在群论中，有一种特殊且重要的子群，谓之正规子群，
有了正规子群的概念，我们可以定义商群，
从而得到群同态基本定理及群同构定理，
在环论中，有与正规子群相平行的概念，谓之理想，
通过理想，我们可以定义商环，从而得到环同态基本定理，
在本节中，我们将给出理想和商环的定义，以及理想的初步性质，
并用理想的性质证明中国剩余定理，
环同态基本定理及环同构定理将在下一节给出，

定义 3.1 设{R;+,•}是环，I 是 R 的非空子集，
若 I 是{R;+}的子群，
且对属于 I 的任意 a，属于 R 的任意 r，有 ra 属于 I(或 ar 属于 I)，
则称 I 是 R 的左(或右)理想，
若 I 既是 R 的左理想又是 R 的右理想，则称 I 是 R 的双边理想，简称理想，
显然，在交换环中，每个左或右理想都是双边理想，
在有 1 的环 R 中，若 I 是 R 的理想，且 1 属于 I，则 I=R，
更一般地，若 a 属于 I，且 a 属于 U(R)，则 I=R，
对任意一个环 R，{0}和 R 都是 R 的理想，称这两个理想为 R 的平凡理想，
平凡理想之外的理想(如果存在的话)称为 R 的非平凡理想，
若 I 是环 R 的理想且 I≠R，则称 I 是环 R 的真理想，
不难看出，理想的定义又可以叙述为:
若 I 是环 R 的子环，且对属于 I 的任意 a，属于 R 的任意 r，
有 ra 属于 I，ar 属于 I
则 I 是 R 的理想，

关于理想，我们有下面的判别定理，

定理 3.1 设 I 是环 R 的非空子集，

则 I 是环 R 的理想的充分必要条件是下面两个条件成立:

(1)对属于 I 的任意 a，b，有 a−b 属于 I;

(2)对属于 I 的任意 a，和对属于 R 的任意 r，有 ar，ra 属于 I，

证: 必要性是显然的，下面证明充分性，

由条件(1)可知，I 是环{R;+}的子群，再由条件(2)可知，I 是环 R 的理想，

例 3.1 求整数环 Z 的所有理想，

解: 我们已经知道{Z;+}的所有子群为{⟨n⟩|n 是非负整数}，

另外，又易知⟨n⟩是 Z 的理想，所以 Z 的所有理想为{⟨n⟩|n 是非负整数}，

实际上，我们可以直接证明 Z 的理想形式为⟨n⟩，

令 I 是整数环 Z 的一个非零理想，

则存在不为 0 的属于 I 的 m，不妨假设 m＞0，进而考虑集合{m∈I|m＞0}，

显然，集合{m∈I|m＞0}是自然数的一个非空子集，

所以在集合{m∈I|m＞0}中存在一个最小的正整数 n，

下面我们证明 I=⟨n⟩，

因为对属于 I 的任意 x，有 x=nq+r，其中 0⩽r＜n，而且 x，nq 属于 I，

所以 r 属于 I，

但是，我们已假定 n 是 I 中最小的正整数，所以只能有 r=0，

于是 x=nq 属于⟨n⟩，即 I 包含于⟨n⟩，

而 n 属于 I，所以必有⟨n⟩包含于 I，

因而，I=⟨n⟩，

例 3.2 求剩余类环 Z_n 的所有理想，

解: 因为{Z_n;+}的所有子群为{⟨$\bar{s}$⟩|s 是 n 的正因数}，且容易验证⟨$\bar{s}$⟩是 Z_n 的理想，

所以 Z_n 的所有理想为{⟨$\bar{s}$⟩|s 是 n 的正因数}，

例 3.3 证明在除环中只有平凡理想，

证: 若 I 是除环 R 的非零理想，属于 I 的 a 不等于 0，

则属于 I 的 aa^{-1} 等于 1，从而 I=R，

一般地，称只有平凡理想的环为单纯环，显然，除环和域都是单纯环，

定义 3.2 设 R 是环，$S_1, S_2, \cdots, S_n$ 是 R 的非空子集，

称 $S_1+S_2+\cdots+S_n=\{s_1+s_2+\cdots+s_n \mid s_i \in S_i, i=1, 2, \cdots, n\}$ 是 $S_1, S_2, \cdots, S_n$ 的和，

