الفصل الرابع

الحلقات والحقول Rings and fields

1. الحلقة Ring

تعريف

لتكن A مجموعة مزودة بقانوني تشكيل داخليين هما $(+)$ و $(\times)$.

نقول أن $(A,+,\times)$ حلقة إذا وفقط إذا تحققت الشروط التالية:

1- البنية $(A,+)$ زمرة تبديلية.
2- القانون $(\times)$ تجميعي.

3- القانون $(\times)$ توزيعي على القانون $(+)$:

$$\forall (x,y,z)\in A^3;\ x\times(y+z)=x\times y+x\times z$$
$$(x+y)\times z=x\times z+y\times z$$

4- يقبل القانون $(\times)$ عنصراً حيادياً نرمز له بـ 1 أي:

$$\forall x\in A;\ x\times 1=1\times x=x$$

في حالة كون القانون $(\times)$ تبديلي فإن البنية $(A,+,\times)$ تسمى حلقة تبديلية.

أمثلة

1- إن البنى التالية هي عبارة عن حلقات تبديلية:

$$(\mathbb{R},+,\times),\quad (\mathbb{Q},+,\times),\quad (\mathbb{Z},+,\times)$$

2- البنية $(\mathbb{Z}/n\mathbb{Z},+,\bullet)$ هي حلقة تبديلية حيث:

$$\forall k,k'\in\mathbb{Z}/n\mathbb{Z};\quad [k]+[k']=[k+k'],$$

$; \quad [k]\bullet[k']=[k\times k']$

2. الحساب في الحلقات

مبرهنة (1)

لتكن $(A,+,\times)$ حلقة، عندئذٍ الخواص التالية محققة:

1- $\forall x\in A;\quad x\times 0=0\times x=0$

2- $\forall x\in A;\quad (-1)\times x=-x$

3- $$\forall (x,y,z)\in A^3; (x-y)\times z=x\times y-y\times z \\ x\times(y-z)=x\times y-x\times z$$

الإثبات:

1- $\forall x\in A;\quad x+0=x\Rightarrow x\times(x+0)=x\times x+x\times 0=x\times x$

وبالتالي $x\times 0=0$ وبالشكل نفسه نجد أن $0\times x=0$.

2- $\forall x\in A;\quad (-1)\times x+x=\left((-1)+1\right)\times x=0\times x=0$

وبالتالي $(-1)\times x$ هو نظير x بالنسبة للقانون $(+)$ إذن: $(-1)\times x=-x$

-3

$$\begin{aligned}\forall (x,y,z)\in A^3;\quad x\times(y-z)&=x\times\left(y+(-1)\times z\right)\\&=x\times y+x\times\left((-1)\times z\right)\\&=x\times y+\left(x\times(-1)\right)\times z && \text{لأن × تجميعي}\\&=x\times y+(-x)\times z\\&=x\times y+\left(-(x\times z)\right)\\&=x\times y-x\times z\end{aligned}$$

لاحظ أن

$$\begin{aligned}x\times(-1)+x&=x\times\left((-1)+1\right)\\&=x\times 0=0\Rightarrow x\times(-1)=-x\end{aligned}$$

وكذلك $0 = 0\times z = \left((-x)+x\right)\times z = (-x)\times z + x\times z$ إذن $(-x)\times z$ هو نظير $x\times z$ أي أن $(-x)\times z = -(x\times z)$

ملاحظة:

لاحظ أنه إذا كانت $(A,+,\times)$ حلقة فإن البنية $(A,\times)$ ليست بالضرورة زمرة وكمثال على ذلك الحلقة $(\mathbb{Z},+,\times)$.

3. الحلقات التامة (Entire Ring)

تعريف

لتكن $(A,+,\times)$ حلقة. نقول عن العنصر $x\in A$ أنه قاسم للصفر إذا تحقق الشرطان:

i. $x\neq 0$

ii. يوجد $y\in A$ بحيث $y\neq 0$ و $(x\times y = 0\, or\ y\times x = 0)$.

تعريف

نقول عن الحلقة $(A,+,\times)$ أنها تامة إذا تحقق ما يلي:

1- $A\neq\{0\}$

2- $(\times)$ تبديلي.

3- الحلقة A لا تحوي قواسم للصفر أي $\forall(x,y)\in A^2, x\times y = 0 \Rightarrow x = 0 \quad or \quad y = 0$

ملاحظة هامة

في الحلقات التامة يمكننا الاختصار على العناصر غير المعدومة أي أن

$$\forall \quad (x,y,z)\in A^3;\quad (z\neq 0)\wedge(x\times z = y\times z)\Rightarrow x = y$$

حسب المبرهنة السابقة فإن: $x\times z = y\times z \Rightarrow (x-y)\times z = 0$

وبما أن $z\neq 0$ و A حلقة تامة أي لا تحوي قواسم للصفر فإن $x-y=0$ ومنه $x=y$

بعض الرموز والمصطلحات

لتكن لدينا الحلقة $(A,+,\times)$ وليكن $a\in A$ عنصراً من A و$n\in\mathbb{N}$ فإننا نستخدم الرموز التالية:

$$1-\ na=\begin{cases}\underbrace{a+a+\ldots+a}_{n-times} & if\ \ n\neq 0\\ 0 & if\ \ n=0\end{cases}$$

$$2-\ (-n)a=n(-a)=(-a)+(-a)+\ldots+(-a)$$

$$3-\ a^{n}=\begin{cases}\underbrace{a\times\cdots\times a}_{n-times} & if\ \ n\neq 0\\ 1 & if\ \ n=0\end{cases}$$

إذا لم يكن للعنصر $a\in A$ نظيراً بالنسبة للقانون $(\times)$ فليس هناك أي معنى للكتابة a^{-n}.

أمثلة

1- الحلقات $(\mathbb{Z},+,\times),\ (\mathbb{Q},+,\times),\ (\mathbb{R},+,\times)$, هي حلقات تامة يمكن إثبات ذلك بسهولة.

2- $(\mathbb{Z}/n\mathbb{Z},+,\bullet)$ حلقة تامة $\Leftrightarrow n=0$ أو n عدد أولي.

ولإثبات ذلك نميز الحالات التالية:

- $n=0$ عندئذٍ $\mathbb{Z}/n\mathbb{Z}$ تشاكل تقابلياً $\mathbb{Z}$ وبالتالي $\mathbb{Z}/n\mathbb{Z}$ تامة.
- لنفرض أن n عدداً أولياً وليكن $[0]=[r].[s]$ فهذا يعني أن: $[0]=[rs]$ أي أن $rs\in n\mathbb{Z}$ أي يوجد $z\in\mathbb{Z}$ بحيث $r.s=nz$ أي أن n يقسم $r.s$ وبما أنه أولي فإن n إما أن يقسم r أي أن $[r]=[0]$ و إما n يقسم s وبالتالي $[s]=[0]$ وبالتالي نستنتج أن: $[r][s]=[0]\Rightarrow[r]=[0] or [s]=0$ إذن $\mathbb{Z}/n\mathbb{Z}$ حلقة تامة في حال n عدد أولي.
- إذا لم يكن n أولياً فإن $\exists a,b$ بحيث يكون $n=a.b$ وبما أن $[n]=[0]$ عندئذٍ $[0]=[a][b]$ وحيث $[a]\neq[0],\ \ [b]\neq[0],$ إذن $\mathbb{Z}/n\mathbb{Z}$ ليست تامة.

4. العناصر القلوبة في حلقة (Invertible elements)

تعريف

لتكن $(A,+,\times)$ حلقة، نقول عن العنصر $x\in A$ أنه عنصر قلوب إذا وجـد $x'\in A$ بحيـث يكون $x.x'=x'.x=1$. نرمز لمجموعة العناصر القلوبة في الحلقة A بـ $U(A)$.

