

Using *Mathematica* to Explore Abstract Algebra

Allen C. Hibbard
Central College

■ 4. An Overview of *AbstractAlgebra*

```
Needs["AbstractAlgebra`Master`"]
```

■ 4.1 Groupoids

```
G = FormGroupoid[{0, 2, 1, 4, 6}, Times, GroupoidName -> "ex. 1"]
```

```
Groupoid[{0, 2, 1, 4, 6}, -Operation-]
```

```
Elements[G]
```

```
Operation[G]
```

```
{0, 2, 1, 4, 6}
```

```
Times
```

```
HasIdentityQ[G]
```

```
True
```

```
HasIdentityQ[G, Mode -> Visual]
```

ex. 1 x * y

$\begin{array}{c c} & y \\ \hline x & \end{array}$	0	2	1	4	6
0	0	0	0	0	0
2	0	4	2	8	12
1	0	2	1	4	6
4	0	8	4	16	24
6	0	12	6	24	36

red: left ident.

ex. 1 x * y

$\begin{array}{c c} & y \\ \hline x & \end{array}$	0	2	1	4	6
0	0	0	0	0	0
2	0	4	2	8	12
1	0	2	1	4	6
4	0	8	4	16	24
6	0	12	6	24	36

red: right ident.

```
True
```

HasInversesQ[G, Mode → Textual]

Given a Groupoid G, we say an element g in G has an inverse h if G has an identity e and $g * h = h * g = e$ (where * indicates the operation).

The Groupoid ex.1 contains some elements without inverses. For example, 0 does NOT have an inverse.

False

ClosedQ[G, Mode → Visual]

All the elements marked with yellow are original elements in the set. Those in red are from outside.

ex. 1 x * y

y x	0	2	1	4	6
0	0	0	0	0	0
2	0	4	2	8	12
1	0	2	1	4	6
4	0	8	4	16	24
6	0	12	6	24	36

False

GroupQ[G]

False

CayleyTable[G, Mode → Visual]

For each element, a different color is used. The entries in the table corresponding to the elements are then colored and labeled accordingly.

ex. 1 x * y

y x	0	2	1	4	6
0	0	0	0	0	0
2	0	4	2	8	12
1	0	2	1	4	6
4	0	8	4	16	24
6	0	12	6	24	36

$\{\{0, 0, 0, 0, 0\}, \{0, 4, 2, 8, 12\}, \{0, 2, 1, 4, 6\}, \{0, 8, 4, 16, 24\}, \{0, 12, 6, 24, 36\}\}$

```
gr1 = RightCosets[Z[8], {0, 4}, Mode -> Visual, Output -> Graphics];
```

Z[8] x + y

x \ y	0	4	1	5	2	6	3	7
0	0	4	1	5	2	6	3	7
4	4	0	5	1	6	2	7	3
1	1	5	2	6	3	7	4	0
5	5	1	6	2	7	3	0	4
2	2	6	3	7	4	0	5	1
6	6	2	7	3	0	4	1	5
3	3	7	4	0	5	1	6	2
7	7	3	0	4	1	5	2	6

```
gr2 = CayleyTable[Z[4], Mode -> Visual, Output -> Graphics];
```

For each element, a different color is used. The entries in the table corresponding to the elements are then colored and labeled accordingly.

Z[4] x + y

x \ y	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

```
Show[GraphicsArray[{gr1, gr2}]];
```

z[8]		x + y						
x \ y	0	4	1	5	2	6	3	7
0	0	4	1	5	2	6	3	7
4	4	0	5	1	6	2	7	3
1	1	5	2	6	3	7	4	0
5	5	1	6	2	7	3	0	4
2	2	6	3	7	4	0	5	1
6	6	2	7	3	0	4	1	5
3	3	7	4	0	5	1	6	2
7	7	3	0	4	1	5	2	6

z[4]		x + y			
x \ y	0	1	2	3	
0	0	1	2	3	
1	1	2	3	0	
2	2	3	0	1	
3	3	0	1	2	

```
NormalQ[H = SubgroupGenerated[Symmetric[3], {3, 2, 1}], Symmetric[3]]
```

```
False
```

```
LeftCosets[Symmetric[3], H, Mode -> Visual];
```

```
KEY for S[3]: label used -> element: {g1 -> {3, 2, 1}, g2 ->
{1, 2, 3}, g3 -> {2, 3, 1}, g4 -> {1, 3, 2}, g5 -> {3, 1, 2}, g6 -> {2, 1, 3}}
```