称 $S_1S_2\cdots S_n = \left\{ \sum_{i=1}^{m} s_{i_1}s_{i_2}\cdots s_{i_n} \middle| s_{i_j} \in S_j, m \in Z^+, j = 1,2,\cdots n \right\}$ 是 $S_1, S_2, \cdots, S_n$ 的积

设 $I_1, I_2, \cdots, I_n$ 是环 R 的理想，

则根据定理 3.1 可知，$I_1+I_2+\cdots+I_n$，和 $I_1I_2\cdots I_n$ 是环 R 的理想，

另外，环 R 的任意多个理想的交还是环 R 的理想，

由理想的定义，容易知道 $I_1I_2\cdots I_n$ 包含于 $I_1 \cap I_2 \cap \cdots \cap I_n$ 包含于 $I_1+I_2+\cdots+I_n$，

定义 3.3 设 S 是环 R 的非空子集，

称 R 的所有包含 S 的理想的交为 S 生成的理想，记为$\langle S \rangle$，

若环 R 的理想 $I=\langle S \rangle$，则称 S 是 I 的生成集，并称 S 中的元素是 I 的生成元，

特别地，由一个元素 a($S=\{a\}$)生成的理想称为主理想，记为$\langle a \rangle$，

显然，$\langle \{a_1, a_2, \cdots, a_n\} \rangle = \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_n \rangle$，

下面我们考察主理想中元素的形式 ，

定理 3.2 设 R 是环 ，$a\in R$，则有如下结论:

(1) $\langle a\rangle=\left\{\sum_{i=1}^{n}x_iay_i+xa+ay+ma\middle|x_i,y_i,x,y\in R,m\in Z,n\in Z^+\right\}$

(2)若 R 是有单位元的环, 则$\langle a\rangle=\left\{\sum_{i=1}^{n}x_iay_i\middle|x_i,y_i\in R,n\in Z^+\right\}$

(3)若 R 是交换环 ，则$\langle a\rangle=\{xa+ma|x\in R,m\in Z\}$;

(4)若 R 是有单位元的交换环 ，则$\langle a\rangle=\{ax|x\in R\}=aR$,

证: 在此我们仅证明(1)，

首先 ，根据定理 3.1，容易验证

$I=\left\{\sum_{i=1}^{n}x_iay_i+xa+ay+ma\middle|x_i,y_i,x,y\in R,m\in Z,n\in Z^+\right\}$是环 R 的理想

且$a\in I$，所以$\langle a\rangle$包含于 I，

其次, 包含 a 的任意理想 J 都包含$\sum_{i=1}^{n}x_iay_i,xa,ay,ma$, 即 I 包含于$\bigcap J=\langle a\rangle$

所以$\langle a\rangle=\left\{\sum_{i=1}^{n}x_iay_i+xa+ay+ma\middle|x_i,y_i,x,y\in R,m\in Z,n\in Z^+\right\}$

Z 和 Z_n 都是有 1 的交换环 ，

Z 的每个理想形式为$\langle n\rangle=\{nr|r\in Z\}=nZ$，

Z_n 的每个理想形式为$\langle\bar{s}\rangle=\{\bar{s}\,\bar{a}|\bar{a}\in Z_n\}=\bar{s}Z_n$，

也就是说 ，Z 和 Z_n 的每个理想都是主理想 ，

定义 3.4 称每个理想都是主理想的整环为主理想整环 ，

例如 ，整数环 Z 和剩余类环 Z_p(p 是素数)是主理想整环 ，

例 3.4 在整数环 Z 中 ，$\langle m\rangle+\langle n\rangle=\langle(m,n)\rangle$，$\langle m\rangle\langle n\rangle=\langle mn\rangle$，其中 m，n 属于 Z，$(m,n)$表示 m，n 的最大公因数 ，