1- خواص العناصر القلوبة

1- لتكن $(A,+,\times)$ حلقة فإن مجموعة العناصر القلوبة $U(A)$ هي زمـرة بالنـسبة للقـانون $(\times)$. يمكن التحقق من ذلك بسهولة.

مثال:

في الحلقة $(\mathbb{Z},+,\times)$ زمرة العناصر القلوبة هي المجموعة $U(\mathbb{Z})=\{-1,+1\}$

وفي الحلقة $(\mathbb{Q},+,\times)$ لكل عنصر $q\in\mathbb{Q}$ حيث $q\neq 0$ له مقلوب في إذن $U(\mathbb{Q})=\mathbb{Q}^*$.

2- إذا كانت A,B حلقتين ولنزود $A\times B$ بالقانونين:

$$(a,b)+(a',b')=(a+a',b+b')$$

$$(a,b)\bullet(a',b')=(a\times a',b\times b')$$

عندئذ $(A\times B,+,\bullet)$ حلقة وتقبل $(1_A,1_B)$ عنصراً حيادياً بالنسبة لـ $(\bullet)$

الإثبات سهل ويترك للطالب.

وكذلك يكون $U(A\times B)=U(A)\times U(B)$

$$\forall(x,y)\in U(A\times B)\Rightarrow\exists(x',y')\in A\times B;(x\times x',y\times y')=(1_A,1_B)$$

إذن $x\times x'=1_A$ و $y\times y'=1_B$ وبالتالي $y\in U(B),x\in U(A)$

ومنه $(x,y)\in U(A)\times U(B)\Leftarrow U(A\times B)\subset U(A)\times U(B)$

وبسهولة نجد أن $U(A)\times U(B)\subset U(A\times B)$.

2- ثنائي الحد نيوتن

مبرهنة (2)

لتكن $(A,+,\times)$ حلقة، ولنفرض أن $(a,b)\in A^2$ يحقق ما يلي: $a\times b=b\times a$

عندئذٍ $\forall\, n\in\mathbb{N};\quad (a+b)^n=\sum_{k=0}^{n}C_n^k a^k b^{n-k}$

وكذلك: $\forall\, n\geq 1;\quad (a^n-b^n)=(a-b)\left[\sum_{k=0}^{n-1}a^{n-1-k}b^k\right]$

الإثبات سهل باستخدام مبدأ التدريج على n.

5. المثاليات في حلقة تبديلية (Ideals)

تعريف

لتكن $(A,+,\times)$ حلقة تبديلية. وليكن $I\subseteq A$ جزءاً من A. نقول أن I هو مثالي فـي A إذا تحقق الشرطان:

1- $(I,+)$ زمرة جزئية من $(A,+)$.

2- $\forall\, x\in I$ و $\forall\, a\in A$ فإن $a\times x\in I$ أو $AI\subset I$ نقول أن الجزء I ماص.

نتيجة هامة

إذا كان I مثالياً في A حيث A حلقة تبديلية فإن: $(1_A\in I)\Leftrightarrow I=A$

وذلك لأن: $\forall\, a\in A; a=a\times 1\in I$ إذن $A\subset I$ ومنه $A=I$.

ملاحظة

إن جميع المثاليات في حلقة الأعداد الصحيحة $(\mathbb{Z},+,\times)$ هي من النمط $n\mathbb{Z}$.

الإثبات موجود ضمن التمارين.

تعريف المثال الرئيسي (Principal ideal)

لتكن $(A,+,\times)$ حلقة تبديلية. نقول عن $I \subset A$ أنه مثال رئيسي إذا وفقط إذا وجـد عنـصر $a \in A$ بحيث يكون $I = aA$ أي أن $I = \{a \times b;\ \ b \in A\}$ ونقول أن aA هو المثالي المولـد بالعنصر a.

تعريف الحلقة الرئيسية (Principal Ring)

نقول عن $(A,+,\times)$ أنها حلقة رئيسية إذا تحقق الشرطان:

1- A حلقة تامة.

2- كل مثالي في A مثالي رئيسي.

مثال

حلقة الأعداد الصحيحة $(\mathbb{Z},+,\times)$ هي حلقة رئيسية لأنها حلقة تامة وكذلك كل مثالي مـن $\mathbb{Z}$ هو من النمط $n\mathbb{Z}$ حيث $n \in \mathbb{N}$ إذن يوجد $a = n \in \mathbb{Z}$ بحيث أن $n\mathbb{Z} = a.\mathbb{Z}$.

مبرهنة (3)

لتكن $(A,+,\times)$ حلقة تبديلية، ولتكن $I_1, I_2, \ldots, I_m$ مثاليات في A، إذن كل من:

$$K = \sum_{k=1}^{m} I_k = \{a_1 + \cdots + a_m, a_i \in I_i\}, \quad J = \bigcap_{k=1}^{n} I_k$$

هي مثالي في A.

6. التشاكلات الحلقية (Morphisms of Rings)

تعريف

لتكن $(A,+,\times)$ و $(B,+,\times)$ حلقتين، وليكن $f:A\to B$

نقول أن f تشاكل حلقي من A إلى B إذا تحققت الشروط التالية:

1- $f(1_A)=1_B$.

2- $\forall(x,y)\in A^2;\quad f(x+y)=f(x)+f(y)$

3- $\forall(x,y)\in A^2;\quad f(x\times y)=f(x)\times f(y)$

ونقول عن f أنه تشاكل حلقي تقابلي إذا كان تقابلاً.

مبرهنة (4)

لتكن $(A,+,\times)$ و $(B,+,\times)$ حلقتين تبديليتين. وليكن $f:A\to B$ تشاكلاً حلقياً. إن الصورة العكسية لأي مثالي I من B هي مثالي في A. وبشكل خاص لدينا $f^{-1}(\{0\})=\ker f$ مثالي في A. وتتحقق المساواة $\ker f=\{0\}$ إذا وفقط إذا كان f متبايناً.

الإثبات: يتم مباشرة باستخدام التعاريف.

7. تطبيق (حلقة الأعداد الصحيحة)

1- القسمة التقليدية في $\mathbb{Z}$ (Euclidean division)

مبرهنة (5)

ليكن $(a,b)\in\mathbb{Z}\times\mathbb{N}$ حيث $b\neq 0$. عندئذ $\exists!(q,r)\in\mathbb{Z}^2$ يحقق $a=bq+r$ حيث $0\leq|r|<b$.

نقول أن q هو حاصر القسمة و r هو باقي القسمة الأقليدية لـ a على b .

الإثبات:

بملاحظة أن $\mathbb{Z}|b\mathbb{Z}$ هي زمرة خارج القسمة وإن كل عنصر من هذه الزمرة يكتب بالشكل التالي: $\forall\quad [r]\in\mathbb{Z}|b\mathbb{Z};\ [r]=r+b\mathbb{Z};\quad |r|<b$ إذن من أجل أي عنصر فإن

$\exists q\in\mathbb{Z};\quad a=r+bq$

تعريف قابلية القسمة (Divisibility)

ليكن $(a,b)\in\mathbb{Z}^2$ عددين صحيحين. نقول أن العدد الصحيح a يقسم العدد الصحيح b إذا وفقط إذا تحقق الشرط التالي: $\exists k\in\mathbb{Z};\quad b=k\times a$ ونرمز لذلك بـ $a|b$ أي أن:

$$a|b\Leftrightarrow\exists k\in\mathbb{Z};\quad n=k\times a$$

ملاحظات

1- $\forall n\in\mathbb{N};\quad n|0$; لأن $0=0.n$، إذن n عدد طبيعي يقسم الصفر.