S[3]		x * y					
x \ y	g1	g2	g3	g4	g5	g6	
g1	g1	g2	g3	g4	g5	g6	
g2	g2	g1	g3	g4	g5	g6	
g3	g3	g4	g3	g5	g6	g2	
g4	g4	g3	g4	g1	g2	g5	
g5	g5	g6	g5	g2	g1	g3	
g6	g6	g5	g6	g4	g3	g1	

■ 4.2 Ringoids

```
SwitchStructureTo[Ring]
```

```
Ring
```

```
R = FormRingoid[{0, 2, 1, 4, 6}, Plus, Times, FormatElements -> True, FormatOperator ->
False]
```

```
Ringoid[{-Elements-}, Plus, Times]
```

```
RingQ[R]
```

```
False
```

```
RandomElement[PolynomialsOver[BooleanRing[3]], 2, Monic -> True]
```

```
{ } + {1, 3} x + {1, 2, 3} x2
```

```
Unity[BooleanRing[3]]
```

```
{1, 2, 3}
```

```
RandomMatrix[LatticeRing[12], 3, MatrixType -> GL] // MatrixForm
```

$$\begin{pmatrix} 4 & 6 & 4 \\ 4 & 12 & 12 \\ 12 & 1 & 12 \end{pmatrix}$$

```
GF[9]
```

```
Ringoid[{0, x, 2 x, 1, 1 + x, 1 + 2 x, 2, 2 + x, 2 + 2 x}, -Addition-, -Multiplication-]
```

■ 4.3 Morphoids

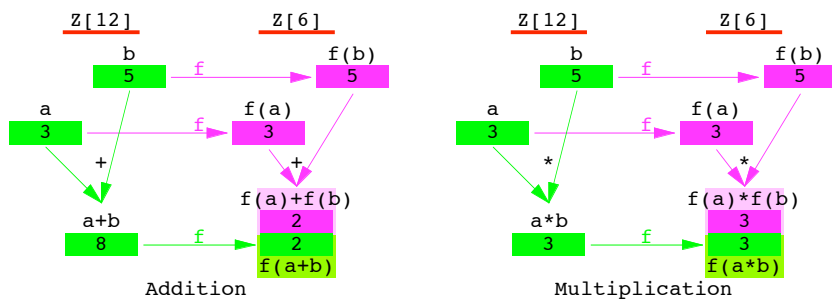
```
f = FormMorphoid[Mod[#, 6]&, Z[12], Z[6]]
```

```
Morphoid[Mod[#1, 6] &, -Z[12]-, -Z[6]-]
```

```
MorphismQ[f]
```

```
True
```

```
PreservesQ[f, {3, 5}, Mode -> Visual]
```



```
True
```

```
SwitchStructureTo[Group];
```

```
FormMorphoid[Mod[#, 6]&, Z[12], Z[6]]
```

```
Morphoid[Mod[#1, 6] &, -Z[12]-, -Z[6]-]
```

```
FormMorphoidSetup[D[4], Z[8]];
```

Domain		Codomain	
1	1	1	0
Rot	2	2	1
Rot ²	3	3	2
Rot ³	4	4	3
Ref	5	5	4
Rot**Ref	6	6	5
Rot ² **Ref	7	7	6
Rot ³ **Ref	8	8	7

```
h = FormMorphoid[{1, 3, 5, 7, 2, 4, 6, 8}, D[4], Z[8]]
```

```
Morphoid[{1 → 0, Rot → 2, Rot2 → 4, Rot3 → 6, Ref → 1,
  Rot ** Ref → 3, Rot2 ** Ref → 5, Rot3 ** Ref → 7}, -D[4]-, -Z[8]-]
```

```
MorphismQ[h, Mode → Visual]
```

The table entry corresponding to the computation $a*b$ in the domain of the morphoid is colored if and only if the pair $\{a,b\}$ is preserved by the morphoid; i.e., $f(a*b) = f(a)*f(b)$

KEY for D[4]: label used → element: {g1 → 1, g2 → Rot, g3 → Rot², g4 → Rot³, g5 → Ref, g6 → Rot**Ref, g7 → Rot²**Ref, g8 → Rot³**Ref}

