Week 3 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之前、阅读正文时和阅读正文后随时参阅，以期获得最好的效果.

(1) 在上周的结尾，我们通过同余的例子引入了一种基于子群定义的一种特殊的等价关系 $\sim$，在本周，我们将更进一步基于此引入陪集分解的概念. 我们强烈建议读者与 $(\mathbb{Z};+)$ 的子群、同余关系、同余类的概念对照着理解一般的抽象子群 H、H 定义的等价关系 $\sim$，以及陪集的概念，否则将较难理解这组概念的实际意义. 我们在笔记中将为读者详细梳理这一例子，请格外注意. 详见从同余关系看陪集分解.

建立起了等价关系 $\sim$ 与陪集的联系后，我们进一步地引入了对整个群 G 的陪集分解，并作为推论得到了群论中的重要定理——Lagrange 定理. 它作为子群构成的必要条件，将在我们对子群的研究中发挥重要作用. 此外，我们在此第一次引入了商集 $G/H:=\{aH \mid a\in G\}$ 的概念. 在后续的学习中，我们将会看到，当子群 H 为正规子群时，商集 G/H 将构成群.

(2) 我们将实数上的一般整数次幂引入了群中. 这将为我们后续的讨论带来方便.

(3) 在 Week 2 中，我们给出了子集 S 生成的子群 $\langle S\rangle$ 的一个具体的表达式. 基于此，我们开始研究最简单的情况，即 S 为单元素集的情况，这就是循环群. 为了确定循环群的元素个数，我们自然地引入了阶的概念，进而彻底确定了循环群的结构. 熟悉初等数论的读者不妨将其与初等数论中"阶"的概念进行对比.

(4) 最后，我们引入了同态与同构的概念并给出了若干例子，其中的一部分并不显然.

群的左陪集分解.

给定群 G 及群 G 的子群 H. 如下定义 G 上的二元关系 $\sim$.

$\forall a,b\in G$, $a\sim b \overset{\wedge}{\Longleftrightarrow} a^{-1}b\in H$.

例子：$G:=(\mathbb{Z};+)$. $H:=\{nq \mid n\in\mathbb{Z}\}$, $q\in\mathbb{Z}$

则此处的 $\sim$ 即为 $\equiv(\mathrm{mod}\ n)$.

Fact.

(1) $(G,\sim)$ 是一个等价关系 $\Longrightarrow$ 集合的划分，在此处即陪集分解.

(2) $\forall a,b\in G$, $a\sim b\Longleftrightarrow \exists h\in H$ st. $b=ah$.

pf: (2) 若有 $a^{-1}b\in H$，则有 $a^{-1}b=h\in H$. 即 $b=ah$

若有 $b=ah$, $h\in H$. 则有 $a^{-1}b=a^{-1}(ah)=h\in H$.

(1) 自反性：$a\sim a\Longleftrightarrow a^{-1}a=e\in H$. 成立

对称性：$a\sim b\Longleftrightarrow a^{-1}b\in H\Longleftrightarrow (a^{-1}b)^{-1}=b^{-1}a\in H\Longleftrightarrow b\sim a$

传递性：$a\sim b, b\sim c\Rightarrow a^{-1}b, b^{-1}c\in H\Rightarrow (a^{-1}b)(b^{-1}c)=a^{-1}c\in H\Rightarrow a\sim c$.

从证明过程中我们可以看到 H 的群性质起到了重要作用.

(3) 设 $a\in G$，则有 $[a]=aH$. 其中 $[a]=\{b \mid a\sim b\}$. $aH:=\{ah \mid h\in H\}$ (2)的推论.

称作"左陪集". 类似地可定义"右陪集".

亦即，a 所在的等价类 $=$ a 所在的关于 H 的左陪集.

记 $G/H:=\{aH \mid a\in G\}$ 为全体等价类. 称为 G 对 H 的商集.

由等价类的性质，我们有：$xH\cap yH\neq\phi\Longleftrightarrow xH=yH\Longleftrightarrow x^{-1}y\in H$.

至此，我们将群 G 对其子群 H 划分为了若干等价类.

从同余关系看陪集分解.

在 Week 2 中，我们已经明确，$(\mathbb{Z};+)$ 的任意子群 H 都具有 $H=\{nq \mid q\in\mathbb{Z}\}$, $n\in\mathbb{Z}$ 的形式.