2- $\forall n\in\mathbb{N};\ 0|n\Rightarrow n=0$ لأن $\forall n\in\mathbb{N};\quad 0|n\Rightarrow n=k\times 0=0$

3- $\forall(a,b,c,d)\in\mathbb{Z}^4;\begin{cases}a|b\\ c|d\end{cases}\Rightarrow ac\,|\,bd$

$\exists k_1\in Z;\quad b=k\times a\Leftarrow a|b$ و $\exists k_1\in Z;d=l\times d\Leftarrow c|d$ وبالتالي
$b\times d=k_1\times a\times k_2\times c=k_1\times k_2\times a\times c$ أي يوجد $k=k_1\times k_2\in\mathbb{Z}$ حيث $b\times d=k\times a\times c$.

مبرهنة (6)

إذا كان $(a,b)\in Z^2$ عندئذٍ $a|b\Leftrightarrow(b\in a\mathbb{Z})\Leftrightarrow b\mathbb{Z}\subset a\mathbb{Z}$.

تعريف التطابق (Congruency)

ليكن لدينا العدد الطبيعي $0<n$ وليكن $(a,b)\in\mathbb{Z}^2$. نقول أن a متطابق أو منسجم مع b وفق n إذا كان n يقسم العدد الصحيح $(b-a)$ ونكتب $a\equiv b\ med(n)$ أي أن:

$$a\equiv b\ \mathrm{mod}(n)\Leftrightarrow n\,|\,(b-a)\Leftrightarrow\exists k\in\mathbb{Z};b-a=k\times n\Leftrightarrow b=a+k\times n$$

مبرهنة (7)

ليكن $0<n$ عدد طبيعي و $(a,b)\in\mathbb{Z}^2$ عندئذٍ: $a\equiv b\ \mathrm{mod}(n)\Leftrightarrow r_a=r_b$ حيث r_a يمثل باقي قسمة a على n و r_b يمثل باقي قسمة b على n.

مبرهنة (8)

ليكن $n\in\mathbb{N}^*$. إن العلاقة $\equiv$ المعرفة على $\mathbb{Z}$ بالشكل التالي:
$\forall(a,b)\in\mathbb{Z}^2;a\equiv b\Leftrightarrow a\equiv b\ \mathrm{mod}(n)$ هي علاقة تكافؤ.

مبرهنة (9)

ليكن $(a,b,c,d)\in\mathbb{Z}^4$, $n\in\mathbb{N}^*$ و ولنفرض أن: $a\equiv b\mathrm{mod}(n)$ و $c\equiv d\bmod(n)$

عندئذٍ:

1- $a+c=(b+d)\bmod(n)$

2- $a.c=(b.d)\bmod(n)$

3- $\forall k\in\mathbb{N}, a^k\equiv b^k\mathrm{mod}(n)$

ملاحظة:

إذا كان $n\in\mathbb{N}^*$ فإن $\mathbb{Z}|n\mathbb{Z}=\{[0],[1],\ldots,[n-1]\}$

إن عناصر المجموعة $\mathbb{Z}|n\mathbb{Z}$ تمثل صفوف تكافؤ العلاقة $\equiv$ وتمثل باقي القسمة الإقليدية لعناصر $\mathbb{Z}$ على العدد الطبيعي $0<n$.

مثال1:

أوجد باقي القسمة الأقليدية للعدد $a=126745$ على العدد $n=9$.

الحل:

إن $\mathbb{Z}|9\mathbb{Z}=\{[0],[1],\ldots,[8]\}$ إذن باقي قسمة a على n هو عنصر من المجموعة $\{0,1,2,\ldots,8\}$.

لاحظ أن العدد a لا يقبل القسمة المنتهية على 9. لكن $a-7=126738$ يقبل القسمة على 9 إذن يوجد $k\in\mathbb{Z}$ بحيث يكون $126745-7=9k$ وبالتالي $r_a=r_7$ حسب النظرية (7) $7=9\times0+7$ أي $\gamma_7=7$ وبالتالي $\gamma_a=7$.

مثال2:

أوجد باقي قسمة العدد $a=121^{1256}$ على 7.

الحل:

نطبق المبرهنة 9 أي r_a يساوي إلى r_{121}.

إن $\mathbb{Z}|7\mathbb{Z}=\{[0],[1],\ldots,[6]\}$: وبالتالي $r_a\in\{0,1,2,\ldots,6\}$

نلاحـظ أن $121-2=119=7k$ أي أن $2\equiv 121 \bmod (7)$. إذن بـاقي القـسمة هـو 2 لأن $2=7.0+2$

مثال3:

أوجد العدد الصحيح $x\in\mathbb{Z}$ بحيث يقبل x^2-4x+3 القسمة على 6.

الحل:

يجب أن يكون: $x^2-4x+3=6k$ حيث $k\in\mathbb{Z}$ أي أن $(x-1)(x-3)=6k$

وبالتالي 6 يقسم $(x-3)$ أو يقسم $(x-1)$ أي أن $x=6k_1+1$ أو $x=6k_2+3$

مثلاً من أجل $k_1=2$ ومن أجل $x=13$ نجد أن $(x-1)(x-3)=12\times 10=120=6\times 20$

ومن أجل $k_2=2$ ومن أجل $x=15$ نجد أن $(x-1)(x-3)=14\times 12=6\times 28$.

2- القاسم المشترك الأعظمي والمضاعف المشترك الأصغري

(Greatest Common Divisor and Least Common Multiple)

(GCD and LCM)

تعريف

ليكن $(a,b)\in\mathbb{Z}^2$ عندئذٍ:

1- إن مجموعة القواسم المشتركة للعددين الصحيحين $(a,b)\in\mathbb{Z}^2$ والمحتواة في $\mathbb{N}^*$ تحوي أكبر عنصراً ونرمز له بـ $\delta=\gcd(a,b)$ ونسميه القاسم المشترك الأعظمي لـ (a,b).

2- مجموعة المضاعفات المشتركة للعددين $(a,b)\in\mathbb{Z}^2$ والمحتواة في $\mathbb{N}^*$ تحوي اصغر عنصر نرمز له بـ $\mu=LCM(a,b)$ وندعوه المضاعف المشترك الأصغر لـ (a,b).

مبرهنة (10)

ليكن $(a,b)\in\mathbb{Z}^{*2}$ حيث $\delta=\gcd(a,b)$ و $\mu=lcm(a,b)$ عندئذٍ:

$$\mu\mathbb{Z}=a\mathbb{Z}\cap b\mathbb{Z} \text{ و } \delta\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}=\{au+bv\,;\,(u,v)\in\mathbb{Z}^2\}$$

مبرهنة (11)

ليكن $(a,b)\in Z^{*2}$. أثبت ما يلي من أجل أي عدد صحيح $k\in Z^{*}$ فإن:

$$lcm\,(am,kb)=k\ lcm\,(a,b) \ \text{و}\ \gcd(ka,kb)=k\gcd(a,b)$$

الحل:

لنفرض أن $\delta`=\gcd(ka,kb)$ فإن

$$\begin{aligned}\delta`\mathbb{Z}&=(ka)\mathbb{Z}+(kb)\mathbb{Z}=\left\{(ka)u+(kb)v\,;\quad (u,v)\in\mathbb{Z}^2\right\}\\&=\left\{k\,(au)+k\,(bv);\quad (u,v)\in\mathbb{Z}^2\right\}\\&=k\,\left\{au+bv\,;\quad (u,v)\in\mathbb{Z}^2\right\}\\&=k\,\delta\mathbb{Z}\end{aligned}$$