D[4]		x * y							
y \ x		g1	g2	g3	g4	g5	g6	g7	g8
g1	g1	g2	g3	g4	g5	g6	g7	g8	
g2	g2	g3	g4	g1	g6	g7	g8	g5	
g3	g3	g4	g1	g2	g7	g8	g5	g6	
g4	g4	g1	g2	g3	g8	g5	g6	g7	
g5	g5	g8	g7	g6	g1	g4	g3	g2	
g6	g6	g5	g8	g7	g2	g1	g4	g3	
g7	g7	g6	g5	g8	g3	g2	g1	g4	
g8	g8	g7	g6	g5	g4	g3	g2	g1	

```
False
```

■ 5. Questions Answered with *AbstractAlgebra*

```
SomeGroups = {Z[5], Dihedral[4], U[12], Z[18], U[24], Symmetric[3],
  DirectProduct[Z[2], Z[3]], RootsOfUnity[6], Alternating[4], Cyclic[8], Klein4}
```

```
Klein4::warning : The elements e, a, b, c are considered
  strings and thus need to have double quotes around them when being used.
```

```
{Groupoid[{0, 1, 2, 3, 4}, Mod[#1 + #2, 5] &],
  Groupoid[{1, Rot, Rot2, Rot3, Ref, Rot ** Ref, Rot2 ** Ref, Rot3 ** Ref}, -Operation-],
  Groupoid[{1, 5, 7, 11}, Mod[#1 #2, 12] &],
  Groupoid[{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17}, Mod[#1 + #2, 18] &],
  Groupoid[{1, 5, 7, 11, 13, 17, 19, 23}, Mod[#1 #2, 24] &],
  Groupoid[{{1, 2, 3}, {1, 3, 2}, {2, 1, 3}, {2, 3, 1}, {3, 1, 2}, {3, 2, 1}}, -Operation-],
  Groupoid[{{0, 0}, {0, 1}, {0, 2}, {1, 0}, {1, 1}, {1, 2}}, -Operation-],
  Groupoid[{1, eiπ/3, e2iπ/3, -1, e-2iπ/3, e-iπ/3}, ei (Arg[#1]+Arg[#2]) &],
  Groupoid[{{1, 2, 3, 4}, {1, 3, 4, 2}, {1, 4, 2, 3}, {2, 1, 4, 3}, {2, 3, 1, 4}, {2, 4, 3, 1},
    {3, 1, 2, 4}, {3, 2, 4, 1}, {3, 4, 1, 2}, {4, 1, 3, 2}, {4, 2, 1, 3}, {4, 3, 2, 1}},
  -Operation-], Groupoid[{1, g, g2, g3, g4, g5, g6, g7}, -Operation-],
  Groupoid[{e, a, b, c}, -Operation-]}
```

```
TableForm[Table[G = SomeGroups[[k]]; g = RandomElement[G];
  {GroupoidName[G], g, h = GroupInverse[G, g], OrderOfElement[G, g], OrderOfElement[G, h]},
  {k, 1, Length[SomeGroups]}],
  TableHeadings → {None, {"group", "g", "g-1", "|g|", "|g-1|\n"}},
  TableSpacing → {0.5, 3}, TableDepth → 2]
```

group	g	g ⁻¹	g	g ⁻¹
Z[5]	2	3	5	5
D[4]	Rot	Rot ³	4	4
U[12]	5	5	2	2
Z[18]	5	13	18	18
U[24]	5	5	2	2
S[3]	{3, 1, 2}	{2, 3, 1}	3	3
Z[2] x Z[3]	{0, 1}	{0, 2}	3	3
RootsOfUnity[6]	e ^{2iπ/3}	e ^{-2iπ/3}	3	3
A[4]	{1, 4, 2, 3}	{1, 3, 4, 2}	3	3
Cyclic[8]	g ⁵	g ³	8	8
Klein4	c	c	2	2

```
TableForm[Table[G = SomeGroups[[k]]; g = RandomElement[G];
  {GroupoidName[G], g, OrderOfElement[G, g], Order[G]}, {k, 1, Length[SomeGroups]}],
  TableHeadings -> {None, {"group", "g", "|g|", "|G|\n"}},
  TableSpacing -> {0.5, 3}, TableDepth -> 2]
```

group	g	g	G
Z[5]	3	5	5
D[4]	Rot ³ ** Ref	2	8
U[12]	7	2	4
Z[18]	3	6	18
U[24]	23	2	8
S[3]	{3, 1, 2}	3	6
Z[2] x Z[3]	{0, 1}	3	6
RootsOfUnity[6]	$e^{-\frac{2i\pi}{3}}$	3	6
A[4]	{1, 3, 4, 2}	3	12
Cyclic[8]	g ⁴	2	8
Klein4	a	2	4

```
Table[G = SomeGroups[[k]];
  H = RandomElements[G, Random[Integer, {1, Order[G]}], Replacement -> False];
  SubgroupQ[H, G, Mode -> Visual], {k, 1, Length[SomeGroups]}]
(* since randomly generated, results will vary *)
```

All the elements marked with yellow are
original elements in the set. Those in red are from outside.