对于给定的 n, H，这里的等价关系 $\sim$ 就被定义为：

$$a\sim b\overset{\wedge}{\Longleftrightarrow} a^{-1}b\in H\Longleftrightarrow b-a=nq,\ \exists q\in\mathbb{Z}\Longleftrightarrow n\mid b-a\Longleftrightarrow a\equiv b\ (\mathrm{mod}\ n)$$

读者自此可以看出这里 $a^{-1}b$ 的含义. 在同余的例子中，它所做的就是"消去余数".

那么这里的陪集，即等价类是什么呢？事实上就是所有模 n 的同余类

$0H=0+H=\{nq \mid q\in\mathbb{Z}\}=\{a \mid a\sim 0$，即 $a\equiv 0\ (\mathrm{mod}\ n)\}$

$1H=1+H=\{1+nq \mid q\in\mathbb{Z}\}=\{a \mid a\sim 1$，即 $a\equiv 1\ (\mathrm{mod}\ n)\}$

……

$(n-1)H=(n-1)+H=\{(n-1)+nq \mid q\in\mathbb{Z}\}=\{a \mid a\sim n-1$，即 $a\equiv n-1\ (\mathrm{mod}\ n)\}$

为什么称 G/H 为"商集"呢？我们不妨如此理解. 商集的每个元素是一个 $\sim$ 等价类，元素之间没有等价关系，而等价类内部的等价关系也在商集的这个层次被我们忽略了，可以理解为等价关系 $\sim$ 被"除掉了"，所有等价的元素被"约掉了".

Lagrange Thm.

对有限群 G 及其子群 H，有 $|G|=|H|\cdot|G/H|$. 特别地，有 $|H|\,\big|\,|G|$

pf: $(G;\sim)$ 为等价关系 $\Rightarrow$ G/H 构成 G 的分划，即它们两两无交且并为 G

$\Rightarrow |G|=\sum\limits_{A\in G/H}|A|$ ⊛

由群的消去律，有 $\forall a\in G$, $|aH|=|H|$. (假设有 $ah_1=ah_2\Rightarrow a^{-1}(ah_1)=a^{-1}(ah_2)$，即 $h_1=h_2$)

则有⊛ $=\sum\limits_{A\in G/H}|H|=|H|\cdot|G/H|$.

Lagrange Thm. 给出了构成子群的一个必要条件，但这个条件并非充分的.

一个反例是，12 阶群没有 6 阶子群.

推论：设 G 有限且 $|G|$ 为素数，则 G 的子群仅有平凡子群 G、$\{e\}$.

(反之亦成立. 若 G 仅有平凡子群，则 G 有限，且 $G=\{e\}$ 或 $|G|$ 为素数)

注：存在与"左陪集分解"完全对称的"右陪集分解".

元素的幂

我们尝试将 $\mathbb{R}$ 上的幂运算性质推广到群上.

考虑半群 $(G;\cdot)$. 定义：$a^1:=a$,

$\forall k\in\mathbb{Z}^+$, $a^{k+1}:=a^k\cdot a$

则有：对 $m,n\in\mathbb{Z}^+$，有 $a^m\cdot a^n=a^{m+n}$

$(a^m)^n=a^{mn}$

(上述性质是容易证明的).

(正因有这样的性质，我们可以在任意的半群上执行快速幂算法.)

进一步地，考虑 $(G;\cdot)$ 为幺半群. $\forall a\in G$, $a^0:=e$

则上述性质从 $\mathbb{Z}^+$ 推广到 $\mathbb{N}$

更进一步地，考虑 $(G;\cdot)$ 为群. 对 $a\in G$, $m\in\mathbb{N}$.

定义 $a^{-m}:=(a^{-1})^m$ (事实上，我们会发现 $(a^{-1})^m=(a^m)^{-1}$，基于 $(xy)^{-1}=y^{-1}x^{-1}$ 对 m 归纳是容易的)

易于验证此时仍有 $a^{m+n}=a^m\cdot a^n$,

$(a^m)^n=a^{mn}$

回顾：设 $\{H_i \mid i\in I\}$ 为群 $(G;\cdot)$ 的一组子群，则 $\bigcap\limits_{i\in I}H_i$ 为子群.

$\Rightarrow$ 设 $S\subseteq G$，总存在唯一的子群 H 使得：

1) $S\subseteq H$. (2) $S\subseteq H'\leq G\Rightarrow H\subseteq H'$.