حيث $\delta=\gcd(a,b)$ and $\delta\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$ إذن $\delta`=k\,\delta$

مبرهنة إقليدس (12)

ليكن $(a,b)\in Z^{*2}$ عندئذٍ إذا تحقق الشرط التالي $\begin{cases}a=bq+r,\\ 0\le r<|b|\end{cases}$ $\exists!(a,r)\in N^{\,2};$

فإن: $\gcd(a,b)=\gcd(b,r)$

ملاحظة

إن مبرهنة إقليدس تمكننا من إيجاد خوارزمية إقليدس لحساب القاسم المشترك للعددين $(a,b)\in\mathbb{N}^{*2}$ حيث $0<a<b$ وذلك دون الإخلال بعمومية المسألة لأن:

$$\gcd(a,b)=\gcd\left(|a|,|b|\right)=\gcd\left(|b|,|a|\right)$$

3- خوارزمية إقليدس (Euclidean Algorithm)

نعرف المتتالية $(r_k)_{k\ge 0}$ تدريجياً كما يلي:

نضع $r_0=a$ و $r_1=b$ ومن ثم نعرف r_{k+1} على أنه باقي قسمة r_{k-1} على $r_k\neq 0$ أي بالاعتماد على مبرهنة إقليدس:

$$\exists!(q_k,r_{k+1})\in\mathbb{Z}^2;\quad r_{k-1}=q_k r_k+r_{k+1};\quad 0\le r_{k+1}<r_k$$

إن السلسلة $(r_k)_{k\ge0}$ متناقصة تماماً. عندئذ يوجد رتبة $n\ge1$ بحيث يكون $r_n\neq0$ ولكن $r_{n+1}=0$. إذن حسب نظرية إقليدس فإن $\gcd(a,b)=\gcd(r_k,r_{k+1})$ $\forall\,k\in N_{n-1},$

بما أن r_n تقسم r_{n-1} فإن $\gcd(r_n,r_{n-1})=r_n$ وبالتالي r_n هو $\gcd(a,b)$ ونمثل ذلك بالجـدول التالي:

k	1	2	$\dots$	$n-1$	n
r_{k-1}	a	b	$\dots$	r_{n-2}	r_{n-1}
r_k	b	r_2	$\dots$	r_{n-1}	$\boxed{r_n=d}$
r_{k+1}	r_2	r_3	$\dots$	r_n	0

مثال

أوجد القاسم المشترك للعددين $b=2047$ و $a=5313$.

k	1	2	3	4	5	6
r_{k-1}	5313	2047	1219	828	391	46
r_k	2047	1219	828	391	46	$\boxed{23}$
r_{k+1}	1219	828	391	46	23	0

نلاحظ أن عندما $k=1$ فإن $r_0=5313$ و $r_1=2047$

و$r_2=2047\times 2+1219$ أي أن 1216 هو باقي قسمة r_0 علـى r_1 و نتـابع لنحـصل علـى $d=\gcd(5313,2047)=23$.

4- الأعداد الأولية (Prime numbers)

ليكن $n\in\mathbb{N}^*$ عدد طبيعي غير معدوم وليكن $(x_1,x_2,\dots,x_n)\in\mathbb{Z}^{*n}$ عندئذٍ:

- نقول أن الأعداد الصحيحة $(x_1,x_2,\dots,x_n)$ أولية فيما بينها إذا وفقط إذا كان $\gcd(x_1,x_2,\dots,x_n)=1$.
- نقول أن الأعداد الصحيحة أولية فيما بينها مثنى مثنى إذا وفقط إذا كان:

$$\forall\,(i.j)\in\mathbb{N}_n^2;\quad i\neq j\Rightarrow \gcd(x_i,x_j)=1$$

ملاحظة

نقوم بتعميم تعريف القاسم المشترك الأكبر والمضاعف المشترك الأصغر كما يلي:

- نعرف $d=\gcd(x_1,\ldots,x_n)$ بأنه عنصر $d\in\mathbb{N}$ يحقق $d\mathbb{Z}=x_1\mathbb{Z}+x_2\mathbb{Z}+\cdots+\cdots x_n\mathbb{Z}$
- ونعرف $m=lcm(x_1,\cdots,x_n)$ بأنه العنصر $m\in\mathbb{N}$ يحقق $m\mathbb{Z}=\bigcap_{i=1}^{n}(x_i\mathbb{Z})$

ملاحظة

لاحظ أن الأعداد الصحيحة 3,6,7 أولية فيما بينها ولكنها ليست أولية فيما بينها مثنى مثنى لأن $3|6$.

إذن إذا كانت $(x_1,\ldots,x_n)$ أولية مثنى مثنى فإنها أولية فيما بينها ولكن العكس غير صحيح بالضرورة.

مبرهنة(13) بيزو(Bezout's theorem)

لتكن $(a,b)\in\mathbb{Z}^{*2}$. إن التكافؤ التالي محقق:

$$\gcd(a,b)=1\Leftrightarrow(\exists\,(u,v)\in Z^2;\,au+bv=1)$$

الإثبات:

إن الإثبات واضح باستخدام المبرهنة (10). إن $(\gcd(a,b))\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$ ولكن $\gcd(a,b)=1$ أي

$$\begin{aligned}\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}&\Leftrightarrow 1\in a\mathbb{Z}+b\mathbb{Z}\\&\Leftrightarrow\exists\,(u,v)\in Z^2;\quad au+bv=1\end{aligned}$$

استخدام خوارزمية إقليدس لإيجاد ثنائية بيزو:

ليكن لدينا العددين $(a,b)\in\mathbb{N}^{*2}$ الأوليين فيما بينهما. إن خوارزمية إقليدس تمكننا من إيجاد ثنائية بيزو $(u,v)\in\mathbb{Z}$ حيث $au+bv=1$ كما يلي:

نوجد المتتاليتين $(q_k)_{k\geq0}$, $(r_k)_{k\geq0}$ المعرفتين في خوارزمية إقليدس.

لاحظ أن $\gcd(a,b)=r_n=1$. نضع $(r_0=a)\wedge(r_1=b)$ ونعرف بالتدريج المتتالية $(r_k)_{k>0}$ كمايلي: $r_{k-1}=q_k r_k+r_{k+1}$ $\forall\ \ k\geq1;$ حيث $0<r_{k+1}\leq r_k$; ونعرف المتتاليتين $(u_k),(v_k)$ كما يلي: $r_k=u_k a+v_k b$ $\forall\ \ k\in\mathbb{N}_n,$

نثبت صحة هذه العلاقة بالتدريج حيث نضع $(u_0,v_0)=(1,0),(u_1,v_1)=(0,1)$ و بالتالي :

$$\forall k \in \mathbb{N}_n \setminus \{1\}; \quad \begin{cases} u_{k+1} = u_{k-1} - q_k u_k \\ v_{k+1} = v_{k-1} - q_q v_k \end{cases}$$

ونحصل على $1 = au_n + bv_n$. أي نحصل على الجدول التالي:

r_k	$r_0 = a$	$r_1 = b$	r_2	$\dots$	$r_n = 1$
q_k	-	q_1	q_2	$\dots$	q_n
u_k	1	0	u_2	$\dots$	$u_n = u$
v_k	0	1	v_2	$\dots$	$v_n = v$

مثال

حل المعادلة التالية: $22x + 7y = 1$

الحل:

نلاحظ أن 7 و 22 أوليان فيما بينهما إذن نبحث عن $(u,v) \in Z^*$ حيث:

$22u + 7v = 1$

بتطبيق خوارزمية إقليدس:

k	r_k	q_k	u_k	v_k
0	22	-	1	0
1	7	3	0	1
2	1	$q_2 = 7$	1	-3

لاحظ: $r_0 = a = 22$ وأن $r_1 = b = 7$ و $r_2 = 22 - 3 \times 7 = 1$ ومنه: $q_1 = 3$

$\frac{r_1}{r_2} = 7 \Rightarrow r_1 = 7r_2 + 0$ ومنه $q_2 = 7$.