Z[5] x + y

x \ y	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

KEY for D[4]: label used -> element: {g1 -> Ref, g2 -> Rot, g3 -> Rot², g4 -> 1, g5 -> Rot³, g6 -> Rot**Ref, g7 -> Rot²**Ref, g8 -> Rot³**Ref}

D[4] x * y

x \ y	g1	g2	g3	g4	g5	g6	g7	g8
g1	g1	g4	g8	g7	g1	g6	g5	g3
g2	g2	g6	g3	g5	g2	g4	g7	g8
g3	g3	g7	g5	g4	g3	g2	g8	g1
g4	g4	g1	g2	g3	g4	g5	g6	g7
g5	g5	g8	g4	g2	g5	g3	g1	g6
g6	g6	g2	g1	g8	g6	g7	g4	g5
g7	g7	g3	g6	g1	g7	g8	g2	g4
g8	g8	g5	g7	g6	g8	g1	g3	g2

U[12] x * y

x \ y	11	7	1	5
11	1	5	11	7
7	5	1	7	11
1	11	7	1	5
5	7	11	5	1

Z[18] x + y

x \ y	4	11	7	3	14	2	13	0	10	15	17	9	16	6	8	12	1	5
4	8	15	11	7	0	6	17	4	14	1	3	13	2	10	12	16	5	9
11	15	4	0	14	7	13	6	11	3	8	10	2	9	17	1	5	12	16
7	11	0	14	10	3	9	2	7	17	4	6	16	5	13	15	1	8	12
3	7	14	10	6	17	5	16	3	13	0	2	12	1	9	11	5	4	8
14	0	7	3	17	10	16	9	14	6	11	13	5	12	2	4	8	15	1
2	6	13	9	5	16	4	15	2	12	17	1	11	0	8	10	14	3	7
13	17	6	2	16	9	15	8	13	5	10	12	4	11	1	3	7	14	0
0	4	11	7	3	14	2	13	0	10	15	17	9	16	6	8	12	1	5
10	14	3	17	13	6	12	5	10	2	7	9	1	8	16	0	4	11	5
15	1	8	4	0	11	17	10	15	7	12	14	6	13	3	5	9	16	2
17	3	10	6	2	13	1	12	17	9	14	16	8	15	5	7	11	0	4
9	13	2	16	12	5	11	4	9	1	6	8	0	7	15	17	3	10	14
16	2	9	5	1	12	0	11	16	8	13	15	7	14	4	6	10	17	3
6	10	17	13	9	2	8	1	6	16	3	5	15	4	12	14	0	7	11
8	12	1	15	11	4	10	3	8	0	5	7	17	6	14	16	2	9	13
12	16	5	1	15	8	14	7	12	4	9	11	3	10	0	2	6	13	17
1	5	12	8	4	15	3	14	1	11	16	0	10	17	7	9	13	2	6
5	9	16	12	8	1	7	0	5	15	2	4	14	3	11	13	17	6	10

U[24] x * y

x \ y	7	1	5	11	13	17	19	23
7	1	7	11	5	19	23	13	17
1	7	1	5	11	13	17	19	23
5	11	5	1	7	17	13	23	19
11	5	11	7	1	23	19	17	13
13	19	13	17	23	1	5	7	11
17	23	17	13	19	5	1	11	7
19	13	19	23	17	7	11	1	5
23	17	23	19	13	11	7	5	1

KEY for S[3]: label used → element: {g1 → {2, 3, 1}, g2 → {1, 2, 3}, g3 → {3, 1, 2}, g4 → {2, 1, 3}, g5 → {1, 3, 2}, g6 → {3, 2, 1}}

S[3] x * y

$\begin{array}{c c} y \\ \hline x \end{array}$	g1	g2	g3	g4	g5	g6
g1	g3	g1	g2	g6	g4	g5
g2	g1	g2	g3	g4	g5	g6
g3	g2	g3	g1	g5	g6	g4
g4	g5	g4	g6	g2	g1	g3
g5	g6	g5	g4	g3	g2	g1
g6	g4	g6	g5	g1	g3	g2