证: 首先证$\langle m\rangle+\langle n\rangle=\langle(m,n)\rangle$，

因为对属于 Z 的任意 m，n，存在属于 Z 的 s，t，使得$(m,n)=ms+nt$，

所以(m,n)属于$\langle m\rangle+\langle n\rangle$，因此 ，$\langle(m,n)\rangle$包含于$\langle m\rangle+\langle n\rangle$，

另外 ，由于$(m,n)|m$，$(m,n)|n$，所以$\langle m\rangle$包含于$\langle(m,n)\rangle$且$\langle n\rangle$包含于$\langle(m,n)\rangle$，

从而$\langle m\rangle+\langle n\rangle$包含于$\langle(m,n)\rangle$，结论得证 ，

然后证$\langle m\rangle\langle n\rangle=\langle mn\rangle$，由下式即可得证

$$\langle m\rangle\langle n\rangle=\left\{\sum_{i=1}^{k}(ms_i)(nt_i)\,\middle|\,s_i,t_i\in Z,k\in Z^+\right\}=\{mns\mid s\in Z\}=\langle mn\rangle$$

例 3.5 求高斯整环 Z[i]的理想$\langle 1+i\rangle$，

解: 因为 Z[i]是有 1 的交换环 ，所以

$\langle 1+i\rangle$

$=(1+i)Z[i]$

$=\{(1+i)(a+bi)|a,b\in Z\}$

$=\{(a-b)+(a+b)i|a,b\in Z\}$，

设 $a-b=x$，则

$\langle 1+i\rangle$

$=\{x+(2b+x)i\mid x,b\in Z\}$

$=\{x+yi\mid x\equiv y(\mathrm{mod}\ 2)\}$，

下面，我们借助理想来构造商环，

设 R 是环，I 是环 R 的理想，则{I;+}是{R;+}的交换子群，

从而是正规子群，于是存在交换商群{R/I;+}，

R/I 上的加法运算为$(x+I)+(y+I)=(x+y)+I, x, y\in R$，

若在商群{R/I;+}上定义“乘法”运算$(x+I)\bullet(y+I)=xy+I, x, y\in R$，

则“•”确是 R/I 上的运算，

即{R/I;+,•}构成一个环，称其为环 R 关于理想 I 的商环，

事实上，

(1)若 $x_1+I=x_2+I, y_1+I=y_2+I$，则 x_1-x_2, y_1-y_2 属于 I，

所以 $x_1y_1-x_2y_2=x_1(y_1-y_2)+(x_1-x_2)y_2$ 属于 I，即 $x_1y_1+I=x_2y_2+I$，

因而“•"是 R/I 上的运算

(2)运算“•”满足结合律，即$[(x+I)\bullet(y+I)]\bullet(z+I)=(x+I)\bullet[(y+I)\bullet(z+I)]$，

(3)对属于 R 的任意 x, y, z，有

$[(x+I)+(y+I)]\bullet(z+I)$

$=(x+y)z+I$

$=(xz+I)+(yz+I)$

$=(x+I)\bullet(z+I)+(y+I)\bullet(z+I)$，

$(z+I)\bullet[(x+I)+(y+l)]$

$=z(x+y)+I$

$=(zx+I)+(zy+I)$

$=(z+I)\bullet(x+I)+(z+I)\bullet(y+I)$，

即运算“•”对“+”具有分配律，这就是说，{R/I;+,•}确是一个环，

注意，商环中的零元是 I, x+I 的负元是 −x+I，

特别地，若 R 是交换环，则 R 的商环也是交换环，

有时我们将商环 R/I 中的元素 x+I 记为$\overline{x}$，则$\overline{x}+\overline{y}=\overline{x+y}$，$\overline{x}\bullet\overline{y}=\overline{xy}$，