إن $u_{k+1} = u_{k-1} - q_k u_k \Rightarrow u_2 = u_0 - q_1 u_1 = 1 - 7 \times 0 = 1$ وكذلك

$v_{k+1} = v_{k-1} - q_k v_k \Rightarrow v_2 = v_0 - q_1 v_1 = 0 - 3 \times 1 = -3$ أي أن $(u = 1) \wedge (v = -3)$.

تعريف

نقول العدد $n \in \mathbb{N}$ أنه أولياً في الحلقة $\mathbb{Z}$ إذا كان غير خزول في $\mathbb{Z}$ أي أن قواسم n هي 1 و n فقط. نرمز لمجموعة الأعداد الأولية بـ P .

خواص الأعداد الأولية

1- إذا كان p عدد أولياً و $n \in \mathbb{Z}$ فإما p يقسم n أو يكون $\gcd(n,p)=1$

2- إذا كان p عدداً أولياً و $(a,b)\in\mathbb{Z}^2$ فإن $P|ab \Rightarrow (P|a)\vee(P|b)$

3- إذا كانت p و $q_1,q_2,\dots,q_r$ أعداداً أولية وكان $p|q_1q_2\dots q_r$ عندئذٍ يوجد $k\in\mathbb{N}_r$ بحيث يكون $p=q_k$.

الإثبات:

1- إن العددين n,p إما أن يكونا أوليان فيما بينهما وبالتالي $\gcd(n,p)=1$ وإما أن يكونا غير أوليين وبالتالي ليكن $\delta=\gcd(n,p)$. بما أن p أولي أي غير خزول فإن $\delta=p$ ومنه $p|n$.

2- p أولي ولدينا $p|ab$ عندئذ (p يقسم a) أو (p يقسم b) وذلك باستخدام الخاصة الأولى كما يلي:

لنأخذ مثلاً p و a فإما p و a أوليان فيما بينهما أو أن $p|a$. إذا كان $p|a$ يكون تم المطلوب. أما إذا كان a,p أوليان و $p|ab$ فإن $p|b$ (أثبت ذلك).

3- يتم الإثبات بسهولة بالاعتماد على الخاصتين السابقتين.

مبرهنة (14)

ليكن $n\in\mathbb{N}\setminus\{0,1\}$. عندئذٍ n يكتب بشكل وحيد كما يلي:

$n=\prod_{p\in P} p^{v_p(n)}$ حيث $v_p(n)$ ونصطلح أن $v_p(n)=0$ عندما p عدد أولي و يقسم n .

ملاحظة

كل عدد $n\in\mathbb{Z}$ غير معدوم يكتب بشكل وحيد كما يلي: $n=\pm\prod_{p\in P} p^{v_p(n)}$

مثال $100=10.10$

$$=(2\times 5)\times(2\times 5)=2^2\times 5^2$$

إذن 100 كتب بشكل جداء بواسطة العددين الأوليين 2 and 5 .

مبرهنة (15)

أيا كان $(a,b)\in N^{*2}$ فعندئذٍ:

$$1-\ \gcd(a,b)=\prod_{p\in P} p^{\min(v_p(a),v_p(b))}$$

$$2-\ lcm\,(a,b)=\prod_{p\in P} p^{\max(v_p(a),v_p(b))}$$

مثال

أوجد القاسم المشترك الأكبر والمضاعف المشترك الأصغر للعددين:

$a=100$ و $b=73$

الحل:

نلاحظ أن $100=2^2.5^2=3^0.2^{2.}.5^2$ وأن $75=25.3=3.5^2=3.2^0.5^2$

ومنه:

$$\gcd(100,75)=\prod_{p\in P} p^{\min(v_p(a),v_p(b))}=5^2.2^0.3^0=25$$

$$lcd\,(100,75)=\prod_{p\in P} p^{\max(v_p(a),v_p(b))}=5^2.2^2.3=300$$

8. الحقول (Fields)

تعريف

لتكن $\mathbb{k}$ مجموعة مزودة بقانوني تشكيل داخليين (+) و($\times$) نقول أن البنية $(\mathbb{k},+,\times)$ هي حقل إذا وفقط إذا تحقق:

-1 $(\mathbb{k},+,\times)$ هي حلقة.

-2 كل عنصر غير معدوم من $\mathbb{k}$ له مقلوب في $\mathbb{k}$ بالنسبة للقانون $(\times)$ أي:

$(\forall x \in \mathbb{k};\quad x \neq 0) \Rightarrow x^{-1} \in \mathbb{k}$ أو بشكل آخر $\mathbb{k} \setminus \{0\} = U(\mathbb{k})$

إذا كان $(\times)$ تبديلي قلنا أن $\mathbb{k}$ حقل تبديلي $\Leftrightarrow U(\mathbb{k})$ زمرة تبديلية.

ملاحظة

إن $0 = 0_{\mathbb{k}}$ هو العنصر الحيادي بالنسبة للقانون (+) في $\mathbb{k}$.

مثال

إن البنى التالية $(\mathbb{C},+,\times),\quad (\mathbb{R},+,\times),\quad (\mathbb{Q},+,\times)$ هي حقول ولكن البنية $(\mathbb{Z},+,\times)$ ليست حقلاً لأن العناصر الوحيدة القابلة للقلب هي -1 و $+1$.

مبرهنة (16)

إن قانون الاختزال محقق في الحقل $(\mathbb{k},+,\times)$ أي أن:

$$\forall (a,x,y) \in \mathbb{k}^3, a \neq o_k,\quad a \times x = a \times y \Rightarrow x = y$$

الحقول الجزئية

ليكن $\mathbb{k}' \subset \mathbb{k}$ حيث $(\mathbb{k},+,\times)$ حقل. نقول أن $\mathbb{k}'$ حقل جزئي مـن $\mathbb{k}$ إذا وفقـط إذا تحققـت الشروط:

-1 $\mathbb{k}'$ هو حلقة جزئية من الحلقة $(\mathbb{k},+,\times)$.

-2 $\mathbb{k}' = U(\mathbb{k}')$

تشاكلات الحقول

ليكن $f:(\Bbbk,+,\times)\to(\Bbbk',+,\times)$ حيث $\Bbbk',\Bbbk$ حقلين. نقول عن f أنه تشاكل حقلي إذا وفقط إذا كان تشاكلاً حلقياً.

مبرهنة (17)

ليكن $k\in\Bbbk$ حيث $(\Bbbk,+,\times)$ حقل. عندئذٍ:

$$\sum_{i=0}^{n}k^{i}=1+k+k^{2}+\cdots+k^{n}=\begin{cases}(1-k)^{-1}(1-k^{n+1}); & k\neq 1\\ (n+1)1_{k}; & k=1\end{cases}$$

وحيث $1_{\Bbbk}$ هو الحيادي بالنسبة للقانون $(\times)$ في الحقل $\Bbbk$.

تمارين Exercises

التمرين الأول:

لتكن $(A,+,\times)$ حلقة تحقق الشرط التالي:

$$\forall x\in A;\quad x^{2}=x$$

1- أثبت أن: $\forall\quad (x,y)\in A^{2};\quad x\times y+y\times x=0$

2- أثبت أن: $\forall\quad x\in A;\quad 2x=0$

- بين أن A هي حلقة تبديلية.