KEY for Z[2] x Z[3]: label used \rightarrow element: {g1 \rightarrow {1, 2}, g2 \rightarrow {1, 0}, g3 \rightarrow {0, 1}, g4 \rightarrow {0, 0}, g5 \rightarrow {0, 2}, g6 \rightarrow {1, 1}}

Z[2] x Z[3] x * y

$\begin{array}{c c} y \\ \hline x \end{array}$	g1	g2	g3	g4	g5	g6
g1	g3	g5	g2	g1	g6	g4
g2	g5	g4	g6	g2	g1	g3
g3	g2	g6	g5	g3	g4	g1
g4	g1	g2	g3	g4	g5	g6
g5	g6	g1	g4	g5	g3	g2
g6	g4	g3	g1	g6	g2	g5

KEY for RootsOfUnity[6]: label used \rightarrow element: {g1 \rightarrow 1, g2 \rightarrow -1, g3 \rightarrow $E^{(-I/3)*Pi}$, g4 \rightarrow $E^{((-2*I)/3)*Pi}$, g5 \rightarrow $E^{(I/3)*Pi}$, g6 \rightarrow $E^{((2*I)/3)*Pi}$ }

RootsOfUnity[6] x * y

$\begin{array}{c c} y \\ \hline x \end{array}$	g1	g2	g3	g4	g5	g6
g1	g1	g2	g3	g4	g5	g6
g2	g2	g1	g6	g5	g4	g3
g3	g3	g6	g4	g2	g1	g5
g4	g4	g5	g2	g6	g3	g1
g5	g5	g4	g1	g3	g6	g2
g6	g6	g3	g5	g1	g2	g4

KEY for A[4]: label used \rightarrow element: {g1 \rightarrow {3, 1, 2, 4}, g2 \rightarrow {1, 4, 2, 3}, g3 \rightarrow {2, 1, 4, 3}, g4 \rightarrow {3, 2, 4, 1}, g5 \rightarrow {3, 4, 1, 2}, g6 \rightarrow {4, 1, 3, 2}, g7 \rightarrow {1, 3, 4, 2}, g8 \rightarrow {2, 4, 3, 1}, g9 \rightarrow {1, 2, 3, 4}, g10 \rightarrow {4, 2, 1, 3}, g11 \rightarrow {2, 3, 1, 4}, g12 \rightarrow {4, 3, 2, 1}}

A[4] x * y

x \ y	g1	g2	g3	g4	g5	g6	g7	g8	g9	g10	g11	g12	
g1	g1	g11	g5	g7	g3	g8	g12	g4	g2	g1	g6	g9	g10
g2	g3	g7	g6	g8	g11	g1	g9	g12	g2	g5	g10	g4	
g3	g10	g11	g9	g6	g12	g4	g8	g7	g3	g1	g2	g5	
g4	g12	g1	g11	g10	g6	g7	g5	g3	g4	g9	g8	g2	
g5	g7	g4	g12	g2	g9	g11	g1	g10	g5	g8	g6	g3	
g6	g5	g10	g2	g1	g4	g8	g12	g9	g6	g3	g7	g11	
g7	g6	g9	g1	g12	g10	g3	g2	g4	g7	g11	g5	g8	
g8	g4	g3	g10	g5	g1	g9	g11	g6	g8	g2	g12	g7	
g9	g1	g2	g3	g4	g5	g6	g7	g8	g9	g10	g11	g12	
g10	g2	g12	g8	g9	g7	g5	g6	g11	g10	g4	g3	g1	
g11	g9	g8	g4	g7	g2	g10	g3	g5	g11	g12	g1	g6	
g12	g8	g6	g5	g11	g3	g2	g10	g1	g12	g7	g4	g9	

Cyclic[8] x * y

x \ y	g	4	2	3	7	6	1	5
g	2	5	3	4	1	7	g	6
4	5	1	g	g	g	g	g	g
2	3	6	4	5	g	1	2	7
g	g	g	g	g	g	g	g	g
3	4	7	5	6	2	g	g	1
7	1	3	g	2	6	5	7	4
6	7	2	1	g	5	4	6	3
1	g	4	2	3	7	6	1	5
5	6	g	7	1	4	3	5	2
g	g	g	g	g	g	g	g	g

