$。且 $\forall a,b\in H$ 总有 $a+b\in H$，$-a\in H$。

则 $\exists c\in\mathbb{N}$，s.t. $H=\{cq\mid q\in\mathbb{Z}\}$。

(2) 设 $c\in\mathbb{Z}$，$H=\{cq\mid q\in\mathbb{Z}\}$。则 $a,b\in H$，有 $a+b\in H$，$-a\in H$.

pf：只证(1)。

先证 $0\in H$。由 $H\neq\phi$。任取 $x\in H$。则由条件有 $-x\in H$。

从而 $x+(-x)=0\in H$.

考虑 $A=H\cap\mathbb{Z}^+$。分两种情况讨论。

1° 若 $A=\phi$。下证 $H=\{0\}$。假设 $\exists a<0$，$a\in H$

则有 $-a>0$，$-a\in H$。矛盾。故 $H=\{0\}$。取 $c=0$ 满足要求。

2° 若 $A\neq\phi$。则由命题知 $A=\{cq\mid q\in\mathbb{Z}^+\}$，$\exists c\in\mathbb{Z}^+$.

下证 $H=\{cq\mid q\in\mathbb{Z}\}$.

显然有 $\{cq\mid q\in\mathbb{Z}\}\subseteq H$.

任取 $h\in H$。若 $h>0$，则 $h\in A\Rightarrow h=cq$，$\exists q\in\mathbb{Z}^+$

若 $h<0$。则 $-h\in A\Rightarrow -h=cq\Rightarrow h=c\cdot(-q)$。$\exists q\in\mathbb{Z}^+$.

即总有 $h\in\{cq\mid q\in\mathbb{Z}\}$. $\Rightarrow H\subseteq\{cq\mid q\in\mathbb{Z}\}$.

$\Rightarrow H=\{cq\mid q\in\mathbb{Z}\}$.

由此我们可以看出，$(\mathbb{Z};+)$ 的子群都具有 $\{cq\mid q\in\mathbb{Z}\}$，$c\in\mathbb{Z}$ 的结构。

更抽象地，接下来我们定义一般群的子群。（记作 $H\le G$）

Def. 设 $(G;\cdot)$ 构成群。称 $H\subseteq G$ 为 G 的子群，若 H 满足如下三个条件：

(1) $H\neq\phi$

(2) H 对运算 $\cdot$ 封闭

(3) $\forall a\in H$，有 $a^{-1}\in H$（其中 a^{-1} 是 a 在群 $(G;\cdot)$ 中的逆元）

我们可以看出上述定理的条件描述的正是这种定义的特例。

回顾：线性空间的子空间：

称 $U\subseteq\mathbb{R}^n$ 为 $\mathbb{R}^n$ 的 $\mathbb{R}$-子空间，若 (1) $U\neq\phi$ (2) $\forall x,y\in U$，$x+y\in U$ (3) $\forall a\in\mathbb{R}$，$\forall x\in U$，$ax\in U$.

这里我们也要求封闭性的保持。这是我们对代数结构的子结构研究的一般要求（运算的继承）

Fact.

(1) 设 H 是 $(G;\cdot)$ 的子群。则 $e_G\in H$，且 $(H;\cdot)$ 构成群。

pf：先证 $e_G\in H$。由 $H\neq\phi$。任取 $x\in H$。由定义知 $x^{-1}\in H$.

从而由封闭性有 $x\cdot x^{-1}=e_G\in H$.

验证 $(H;\cdot)$ 构成群——二元运算的定义与封闭性、结合律的成立（继承自 G）

幺元的存在（由逆元性质与封闭性保证）.

逆元的存在（定义）

(2) 设有 $H\subseteq G$，且 H、G 对运算 $\cdot$ 都构成群。则 H 是 G 的子群。

pf：只验证逆元性质。

先证 $e_G\in H$（我们现在还不知道 $e_G=e_H$）

由已知，$e_H\cdot e_H=e_H$（因为 e_H 是 H 的幺元）

又 $e_H\in G$。故有 $e_H=e_H\cdot e_G$（因为 e_G 是 G 的幺元）

从而 $e_H\cdot e_H=e_H\cdot e_G$

由 G 中的消去律，有 $e_H=e_G\in H$.