例 3.6 求商环 $Z_{12}/\langle\overline{3}\rangle$

解: 因为 Z_{12} 是有单位元的交换环 ，所以$\langle\overline{3}\rangle=\overline{3}Z_{12}=\{\overline{0}\ ,\ \overline{3}\ ,\ \overline{6}\ ,\ \overline{9}\}$，

$\langle\overline{3}\rangle$在 Z_{12} 中的(加法)左陪集有: $\overline{0}+\langle\overline{3}\rangle$，$\overline{1}+\langle\overline{3}\rangle$和$\overline{2}+\langle\overline{3}\rangle$，

因此 ，$Z_{12}/\langle\overline{3}\rangle=\{\overline{0}+\langle\overline{3}\rangle\ ,\ \overline{1}+\langle\overline{3}\rangle\ ,\ \overline{2}+\langle\overline{3}\rangle\}$，

例 3.7 求商环 $F[x]/\langle x\rangle$，其中 F[x]是数域 F 上的一元多项式环 ，

解: 因为 F[x]是有 1 的交换环 ，所以$\langle x\rangle=xF[x]$，

由带余除法可知 ，对属于 F[x]的任意 f(x)，

存在有属于 F[x]的 q(x)，和属于 F 的 r，使得 $f(x)=xq(x)+r$，

因为 x 属于$\langle x\rangle$，所以 $f(x)-r$ 属于$\langle x\rangle$，

因此 $F[x]/\langle x\rangle$

$=\{f(x)+\langle x\rangle|f(x)\in F[x]\}$

$=\{r+\langle x\rangle|r\in F\}$，

例 3.8 求商环 $Z[i]/\langle 1+i\rangle$，

解: 由例 3.5 知道 ，$\langle 1+i\rangle=\{x+yi|x\equiv y(\mathrm{mod}\ 2)|$，

令 a+bi 属于 Z[i]，则

(1)若 a，b 的奇偶性相同 ，则 a+bi 属于$\langle 1+i\rangle$，

即 $a+bi+\langle 1+i\rangle=0+\langle 1+i\rangle$，$\overline{a+bi}=\overline{0}$ ，

(2)若 a，b 的奇偶性不同 ，则 $a-1+bi$ 属于$\langle 1+i\rangle$，而 $a+bi=1+(a-1)+bi$，

所以 $a+bi+\langle 1+i\rangle=1+\langle 1+i\rangle$，即 $\overline{a+bi}=\overline{1}$ ，

综上 ，$Z[i]/\langle 1+i\rangle=\{\overline{0}\ ,\ \overline{1}\}$，

定义 3.5 令 R 是有 1 的交换环 ，I，J 是环 R 的理想 ，

如果 I+J=R，则称理想 I 和 J 互素 ，

定理 3.3(中国剩余定理)令 R 是有 1 的交换环 ，I_i 是环 R 的理想 ，

且两两互素$(I_i+I_j=R)$，其中$(1\leqslant i\leqslant n)$

则对于任意给定的属于 R 的元素 $x_i(1\leqslant i\leqslant n)$，存在有属于 R 的 x，使得

$$\begin{cases} x \equiv x_1 (\mathrm{mod}\ I_1) \\ x \equiv x_2 (\mathrm{mod}\ I_2) \\ \quad \cdots\cdots\cdots \\ x \equiv x_n (\mathrm{mod}\ I_n) \end{cases}$$

其中符号 $x=y(\mathrm{mod}\ I)$表示 $x-y$ 属于 I，

证: 对于不等于 1 的 i，由于 $I_1+I_i=R$，

所以存在有属于 I_1 的 a_i, 和属于 I_i 的 b，使得 $a_i+b_i=1$，其中 $2\leqslant i\leqslant n$

从而 $1=(a_2+b_2)\cdots(a_n+b_n)$属于$(I_1+I_2)\cdots(I_1+I_n)$包含于 $I_1+I_2I_3\cdots I_n$，