الحل:

1- ليكن $(x,y)\in A^{2}$ فإن $x+y\in A$ لأن $(+)$ قانون تشكيل داخلي. حسب تعريف A فـإن $(x+y)^{2}=(x+y)$ وبالتالي:

$$x+y=(x+y)\times(x+y)$$

$$=(x+y)\times z+(x+y)\times y \qquad \text{حسب خاصة التوزيع}$$

$$=x\times x+y\times x+x\times y+y\times y \qquad (+)\ \text{تبديلي}$$

$$=x^{2}+xy+yx+y^{2}$$

وباستخدام تعريف A نجد أن $x+y=x+xy+yx+y$ و بالتالي $xy+yx=0$

2- $\forall x\in A$ فإن:

(حسب الطلب الأول) $2x=x+x=x\times 1_A+1_A\times x=0$

حيث $1_A\in A$ هو الحيادي بالنسبة للقانون $(\times)$.

3- من الطلب الثاني أن $\forall x\in A$ فإن $x=-x$

وبالتالي $xy=-xy$ باستخدام العلاقة

$$xy+yx=0\Rightarrow -xy+yx=0$$

ومنه $xy=yx$ أي أن القانون $(\times)$ تبديلي.

نسمي كل حلقة $(A,+,\times)$ حيث $\forall x\in A$ فإن $x^2=x$ بالحلقة البوليانية. أي الحلقة البوليانيـة هي حلقة تبديلية ونظير كل عنصر بالنسبة للقانون هي العنصر نفسه.

التمرين الثاني:

أثبت أنه إذا كانت E مجموعة ما فإن $(P(E),\Delta,\cap)$ هي حلقة بوليانية.

الحل:

إن $(P(E),\Delta)$ هي زمرة تبديلية. لأن Δ الفرق التناظري هو تجميعي وتبديلي (أثبت ذلـك) ومن ثم أن المجموعة $\varnothing$ تشكل العنصر الحيادي بالنسبة للقانون Δ لأن:

$$\forall A\in P(E);\quad A\Delta\varnothing=(A\setminus\varnothing)\cup(\varnothing\setminus A)=A\cup\varnothing=A$$

و $\varnothing\Delta A=(\varnothing\setminus A)\cup(A\setminus\varnothing)=\varnothing\cup A=A$

- نظير كل عنصر بالنسبة لـ Δ هو العنصر نفسه أي إذا كانت $A\in P(E)$ فإن:

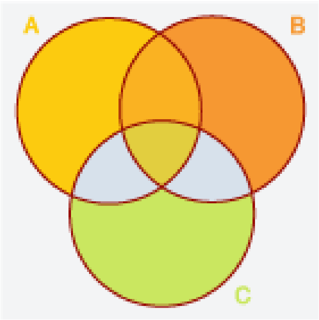
$$A\Delta A=(A\setminus A)\cup(A\setminus A)=\varnothing\cup\varnothing=\varnothing$$

- القانون $(\cap)$ هو تجميعي لأن عملية التقاطع عمليه تجميعية (أثبت ذلك)

- القانون $(\cap)$ توزيعي على (Δ) لأن:

$$
\begin{aligned}
A\cap(B\Delta C)&=A\cap[(B\setminus C)\cup(C\setminus B)]\\
&=A\cap[(B\cap\overline{C})\cup(C\cap\overline{B})]\\
&=[(A\cap B)\cap\overline{C})\cup[(A\cap C)\cap\overline{B}] && \text{حسب توزيع } \cap \text{ على } \cup\\
&=[(A\cap B)\setminus C]\cup[(A\cap C)\setminus B]\\
&=[(A\cap B)\setminus(A\cap C)]\cup[(A\cap C)\setminus(A\cap B)]\\
&=(A\cap B)\Delta(A\cap C)
\end{aligned}
$$

(انظر مخطط فن)



- $\forall A\in A$ فإن $A\cap A=A$
- إن الحيادي بالنسبة للتقاطع هو E لأن:

$$\forall \quad A\in P(E);\quad A\cap E=E\cap A=A$$

- التقاطع عملية تبديلية و بالتالي $(A,\Delta,\cap)$ هي حلقة بوليانية.

التمرين الثالث:

لتكن $A=\{a+b\sqrt{2};(a,b)\in\mathbb{Z}^2\}$ مزودة بجمع وضرب الأعداد الحقيقية:

1- بين أن A حلقة تامة.

2- إذا كان $x=a+b\sqrt{2}$ فإننا نعرف مرافق x ونرمز له بـ $\overline{x}$ بالشكل التالي
$\overline{x}=a-b\sqrt{2}$ و $R(x)=\dfrac{x+\overline{x}}{2}$ و $I(x)=\dfrac{x-\overline{x}}{2\sqrt{2}}$ وأخيرا $N(x)=x\times\overline{x}$

أثبت أن المقادير السابقة هي أعداد صحيحة $\forall x\in A$ وأن

$$\forall(x,y)\in A^2;\quad \overline{x\times y}=\overline{x}\times\overline{y},\quad N(x\times y)=N(x)N(y)$$

-3 أثبت أن $U(A)=\{x\in A: N(x)\in\{-1,+1\}\}$

-4 إذا كان $\omega=1+\sqrt{2}$ أثبت أن:

$$\forall\varepsilon\in\{-1,+1\},\quad \forall n\in\mathbb{Z};\varepsilon\omega^{2}\in U(A)$$

الحل:

1- $(A,+)$ هي زمرة تبديلية ونتحقق عن ذلك بسهولة.

- $\forall x,y\in A;\quad x=a+b\sqrt{2},\ y=a'+b'\sqrt{2}$

عندئذ $x+y=(a+a')+(b+b')\sqrt{2}=(a'+a)+(b'+b)\sqrt{2}$

- $\forall (x,y,z)\in A^{3};\quad x=a+b\sqrt{2}, y=a'+b'\sqrt{2}, z=a''+b''\sqrt{2}$

$$\begin{aligned}\Rightarrow (x+y)+z&=\left((a+a')+(b+b')\sqrt{2}\right)+a''+b''\sqrt{2}\\&=(a+a'+a'')+(b+b'+b'')\sqrt{2}\\&=a+b\sqrt{2}+(a'+a'')++(b'+b'')\sqrt{2}\\&=x+(y+z)\end{aligned}$$

- إن $0\in A$ لأن $0=0+0\sqrt{2}$ وكذلك $\forall x\in A; 0+x=0+0\sqrt{2}+a+b\sqrt{2}=x+0=x$
- $\forall x\in A;\quad -x=-a-b\sqrt{2}\Rightarrow x+(-x)=(-x)+x=0$

إذن $(A,+)$ زمرة تبديلية.

- القانون $(\times)$ هو تجميعي.

$$\forall\quad (x,y,z)\in A^{3};\quad (x\times y)\times z=\left((a+b\sqrt{2})\times(a'+b'\sqrt{2})\right)\times(a''+b''\sqrt{2})$$

$$=\left(aa'+(ab'+ba')\sqrt{2}+2bb'\right)\times(a''+b''\sqrt{2})$$

أثبت أن هذا المقدار يساوي $x\times(y\times z)$

- تحقق أن $(\times)$ توزيعي على الجمع..
- إن $1=1+0\sqrt{2}\in A$ و $\forall x\in A;\quad x-1=1-x=x$

إذن 1 هو الحيادي بالنسبة لـ A .