$\forall a\in H$。由 H 是群，$e_G\in H$ 是 H 的幺元。

故 $\exists b\in H$ 使 $ab=ba=e_G$.（目前还不知 b 是 a 在 G 中的逆元，

$=a\cdot a^{-1}=a^{-1}\cdot a$ 　只知 b 是 a 在 H 中的逆元）

在 G 中对上式用消去律，有 $b=a^{-1}$ 又 $b\in H$ 故 $a^{-1}\in H$.

"子群自身也是群！" 　需要注意的是：子群的幺元、逆元均是"母群"的幺元、逆元

这是需要证明的.

回忆：线性子空间的运算性质.

设 U、V 是 $\mathbb{R}^n$ 的 $\mathbb{R}$-子空间

则有 $U\cap V$ 为子空间

$U+V:=\{x+y\mid x\in U,y\in V\}$ 为子空间.

且有 $\dim(V+U)+\dim(V\cap U)=\dim(U)+\dim(V)$.

那么子群是否也有类似的性质呢？接下来研究子群的基本运算.

子群的交.

(1) $A\le G$，$B\le G$，则有 $A\cap B\le G$. $\Rightarrow$ 任意多个子群的交仍是子群. 对于无穷多的子群仍成立.

pf：1° 非空. 由 $e\in A$，$e\in B$，则有 $e\in A\cap B\Rightarrow A\cap B\neq\phi$

2° 对 $a,b\in A\cap B$. 由 $\left.\begin{array}{l}a,b\in A\Rightarrow a^{-1},b^{-1},ab\in A\\ a,b\in B\Rightarrow a^{-1},b^{-1},ab\in B\end{array}\right\}\Rightarrow a^{-1},b^{-1},ab\in A\cap B$

$\{A_i\mid i\in I\}$ 是 G 的一组子群 $\Rightarrow\bigcap_{i\in I}A_i\le G$. 证明是类似的.

(2) $A\le G$，$B\le G$ $\not\Rightarrow$ $A\cup B\le G$

(3) 类似于线性子空间的加法，能否定义子群的加法？

在研究以上两个问题之前，我们先考虑子群的生成.

回顾：对 $x\in\mathbb{R}^n$. 由 x 生成的子空间 $:=\{ax\mid a\in\mathbb{R}\}$.

$x,y\in\mathbb{R}^n$，由 x,y 生成的子空间 $:=\{ax+by\mid a,b\in\mathbb{R}\}$

Def. 任取 $S\subseteq G$，称 $H\subseteq G$ 是 S 在 G 中生成的子群，如果：

(1) $H\le G$，$S\subseteq H$

(2) H 的最小性：若有 $H'\le G$，$S\subseteq H'$，则 $H\subseteq H'$.

我们可以看到，"用子集定义其生成的子结构"的做法在线性子空间的定义中也是类似的.

但是，H 是否是唯一的？

命题：设 $S\subseteq G$，则 S 在 $(G;*)$ 中生成的子群存在且唯一，记作 $\langle S\rangle$.

pf：唯一性：设 H_1、H_2 都是 S 在 G 中生成的子群.

则由子群的定义有 $H_1\subseteq H_2$，$H_2\subseteq H_1\Rightarrow H_1=H_2$.

存在性：考虑 $T:=\{H\mid H\le G,S\subseteq H\}$.

我们断言：$H\neq\phi$，且 $\bigcap_{H\in T}H=\langle S\rangle$.

由 $S\subseteq H$，可知 $H\neq\phi$.

由子群交的封闭性，可知 $\bigcap_{H\in T}H\le G$.

又 $\forall H\in T$，有 $S\subseteq H$. 有 $S\subseteq\bigcap_{H\in T}H$.