Klein4 x * y

x \ y	c	b	a	e
c	e	a	b	c
b	a	e	c	b
a	b	c	e	a
e	c	b	a	e

{True, False, True, True, False, False, True, True, False, False, False}

```
Flatten[Table[G = DirectSum[Z[m], Z[n]]; {m, n, CyclicQ[G]}, {m, 2, 7}, {n, 2, 7}],
  1] // Partition[#, 9] & // Transpose //
TableForm[#, TableHeadings -> {None, {"m, n, cyclic?"\n"}},
  TableSpacing -> {0.5, 2}, TableDepth -> 2] &
```

```
{m, n, cyclic?}
```

{2, 2, False}	{3, 5, True}	{5, 2, True}	{6, 5, True}
{2, 3, True}	{3, 6, False}	{5, 3, True}	{6, 6, False}
{2, 4, False}	{3, 7, True}	{5, 4, True}	{6, 7, True}
{2, 5, True}	{4, 2, False}	{5, 5, False}	{7, 2, True}
{2, 6, False}	{4, 3, True}	{5, 6, True}	{7, 3, True}
{2, 7, True}	{4, 4, False}	{5, 7, True}	{7, 4, True}
{3, 2, True}	{4, 5, True}	{6, 2, False}	{7, 5, True}
{3, 3, False}	{4, 6, False}	{6, 3, False}	{7, 6, True}
{3, 4, True}	{4, 7, True}	{6, 4, False}	{7, 7, False}

```
TableForm[Table[G = Z[k]; H = CyclicGenerators[G]; {Order[G], H}, {k, 4, 10}],
  TableDepth -> 2, TableSpacing -> {1, 0.5},
  TableHeadings -> {None, {"|Z_n|", "generators\n"}}]
```

```
|Zn| generators
```

4	{1, 3}
5	{1, 2, 3, 4}
6	{1, 5}
7	{1, 2, 3, 4, 5, 6}
8	{1, 3, 5, 7}
9	{1, 2, 4, 5, 7, 8}
10	{1, 3, 7, 9}

```
a = First[ToCycles[RandomPermutation[6]]]
b = First[ToCycles[RandomPermutation[6]]]
MultiplyCycles[a, b]
MultiplyCycles[b, a]
```

```
Cycle[2, 5, 3, 4, 6]
```

```
Cycle[1, 5, 4, 6, 3, 2]
```

```
{3, 1, 5, 2, 6, 4}
```

```
{5, 4, 6, 3, 2, 1}
```

```

G = DirectProduct[Z[7], Z[7]];
 $\beta$  = FormMorphoid[Mod[{2, 6}.#, 7] &, G, Z[7]];
MorphismQ[ $\beta$ ]
(K = Kernel[ $\beta$ ]) // Elements
Img = Image[ $\beta$ ]
QG = QuotientGroup[G, K]
 $\gamma$  = FormMorphoid[ $\beta$ [First[#]] &, QG, Img]
IsomorphismQ[ $\gamma$ , Cautious  $\rightarrow$  True]

True

{{0, 0}, {1, 2}, {2, 4}, {3, 6}, {4, 1}, {5, 3}, {6, 5}}

Groupoid[{0, 1, 2, 3, 4, 5, 6}, Mod[#1 + #2, 7] &]

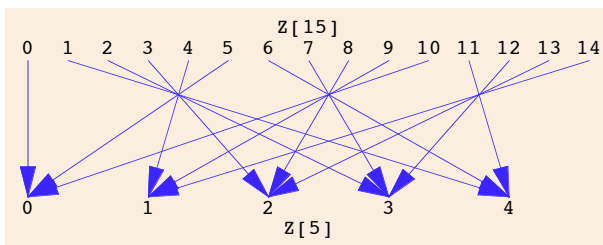
Groupoid[{NS, {0, 1} NS, {0, 2} NS, {0, 3} NS, {0, 4} NS, {0, 5} NS, {0, 6} NS}, -Operation-]

Morphoid[ $\beta$ [First[#1]] &, -Z[7] x Z[7]/NS-, -Z[7]-]

True

VisualizeMorphoid[ZMap[15, 5, 2  $\rightarrow$  3]];

```



```

P = PolynomialsOver[ZR[6]];
TableForm[Table[a = RandomElement[P, 3]; b = RandomElement[P, 2];
{a, b, Degree[P, Multiplication[P][a, b]]}, {10}], TableHeadings  $\rightarrow$ 
{None, {"polynomial a", "polynomial b", "deg(a * b)\n"}}, TableSpacing  $\rightarrow$  {0, 3}]