- الحلقة $(A,+,\times)$ تبديلية لأن $(\times)$ الضرب التبديلي.

$$\begin{aligned} x\times y &= aa'+(ab'+ba')\sqrt{2}+2bb' \\ &= a'a+(b'a+a'b)\sqrt{2}+2b'b \\ &= y\times x \end{aligned}$$

كذلك إذا كان $x\times y=0$ فإن $(a+b\sqrt{2})\times(a'+b'\sqrt{2})=0$

إذن إما $a'+b'\sqrt{2}=0$ أي $a'=b'=0$ أو $a+b\sqrt{2}=0$ أي $a=b=0$

إذن A حلقة تامة.

-2 $\forall x\in A;\quad x=a+b\sqrt{2}\Rightarrow R(x)=\dfrac{x+\overline{x}}{\sqrt{2}}=\dfrac{a+b\sqrt{2}+a-b\sqrt{2}}{2}=a\in\mathbb{Z}$

إذن $R(x)\in\mathbb{Z}$

وكذلك $I(x)=\dfrac{x-\overline{x}}{2\sqrt{2}}=\dfrac{a+b\sqrt{2}-a+b\sqrt{2}}{2\sqrt{2}}=\dfrac{2\sqrt{2}}{2\sqrt{2}}b=b\in\mathbb{Z}$ إذن $I(x)\in\mathbb{Z}$

$$N(x)=x\times\overline{x}=(a+b\sqrt{2})\times(a-b\sqrt{2})=a^2-ab\sqrt{2}+ab\sqrt{2}-2b^2=a^2-2b^2\in\mathbb{Z}$$

إذن $N(x)\in\mathbb{Z}$.

$$\begin{aligned} \forall(x,y)\in A^2\Rightarrow x\times y &= (a+b\sqrt{2})\times(a'+b'\sqrt{2}) \\ &= aa'+ab'\sqrt{2}+a'b\sqrt{2}+2bb' \\ &= aa'+2bb'+(ab'+a'b)\sqrt{2} \end{aligned}$$

لاحظ أن $x\times y\in A$ وبالتالي $\overline{x\times y}=aa'+2bb'-(ab'+a'b)\sqrt{2}$

$$\begin{aligned} \overline{x}\times\overline{y} &= (a-b\sqrt{2})(a'+b'\sqrt{2}) \\ &= aa`-ab`\sqrt{2}-ba`\sqrt{2}+2bb` \\ &= aa'+2bb'-(ab'+a'b)\sqrt{2} \\ &= \overline{x\times y} \end{aligned}$$

وكذلك $N(x\times y)=(x\times y)(\overline{x\times y})=(aa`+2bb`)^2-2(ab`+a`b)^2$. أثبت أن:

$$N(x)N(y)=(aa`+2bb`)^2-2(ab`+a`b)^2=N(x\times y)$$

-3 ليكن $0\neq x\in A$ فإن x يكون قلوباً إذا وجد $A\ni x'$ بحيث $x'\times x=x\times x'=1$ يكفي أن يكفي استخدام العلاقة $x'\times x=1$ لأن القانون $(\times)$ تبديلي:

إن $x'\times x=1\Rightarrow x'\times x\times\overline{x}=\overline{x}$ ومنه $x'\times N(x)=\overline{x}$

إذا كان $x=a+b\sqrt{2}$ فإن $x'=\frac{a-b\sqrt{2}}{N(x)}=\frac{\bar{x}}{N(x)}$ (تذكر أن $N(x)\in\mathbb{Z}$)

لاحظ أنه في حال $N(x)\notin\{-1,+1\}$ فإن $N(x')=\frac{1}{[N(x)]^2}\bar{x}.x=\frac{N(x)}{N^2(x)}=\frac{1}{N(x)}\notin\mathbb{Z}$

أي أن x' لا ينتمي إلى A إلا في حالة $N(x)\in\{-1,+1\}$ ونستنتج أن

$$U(A)=\{x\in A;N(x)\in\{-1,+1\}\}$$

4- $\omega=1+\sqrt{2}$ و $\varepsilon\in\{-1,+1\}$ إذن $\varepsilon\omega^n=\pm(1+\sqrt{2})^n=\pm\omega^n\in A$ (أثبت ذلك)

لاحظ أن $N(\omega)=1-2=-1$ وبالتالي $\omega\in U(A)$. تستطيع بالاعتماد على الطلب الثاني مـن هذا التمرين و باستخدام الخاصة $\forall(x,y)\in A^2;\ N(x\times y)=N(x)\times N(y)$ أن تثبـت أن $N(\omega^n)=(N(\omega))^n$ أي أن $N(\omega^n)=(-1)^n$ ومنه $N(\varepsilon\omega^n)=\pm N(\omega^n)=\pm(1)^n=\pm1$ أي أن $N(\varepsilon\omega^n)\in\{-1,+1\}$ وكذلك $\varepsilon\omega^n\in A$ إذن $\varepsilon\omega^n\in U(A)$.

التمرين الرابع:

إن جميع المثاليات في حلقة الأعداد الصحيحة $(\mathbb{Z},+,.)$ هي من النمط $n\mathbb{Z}$.

الحل:

لقد أثبتنا أن أي زمرة جزئية من $(\mathbb{Z},+,.)$ هي من النمط $n\mathbb{Z}$ لنثبت أن $\forall n\in\mathbb{N}$ فـإن $n\mathbb{Z}$ هي مثالي في $\mathbb{Z}$.

إن الشرط الأول محقق.

(•) تجميعي

$$\forall\quad x\in n\mathbb{Z};\quad \exists z\in\mathbb{Z};\quad x=nz$$

(•) داخلي

$$\Rightarrow\forall p\in\mathbb{Z};\quad p.x=x.p=(n.z).p=n(z.p)$$
$$=nq;\quad q=z.p\in\mathbb{Z}$$

$\mathbb{Z}$ حلقة تبديلية

إذن $\forall x\in n\mathbb{Z}\quad p\in\mathbb{Z};\quad p.x\in n\mathbb{Z}$ إذن $n\mathbb{Z}$ هي مثالي في $\mathbb{Z}$

التمرين الخامس:

لتكن H_1,H_2 زمرتين جزئيتين من الزمرة $(\mathbb{Z},+)$ ولنعرف:

$$H = H_1 + H_2 = \{h_1 , h_2 ; (h_1 \in H_1) \wedge (h_2 \in H_2)\}$$

1- أثبت أن H هي أصغر زمرة جزئية من $(\mathbb{Z},+)$ تحوي المجموعة الجزئية $H_1 \cup H_2$.

2- ما هو شكل المجموعة الجزئية $4\mathbb{Z}+6\mathbb{Z}$.

3- كيف تفسر الاحتواء $a\mathbb{Z}\cup b\mathbb{Z}\subset c\mathbb{Z}$ باستخدام قابلية القسمة؟

الحل:

1- إن 0 الذي هو الحيادي بالنسبة للجمع في $\mathbb{Z}$ وينتمي إلى كل من H_2 و H_1 إذن $0\in H$

ليكن $h_1,h_1'\in H_1$ و $h_2,h_2'\in H_2$ فإن $h_1-h_1'\in H_1,\ \ h_2-h_2'\in H_2$. حسب تعريف الزمـر الجزئية فإن $h_1+h_2-h_1'-h_2' = h_1-h_1'+h_2-h_2'\in H$ أي أن H زمرة جزئية.

لاحظ أن: $H_1\cup H_2\subset H$ لأن $\forall h\in H_1\cup H_2$ فإن $(h_1\in H)\vee(h\in H_2)$

إذن نستطيع أن نكتب h كما يلي $h=h+0=0+h$ أي $h\in H_1+H_2=H$

إذن H ينتمي إلى مجموعة الزمر الجزئية التي تحوي $H_1\cup H_2$. ولنرمز لهذه المجموعـة بـ $G=\left\{G_i\subset\mathbb{Z};\ H_1\cup H_2\in G_i , i\in I\right\}$

حسب المبرهنة (4) من الفصل الثالث فإن $\bigcap_{i\in I}G_i$ هي أصغر زمرة جزئية تحـوي $H_1\cup H_2$.