即 $I_1+I_2I_3\cdots I_n=R$，

因此 ，存在有属于 $I_2I_3\cdots I_n$ 的 y_1，和属于 I_1 的y_1' ，使得$y_1'+y_1=1$，即

$\begin{cases} y_1 \equiv 1 (\mathrm{mod}\ I_1) \\ y_1 \equiv 0 (\mathrm{mod}\ I_2I_3\cdots I_n) \end{cases}$，进而$\begin{cases} y_1 \equiv 1 (\mathrm{mod}\ I_1) \\ y_1 \equiv 0 (\mathrm{mod}\ I_i), i \neq 1 \end{cases}$

类似地 ，存在属于 R 的 y_j, $(j=2,\cdots,n)$使得 $\begin{cases} y_j \equiv 1 (\mathrm{mod}\ I_j) \\ y_j \equiv 0 (\mathrm{mod}\ I_i), i \neq j \end{cases}$

至此 ，令 $x=x_1y_1+x_2y_2+\cdots+x_ny_n$ 即可 ，

注意，中国剩余定理不仅给出同余式方程组解的存在性，

而且也给出了求解的一般方法，一般来说，同余式方程组的解不唯一，

下面是解决这类问题的一个思路，

给定同余式方程组

$$\begin{cases} x \equiv x_1 (\mathrm{mod}\ p_1) \\ x \equiv x_2 (\mathrm{mod}\ p_2) \\ \cdots\cdots\cdots\cdots \\ x \equiv x_n (\mathrm{mod}\ p_n) \end{cases}$$ 其中 $p_1, p_2, \cdots, p_n$ 是两两互素的整数，$x_1, x_2, \cdots, x_n$ 属于 Z，

我们已经知道，在整数环中，$x \equiv x_i (\mathrm{mod}\ p_i) \Leftrightarrow x \equiv x_i (\mathrm{mod}\ \langle p_i \rangle)$，

另外，因为 p_i 与 p_j 互素，所以 $\langle p_i \rangle + \langle p_j \rangle = \langle (p_i, p_j) \rangle = \langle 1 \rangle = Z$，

因而求解上面的同余式方程组等价于用中国剩余定理求解 $\begin{cases} x \equiv x_1 (\mathrm{mod}\ \langle p_1 \rangle) \\ x \equiv x_2 (\mathrm{mod}\ \langle p_2 \rangle) \\ \cdots\cdots\cdots\cdots \\ x \equiv x_n (\mathrm{mod}\ \langle p_n \rangle) \end{cases}$

又因为 $p_1, p_2, \cdots, p_n$ 是两两互素的整数，所以 p_i 与 $p_1 \cdots p_{i-1} p_{i+1} \cdots p_n$ 互素，

再由带余除法可求得 s_i, t_i，使得 $p_i s_i + p_1 \cdots p_{i-1} p_{i+1} \cdots p_n t_i = 1$，

取 $y = p_1 \cdots p_{i-1} p_{i+1} \cdots p_n t_i$，

则 $x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ 就是同余式方程组的一个解，

例 3.9 求同余式方程组$\begin{cases} x \equiv 1(\mathrm{mod}\ 2) \\ x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 4(\mathrm{mod}\ 7) \end{cases}$ 的一个解 ，

解: 由带余除法可知

$1=2\times(-10)+(3\times7)\times1$,

$1=3\times5+(2\times7)\times(-1)$,

$1=7\times1+(2\times3)\times(-1)$,

所以取

$y_1=3\times7\times1=21$,

$y_2=2\times7\times(-1)=-14$,

$y_3=2\times3\times(-1)=-6$,

从而 $x=1\times21+2\times(-14)+4\times(-6)=-31$,

若求同余式方程组的正整数解 ，则由 $1=2\times(-31)+(3\times7)\times3$,

可取 $y_1=3\times7\times3=63$,

从而 ,$x=1\times63+2\times(-14)+4\times(-6)=11$,