```

polynomial a	polynomial b	deg(a * b)
$1 + 2x + 2x^2 + 3x^3$	$4 + 2x + x^2$	5
$4 + 4x + 4x^2 + 5x^3$	$3x + 3x^2$	5
$5 + 5x^2 + 3x^3$	$2 + 5x + 3x^2$	5
$1 + 3x^2 + x^3$	$5 + 2x^2$	5
$1 + 2x + 5x^2 + 5x^3$	$1 + 2x + 4x^2$	5
$5 + 5x + 4x^2 + 4x^3$	$3 + 2x + 3x^2$	4
$4 + 5x + 4x^2 + 4x^3$	$5 + 2x + 3x^2$	4
$2 + 5x + 4x^2 + 5x^3$	$4 + x + 5x^2$	5
$3 + 4x + 3x^2 + x^3$	$2 + x^2$	5
$3x^2 + 4x^3$	$3x + 2x^2$	5

```

d = -6;
{a, b} = Table[Random[Integer, {1, 5}], {2}];
x = a + b Sqrt[d]
y = ZdConjugate[x];
z = Expand[x y]
ZdDivisors[d, z, DivisorsComplete -> True, Combine -> Associates]
ZdDivisors[d, z, DivisorsComplete -> True, Combine -> Products]

1 + 3 i Sqrt[6]

55

{{-55, 55}, {-11, 11}, {-5, 5}, {-1, 1}, {-7 - i Sqrt[6], 7 + i Sqrt[6]},
 {7 - i Sqrt[6], -7 + i Sqrt[6]}, {-1 - 3 i Sqrt[6], 1 + 3 i Sqrt[6]}, {1 - 3 i Sqrt[6], -1 + 3 i Sqrt[6]}}

{{-55, -1}, {-11, -5}, {1, 55}, {5, 11}, {-7 - i Sqrt[6], -7 + i Sqrt[6]},
 {7 - i Sqrt[6], 7 + i Sqrt[6]}, {-1 - 3 i Sqrt[6], -1 + 3 i Sqrt[6]}, {1 - 3 i Sqrt[6], 1 + 3 i Sqrt[6]}}

```

■ Mentioned, but not shown, in article

What can we conclude about the structure of the automorphism group of \mathbb{Z}_n ?

[Simply look at the elements of the automorphism group of \mathbb{Z}_n for several values of n .]

```

TableForm[Table[Elements[AutomorphismGroup[Z[k]]], {k, 4, 8}], TableDepth -> 0]

{{Morphoid[1 -> 1, -Z[4]-, -Z[4]-], Morphoid[1 -> 3, -Z[4]-, -Z[4]-]},
 {Morphoid[1 -> 1, -Z[5]-, -Z[5]-], Morphoid[1 -> 2, -Z[5]-, -Z[5]-],
  Morphoid[1 -> 3, -Z[5]-, -Z[5]-], Morphoid[1 -> 4, -Z[5]-, -Z[5]-]},
 {Morphoid[1 -> 1, -Z[6]-, -Z[6]-], Morphoid[1 -> 5, -Z[6]-, -Z[6]-]},
 {Morphoid[1 -> 1, -Z[7]-, -Z[7]-], Morphoid[1 -> 2, -Z[7]-, -Z[7]-],
  Morphoid[1 -> 3, -Z[7]-, -Z[7]-], Morphoid[1 -> 4, -Z[7]-, -Z[7]-],
  Morphoid[1 -> 5, -Z[7]-, -Z[7]-], Morphoid[1 -> 6, -Z[7]-, -Z[7]-]},
 {Morphoid[1 -> 1, -Z[8]-, -Z[8]-], Morphoid[1 -> 3, -Z[8]-, -Z[8]-],
  Morphoid[1 -> 5, -Z[8]-, -Z[8]-], Morphoid[1 -> 7, -Z[8]-, -Z[8]-]}

```

What is the order of an element in a direct product? Is it related to the order of its coordinates?