记为 $\langle S\rangle$. 我们有 $\langle S\rangle=\{a_1^{c_1}a_2^{c_2}\cdots a_n^{c_n} \mid n\in\mathbb{N}, a_i\in S, c_i=\pm1, i=1,\dots,n\}$. ⊛

注意到，如果 S 仅有一个元素，那么 $\langle S\rangle$ 的形式就会简单很多，我们接下来研究 $|S|=1$ 的情形.

取 $a\in G$. 记 $\langle a\rangle:=\langle\{a\}\rangle \overset{\text{由⊛式}}{=\!=\!=} \{a^j \mid j\in\mathbb{Z}\}$ (对于任意的群，我们已经定义了任意整数幂)

至此，$\langle a\rangle$ 看起来是一个无限群. 但是果真如此吗？从另一个角度问，是否 $\exists i\neq j$, $a_i=a_j$? ⊛

注意到，如果 $\exists c\in\mathbb{Z}$ st. $a^c=e$，那么 a^j, $j\in\mathbb{Z}$ 将会具有"周期性"而仅有有限多个元素.

于是接下来我们来研究方程 $a^c=e$.

一些例子：(从这些例子中，我们将探究⊛的成立条件)

平凡情形：$\langle e\rangle=\{e\}$

$a\in(\mathbb{C}^*,\cdot)$. $\langle a\rangle=\{a^j \mid j\in\mathbb{Z}\}$ 幺元 1.

$a=-1$, $\langle a\rangle=\{\pm1\}$ ⊛成立

$a=i$, $\langle a\rangle=\{i,-1,-i,1\}$ ⊛成立

$a=2$. $\langle a\rangle=\{2^j \mid j\in\mathbb{Z}\}$. ⊛不成立

$GL_2(\mathbb{R}):=\{2$ 阶可逆实方阵$\}$.

考虑 $A_1=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$ $A_2=\begin{pmatrix}1&1\\0&1\end{pmatrix}$

$A_1^2=I_2$. $A_2^j=\begin{pmatrix}1&j\\0&1\end{pmatrix}$, $j\in\mathbb{Z}$

$\Rightarrow\langle A_1\rangle=\{A_1,I_2\}$ $\Rightarrow\langle A_2\rangle=\{A_2^j \mid j\in\mathbb{Z}\}$

看了一些例子，接下来我们给出上述想法的严格描述：

设 $a\in(G;\cdot)$

1) 若存在 $n\in\mathbb{Z}^+$，使 $a^n=e$，则称 a 为有限阶元，并记

$o(a):=\min\{m\in\mathbb{Z}^+ \mid a^m=e\}$，称为 a 在群 G 中的阶.

例如，在 $(\mathbb{C};\cdot)$ 中，$o(-1)=2$, $o(i)=4$.

在 $(GL_2(\mathbb{R}),\cdot)$ 中，$o\begin{pmatrix}-1&0\\0&1\end{pmatrix}=2$.

2) 若 $\forall n\in\mathbb{Z}^+$，均有 $a^n\neq e$，则称 a 为无限阶元，记作 $o(a)=+\infty$.

事实上我们可以看出，一个元素的阶即它生成的循环群的阶：

Fact.

(1) 若 $a\in G$ 为 G 的无限阶元，则 $a^i=a^j$ 蕴含 $i=j$.

pf: $\forall n\in\mathbb{Z}^+$，有 $a^n\neq e$. 则有 $(a^n)^{-1}=a^{-n}\neq e$.

设有 $a^i=a^j$，则有 $a^{-i}\cdot a^i=a^{-i}\cdot a^j$

即 $a^{j-i}=e$

$\Rightarrow j-i=0$. 即 $i=j$.

(2) 设 $a\in G$ 为有限阶元. 记 $o(a)=m\in\mathbb{Z}^+$

1) 对 $j\in\mathbb{Z}$, $a^j=e\Longleftrightarrow m\mid j$

2) 对 $i,j\in\mathbb{Z}$, $a^i=a^j\Longleftrightarrow m\mid j-i\Longleftrightarrow i\equiv j\ (\mathrm{mod}\ m)$

3) $\langle a\rangle=\{a^j \mid j=0,1,\dots,m-1\}$. 且有 $|\langle a\rangle|=m$ (或者说，a^j, $j=0,\dots,m-1$ 互不重复)

Pf:

1) 若有 $m\mid j$. 记 $j=ml$. $l\in\mathbb{Z}$. 则有 $a^j=a^{ml}=(a^m)^l=e^l=e$

若有 $a^j=e$. 设 $j=qm+r$, $q\in\mathbb{Z}$, $0\leq r\leq m-1$

则有 $e=a^{qm+r}=a^{qm}\cdot a^r=(a^m)^q\cdot a^r=a^r$

由 m 的最小性，有 $r=0$. 即 $m\mid j$.