نلاحظ أن $H\in G$ وبالتالي $\bigcap_{i\in}G_i\subset H$ ولنثبت أن $H\subset\bigcap_{i\in I}G_i$.

حسب المبرهنة (5) من الفصل الثالث أيضاً نجد أن $\bigcap_{i\in I}G_i=<H_1\vee H_2>$

$$\Rightarrow \bigcap_{i\in I}G_i=\left\{g_1+g_2+\ldots+g_n;\quad \forall\ i\in\mathbb{N}_n ; g_i\in\left(H_1\cup H_2\right)\cup\left(H_1\cup H_2\right)^{-1}\right\}$$

نلاحظ أنه: $\forall\ h\in H$ فإن: $h=h_1+h_2$ حيث $\left(h_1,h_2\right)\in H_1\times H_2$

إن $h_1\in H_1\subset H_1\cup H_2$ و $h_2\in H_2\subset H_1\cup H_2$ إذن:

$$h_1+h_2\in(H_1\cup H_2)\cup(H_1\cup H_2)^{-1}\Rightarrow h\in\bigcap_{i\in I}G_i$$

و نستنتج أن $H_1+H_2=\bigcap_{i\in I}G_i$ أي H_1+H_2 هي أصغر زمرة جزئية مـن $(Z,+)$ تحـوي $H_1\cup H_2$.

2- نعلم أن أي مجموعة جزئية من $\mathbb{Z}$ هي من الشكل $n\mathbb{Z}$ حيث $n \in \mathbb{N}$ وبالتالي:

$$\begin{aligned}
4\mathbb{Z}+6\mathbb{Z} &= \{h_1+h_2;\quad (h_1,h_2)\in 4\mathbb{Z}\times 6\mathbb{Z}\}\\
&= \{4k+6l;\quad (k,l)\in \mathbb{Z}^2\}\\
&= \{4k+4l+2l;\quad (k,l)\in \mathbb{Z}^2\}\\
&= \{4(k+l)+2l;\quad (k,l)\in \mathbb{Z}^2\}\\
&= \{4m+2l;\quad (m,l)\in \mathbb{Z}^2\}\\
&= \{2.2m+2l;\quad (m,l)\in \mathbb{Z}^2\}\\
&= \{2p+2l;\quad (p,l)\in \mathbb{Z}^2\}\\
&= \{2(p+l);\quad p+l\in \mathbb{Z}\} = 2\mathbb{Z}
\end{aligned}$$

إذن: $4\mathbb{Z}+6\mathbb{Z}=2\mathbb{Z}$ لاحظ أن 2 هو القاسم المشترك الأكبر لـ $(4,6)$ أي $2=\gcd(4,6)$.

3- لاحظ أن القسم الأول من هذا التمرين يمكننا من الكتابة التالية:

$a\mathbb{Z}\cup b\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}$ إذاً إذا كانت $a\mathbb{Z}\cup b\mathbb{Z}\subset c\mathbb{Z}$ فإن $a\mathbb{Z}+b\mathbb{Z}\subseteq c\mathbb{Z}$ لأن $a\mathbb{Z}+b\mathbb{Z}$ هـي أصغر مجموعة جزئية تحوي $a\mathbb{Z}\cup b\mathbb{Z}$ أي يمكننـا أن نقـول أن c هـو قاسـم مـشترك لـ (a,b).

التمرين السادس:

ليكن $(a,b)\in \mathbb{Z}^{*2}$، أثبت ما يلي:

1- إذا كان $a\in\mathbb{Z}$ حيث $(d|a)\wedge(d|b)$ فإن $d|\gcd(a,b)$

2- إذا كان $m\in\mathbb{Z}$ حيث $(a|m)\wedge(b|m)$ فإن $lcm(a,b)\ |m$

الحل:

1- بما أن $(d|a)\wedge(d\ |b)$ فإن $(a\mathbb{Z}\subset d\mathbb{Z})\wedge(b\mathbb{Z}\subset d\mathbb{Z})$ أي أن $(a\mathbb{Z}\cup b\mathbb{Z})\subset d\mathbb{Z}$ ولكـن حسب التمرين السابق والمبرهنة 10 فإن $a\mathbb{Z}\cup b\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}=\delta\mathbb{Z}\subset d\mathbb{Z};\ \delta=\gcd(a,b)$

نستنتج باستخدام المبرهنة 6 من الفصل الثالث أن $d\ |\delta$.

2- ليكن $\mu=lcm(a,b)$ المضاعف المشترك الأصغر لـ b,a.

إذا كان $(a|m)\wedge(b|m)$ حيث $m\in\mathbb{Z}$ و حسب المبرهنة 6 من الفصل الثالث ينتج أن: $(m\mathbb{Z}\subset a\mathbb{Z})\wedge(m\mathbb{Z}\subset b\mathbb{Z})$ أي أن $m\mathbb{Z}\subset a\mathbb{Z}\cap b\mathbb{Z}$ أي $m\mathbb{Z}\subset \mu\mathbb{Z}$ وذلك حسب المبرهنة 10، إذن $\mu|m$.

التمرين السابع:

أوجدالقاسم المشترك الأصغر للعددين $(366,43)$

الحل:

k	1	2	3	4
r_{k-1}	366	43	22	21
r_k	43	22	21	$\boxed{1=d}$
r_{k+1}	22	21	1	0

إذاً $d=\gcd(366,43)$.

التمرين الثامن:

أوجد العددين الصحيحين x و y بحيث: $5313x+2047y=23$

الحل:

لقد وجدنا في مثال سابق إن $\gcd(a,b)=23$ حيث $a=5313$ و $b=2047$

عندئذٍ نحصل على الجدول التالي الذي يعطي قيمة y,x .

k	r_k	q_k	u_k	v_k
0	5313	-	1	0
1	2047	2	0	1
2	1219	1	1	-2
3	828	1	-1	3
4	391	2	2	-5
5	46	8	-5	13
6	23		42	-109
7	0			

فمثلاً: $u_2=u_0-q_1u_1=1-2\times0=1$ ومن ثم نوجد البقية بنفس الطريقة.

$v_2=v_0-q_1v_1=0-2\times1=-2$ ومنه: $x=u_6=42,\quad y=v_6=-109$.

9. الفضاءات الشعاعية والجبورعلى حقل

تعريف الفضاء الشعاعي (Vector space)

ليكن K حقلاً تبديلياً، تسمى فضاء شعاعي على الحقل K، كل بنية جبريـة $(E,+,.)$ تحقـق الشروط التالية:

- البنية $(E,+)$ زمرة تبديلية.
- القانون (.) هو قانون تشكيل خارجي على E مجموع مؤثراتـه الحقـل K ويحقـق الخواص التالية:

$$\forall a \in K,\ \forall (x,y) \in E^2;\ a(x+y) = ax + ay$$

$$\forall (a,b) \in K,\ \forall x \in E;\ \begin{cases}(a+b).x = a.x + b.x\\ (ab).x = a.(b.x)\end{cases}$$

$$\forall x \in E;\ 1_K.x = x$$

تعريف

ليكن K حقلاً تبديلياً. نُسمي جبراً على الحقل K . كل بنية جبرية $(E,+,\times,\bullet)$ تحقق الـشروط التالية:

البنية $(E,+,\bullet)$ فضاء شعاعي على الحقل K .

البنية $(E,+,\times)$ حلقة.

$$\forall a \in K, \forall (x,y) \in E^2;\ (a.x)\times y = a.(x\times y)$$