[Picking a random, nonidentity element from the direct product $U_{15} \times \mathbb{Z}_6$, compute the order of both the element and its coordinates in the coordinate groups.]

```

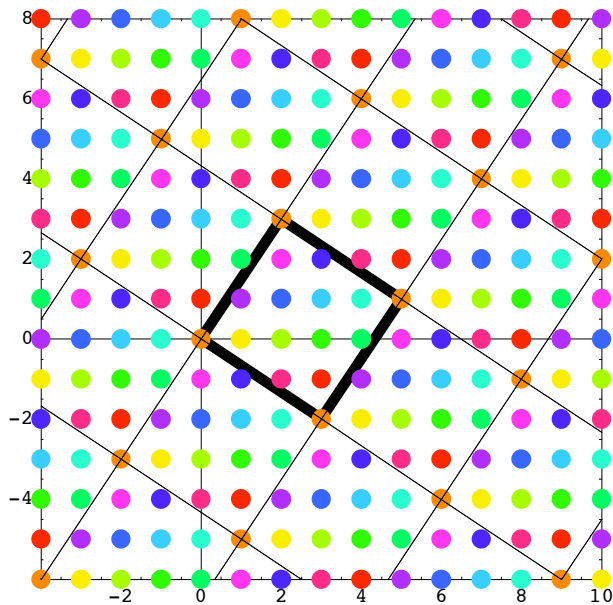
G1 = U[15]; G2 = Z[6]; G = DirectProduct[G1, G2];
TableForm[Table[g = RandomElement[G, SelectFrom -> NonIdentity];
 {g, OrderOfElement[G, g], OrderOfElement[{{G1, First[g]}, {G2, Last[g]}}]}, {8}],
 TableDepth -> 2, TableHeadings -> {None, {"g = {x, y}", "|g|", "{|x|, |y|}\n"}},
 TableSpacing -> {0.5, 3}]

```

$g = \{x, y\}$	$ g $	$\{ x , y \}$
{8, 5}	12	{4, 6}
{11, 1}	6	{2, 6}
{11, 2}	6	{2, 3}
{1, 5}	6	{1, 6}
{1, 1}	6	{1, 6}
{11, 4}	6	{2, 3}
{11, 5}	6	{2, 6}
{2, 1}	12	{4, 6}

Determine the structure of the quotient ring $\mathbb{Z}[i]/\langle 2+3i \rangle$.

```
SwitchStructureTo[Ring]; QuotientRing[Z[I], 2 + 3 I, Mode -> Visual]
```



QuotientRing::J : This quotient ring uses J to represent the principal ideal generated by $2+3i$.

```
Ringoid[{J, 1+J, 2+J, 3+J, 4+J, (4+i)+J, (3+i)+J, (2+i)+J, (3+2i)+J,
(1+i)+J, (2+2i)+J, (2-i)+J, (3-i)+J}, -Addition-, -Multiplication-]
```

Using the Mod p Irreducibility Test (where the degree of the polynomial reduced mod p must be the same as the degree of original), for what p , if any, do we determine whether the polynomial $4x^3 - 5x^2 + x - 8$ is irreducible or not?

[Using the first five primes, reduce this polynomial mod the prime p and then consider the images of this reduced polynomial when the domain \mathbb{Z}_p is used.]

```
f = 4 x^3 - 5 x^2 + x - 8;
TableForm[Table[{k = Prime[j], fk = Poly[Z[k], f],
Map[PolynomialEvaluation[fk, #] &, Elements[Z[k]]]}, {j, 1, 5}], TableDepth -> 2,
TableHeadings -> {None, {"prime", "f reduced", "images of Z_n"}}]
```

prime	f reduced	images of \mathbb{Z}_n
2	$x + x^2$	{0, 0}
3	$1 + x + x^2 + x^3$	{1, 1, 0}
5	$2 + x + 4x^3$	{2, 2, 1, 3, 2}
7	$6 + x + 2x^2 + 4x^3$	{6, 6, 6, 2, 4, 1, 3}
11	$3 + x + 6x^2 + 4x^3$	{3, 3, 6, 3, 7, 9, 0, 4, 1, 4, 4}

Using $x^4 + x^3 + 1$ as the irreducible polynomial in the Galois field of order 16 (with x as a generator), explain why every element in the left column (in multiplicative notation) is equal to the element in the corresponding position in the right column (given in additive notation).

```

IrreduciblePolynomial[x, 2, 4]
TableOfPowers[GF[2, 4]] // MatrixForm

```

 $1 + x^3 + x^4$

$$\begin{pmatrix} 0 & 0 \\ x & x \\ x^2 & x^2 \\ x^3 & x^3 \\ x^4 & 1 + x^3 \\ x^5 & 1 + x + x^3 \\ x^6 & 1 + x + x^2 + x^3 \\ x^7 & 1 + x + x^2 \\ x^8 & x + x^2 + x^3 \\ x^9 & 1 + x^2 \\ x^{10} & x + x^3 \\ x^{11} & 1 + x^2 + x^3 \\ x^{12} & 1 + x \\ x^{13} & x + x^2 \\ x^{14} & x^2 + x^3 \\ 1 & 1 \end{pmatrix}$$