另证：$H:=\{i\in\mathbb{Z} \mid a^i=e\}$

则有 $H\leq(\mathbb{Z};+)$，由 Week 2 结论有 $H=\{mq \mid q\in\mathbb{Z}\}$

2) $a^i=a^j\Longleftrightarrow e=a^{j-i}\Longleftrightarrow m\mid j-i\Longleftrightarrow i\equiv j\ (\mathrm{mod}\ m)$

3) 设 $j\in\mathbb{Z}$ $j=qm+r$. $0\leq r\leq m-1$. 则有 $a^j=a^{qm+r}=a^r\in\{a^i \mid i=0,\dots,m-1\}$. 故 $\langle a\rangle\subseteq\{a^i \mid i=0,\dots,m-1\}$

设 $i,j\in\{0,\dots,m-1\}$, $a^i=a^j$. 则由 2) 有 $i\equiv j\ (\mathrm{mod}\ m)$. 又 $i,j\in\{0,\dots,m-1\}$，则 $i=j$.

即 a^i, $i=0,\dots,m-1$ "互不相同".

可以看到上述结论与初等数论中的"阶"的相关结论完全一致.

这是可以理解的，毕竟本质上都是循环群的结构.

接下来引入循环群的概念

Def. 对群 $(G;\cdot)$，若 $\exists a\in G$，使 $\langle a\rangle=G$. 则称 G 为循环群.

为了更严格地描述对上述"结构相同"的观察，引入：

Def. 对 $(G;*)$, $(H;\circ)$, $*$, $\circ$ 分别是 G、H 上的二元运算，映射 $f:G\to H$.

若 $\forall a,b\in G$，有 $f(a*b)=f(a)\circ f(b)$，则称 f 是 $(G;*)$ 到 $(H;\circ)$ 的同态.

若 $f:G\to H$ 为同态且为双射，则称 f 为同构.

例子：

(1) $(\{1,-1\},\cdot)$, $(\{0,1\},+(\mathrm{mod}\ 2))$

$1\cdot1=1$ $0+0=0$

$1\cdot(-1)=-1$ $0+1=1$ 定义 f：$f(0)=1$, $f(1)=-1$

$(-1)\cdot1=-1$ $1+0=1$ 可以验证 f 为同构.

$(-1)\cdot(-1)=1$ $1+1=0$

(2) $(\mathbb{R};+)$, $(\mathbb{R}^+;\cdot)$

定义 $f:\mathbb{R}\to\mathbb{R}^+$. $f(x)=2^x$. $(\mathbb{R};+)\to(\mathbb{R}^+;\cdot)$

$\forall x,y\in\mathbb{R}$，有 $f(x+y)=2^{x+y}=2^x\cdot2^y=f(x)\cdot f(y)$

又显然 f 为双射. 故 f 为同构.

(3) $f:(\mathbb{R};+)\to(\{z\in\mathbb{C} \mid |z|=1\};\cdot)$

$f(x):=e^{ix}$ 则有 $f(x+y)=e^{i(x+y)}=e^{ix}\cdot e^{iy}$

那么 f 为同态. 但 f 并非同构

但如果将 $(\mathbb{R};+)$ 改为 $([0,2\pi);+)$，则成为同构.

(4) $f:\mathbb{C}\to M_{2\times2}(\mathbb{R})$

$f(a+bi)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$

$\forall\alpha,\beta\in\mathbb{C}$. 有 $f(\alpha+\beta)=f(\alpha)+f(\beta)$

$f(\alpha\beta)=f(\alpha)f(\beta)$

设 $\alpha=a+bi$ $\beta=c+di$

则 $\alpha\beta=(ac-bd)+(ad+bc)i$

$f(\alpha)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$ $f(\beta)=\begin{pmatrix}c&d\\-d&c\end{pmatrix}$

则有 $f(\alpha)f(\beta)=\begin{pmatrix}ac-bd&ad+bc\\-bc-ad&-bd+ac\end{pmatrix}=f(\alpha\beta)$