又 $\forall K\in T$，有 $\bigcap_{H\in T}H\subseteq K$.

从而综上有 $\bigcap_{H\in T}H=\langle S\rangle$.

存在性的证法是常见的处理.

上述给出的构造是很抽象的，我们有如下更具体的形式：

$S\subseteq G$，则 $\langle S\rangle=\{a_1^{c_1}a_2^{c_2}\cdots a_n^{c_n}\mid n\in\mathbb{N},\forall 1\le i\le n,a_i\in S,c_i=\pm 1\}$.

直观来看，上述形式保证了 $\cdot$ 运算与求逆的封闭性.

可以看到它比线性子空间的形式复杂很多，这是因为群中没有交换律.

Fact.

$a,b,c\in(G;\cdot)$，则：$(ab)^{-1}=b^{-1}a^{-1}$. $(a^{-1})^{-1}=a$. $ab=c\Leftrightarrow a=cb^{-1}\Leftrightarrow b=a^{-1}c$

回到子群的"并"与"和"的问题.

对 $A\subseteq G$，$B\subseteq G$，定义 $AB:=\{ab\mid a\in A,b\in B\}$（在代数结构的研究中是常见的做法）.

（对于单点集与子群的情况，这实际上是左、右陪集） 　我们常常通过研究这些子结构上的运算来研究整体的结构.

$A\le G$，$B\le G\not\Rightarrow AB\le G$ 　回顾线性空间的情形：

$(u_1+v_1)+(u_2+v_2)=\underbrace{(u_1+u_2)}_{\in U}+\underbrace{(v_1+v_2)}_{\in V}\in U+V$

这里用到了线性空间的交换律. 不能直接"平移"到群中.

Thm. 设 $A\le G$，$B\le G$. 则下面三个条件等价：

(1) $AB\le G$

(2) $BA\subseteq AB$

(3) $AB=BA$.

此时有 $|AB|=\dfrac{|A||B|}{|A\cap B|}$

关于子群的并：设 $A\le G$，$B\le G$，则 $A\cup B\le G\Longleftrightarrow A\subseteq B$ 或 $B\subseteq A$.

（这就是为什么我们不研究子结构之间的并关系）.

群的陪集分解.

回顾：同余关系（陪集分解的一个例子）

这是我们所熟知的，从略.

从群的角度来看同余关系.

$H\le(\mathbb{Z};+)\Leftrightarrow\exists c\in\mathbb{N}$，$H=\{cq\mid q\in\mathbb{Z}\}$.

对给定的 $n\in\mathbb{N}$. $H:=\{nq\mid q\in\mathbb{Z}\}$.

那么 $a\equiv b\pmod n\Longleftrightarrow n\mid b-a\Leftrightarrow b-a\in H$.

特别地，$a\equiv 0\pmod n\Longleftrightarrow a\in H$.

那么，对于更一般的群、子群、等价关系，是否可以建立类似的关系？

Def. 设 $(G;*)$ 为群，$H\le G$. 如下定义 G 上的二元关系 $\sim$

$\forall a,b\in G$，$a\sim b\Longleftrightarrow a^{-1}b\in H$. 类比于同余定义中的减法.

（可理解为"左模 H"，强调与同余的类比.）

则有 (1) $\sim$ 是 G 上的等价关系.

(2) $a\sim b\Rightarrow xa\sim xb$，$\forall x\in G$.

(3) 对 $a\in G$，有 $[a]=\{ah\mid h\in H\}=aH$.（陪集在此被自然地引入了）.

$\Rightarrow$ Lagrange Thm.，陪集分解

理解上述定义与同余关系的联系.

考虑 $(\mathbb{Z};+)$ 的子群 $H:=\{nq\mid q\in\mathbb{Z}\}$. 按上述方式定义的二元关系 $\sim$：$a\sim b\Leftrightarrow a^{-1}b=-a+b\in H$

亦即 $n\mid b-a$，即 $a\equiv b\pmod n$

该等价关系诱导的等价类即模 n 的同余类.