

# Mathematische Strukturen in Sage

Sehr viele mathematische Strukturen sind bereits in Sage implementiert. Wir sehen uns hier exemplarisch drei Strukturen an: Gruppen, am Beispiel der symmetrischen Gruppe  $S_n$ , Graphen und elliptische Kurven.

## Symmetrische Gruppe

```
In [78]: S5=SymmetricGroup(5)
```

```
In [79]: S5
```

```
Out[79]: Symmetric group of order 5! as a permutation group
```

Angabe von Permutationen  $\sigma \in S_n$  in Listenschreibweise:  $[\sigma(1), \sigma(2), \dots, \sigma(n)]$

```
In [80]: p1=S5([2,1,4,5,3])
p1
```

```
Out[80]: (1,2)(3,4,5)
```

Intern werden Permutationen in **Zyklenschreibweise** umgewandelt. Ein **Zyklus**  $\sigma = (a_1, a_2, \dots, a_k)$  ist die Permutation mit  $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{k-1}) = a_k$  und  $\sigma(a_k) = a_1$ . Jede Permutation kann als Produkt disjunkter Zyklen geschrieben werden.

```
In [81]: S5([2,4,5,6,1,3])
```

```

-----
-
AssertionError                                Traceback (most recent call las
t)
Cell In[81], line 1
----> 1 S5([Integer(2),Integer(4),Integer(5),Integer(6),Integer(1),Integer
(3)])

File /opt/sagemath/sage-10.7/src/sage/structure/parent.pyx:900, in sage.st
ructure.parent.Parent.__call__()
    898 if mor is not None:
    899     if no_extra_args:
--> 900         return mor._call_(x)
    901     else:
    902         return mor._call_with_args(x, args, kwds)

File /opt/sagemath/sage-10.7/src/sage/structure/coerce_maps.pyx:164, in sa
ge.structure.coerce_maps.DefaultConvertMap_unique._call__()
    162         print(type(C), C)
    163         print(type(C._element_constructor), C._element_constru
ctor)
--> 164         raise
    165
    166 cpdef Element _call_with_args(self, x, args=(), kwds={}):

File /opt/sagemath/sage-10.7/src/sage/structure/coerce_maps.pyx:159, in sa
ge.structure.coerce_maps.DefaultConvertMap_unique._call__()
    157 cdef Parent C = self._codomain
    158 try:
--> 159     return C._element_constructor(x)
    160 except Exception:
    161     if print_warnings:

File /opt/sagemath/sage-10.7/src/sage/groups/perm_gps/permgroup.py:900, in
PermutationGroup_generic._element_constructor_(self, x, check)
    896     if compatible_domains and (isinstance(self, SymmetricGroup)
    897                                     or x.gap() in self.gap()):
    898         return self.element_class(x, self, check=False)
--> 900 return self.element_class(x, self, check=check)

File /opt/sagemath/sage-10.7/src/sage/groups/perm_gps/permgroup_element.py
x:480, in sage.groups.perm_gps.permgroup_element.PermutationGroupElement._
_init__()
    478         self._set_list_cycles(g, convert)
    479     else:
--> 480         self._set_list_images(g, convert)
    481 elif isinstance(g, str):
    482     self._set_string(g)

File /opt/sagemath/sage-10.7/src/sage/groups/perm_gps/permgroup_element.py
x:568, in sage.groups.perm_gps.permgroup_element.PermutationGroupElement._
set_list_images()
    566 """
    567 cdef int i, j, vn = len(v)
--> 568 assert vn <= self.n
    569 if convert:
    570     convert_dict = self._parent._domain_to_gap

```

AssertionError:

```
In [82]: S5([1,1,2,3,4])
```

```
-----  
-  
ValueError                                Traceback (most recent call las  
t)  
Cell In[82], line 1  
----> 1 S5([Integer(1),Integer(1),Integer(2),Integer(3),Integer(4)])  
  
File /opt/sagemath/sage-10.7/src/sage/structure/parent.pyx:900, in sage.st  
ructure.parent.Parent.__call__()  
    898 if mor is not None:  
    899     if no_extra_args:  
--> 900         return mor._call_(x)  
    901     else:  
    902         return mor._call_with_args(x, args, kwds)  
  
File /opt/sagemath/sage-10.7/src/sage/structure/coerce_maps.pyx:164, in sa  
ge.structure.coerce_maps.DefaultConvertMap_unique._call__()  
    162         print(type(C), C)  
    163         print(type(C._element_constructor), C._element_constru  
ctor)  
--> 164         raise  
    165  
    166 cpdef Element _call_with_args(self, x, args=(), kwds={}):  
  
File /opt/sagemath/sage-10.7/src/sage/structure/coerce_maps.pyx:159, in sa  
ge.structure.coerce_maps.DefaultConvertMap_unique._call__()  
    157 cdef Parent C = self._codomain  
    158 try:  
--> 159     return C._element_constructor(x)  
    160 except Exception:  
    161     if print_warnings:  
  
File /opt/sagemath/sage-10.7/src/sage/groups/perm_gps/permgroup.py:900, in  
PermutationGroup_generic._element_constructor_(self, x, check)  
    896     if compatible_domains and (isinstance(self, SymmetricGroup)  
    897                                     or x.gap() in self.gap()):  
    898         return self.element_class(x, self, check=False)  
--> 900 return self.element_class(x, self, check=check)  
  
File /opt/sagemath/sage-10.7/src/sage/groups/perm_gps/permgroup_element.py  
x:518, in sage.groups.perm_gps.permgroup_element.PermutationGroupElement.  
__init__()  
    516 # a valid permutation (else segfaults, infinite loops may occur).  
    517 if not is_valid_permutation(self.perm, self.n):  
--> 518     raise ValueError("invalid data to initialize a permutation")  
    519  
    520 # This is more expensive
```

**ValueError:** invalid data to initialize a permutation

Auch die Eingabe kann in Zyklenschreibweise, als Liste der Zyklen, erfolgen.

```
In [83]: p2=S5([(2,3),(1,4)])  
p2
```

```
Out[83]: (1,4)(2,3)
```

Achtung: Multiplikation von Permutationen erfolgt in Sage mit der etwas unüblichen Konvention  $(fg)(x) := g(f(x))$ , anstatt des üblicheren  $(fg)(x) := f(g(x))$ !

```
In [89]: p1, p2
```

```
Out[89]: ((1,2)(3,4,5), (1,4)(2,3))
```

```
In [90]: p1*p2
```

```
Out[90]: (1,3)(2,4,5)
```

```
In [91]: p2*p1
```

```
Out[91]: (1,5,3)(2,4)
```

```
In [92]: p1^-1
```

```
Out[92]: (1,2)(3,5,4)
```

```
In [93]: p1
```

```
Out[93]: (1,2)(3,4,5)
```

Analog zu Vektorräumen: die von Elementen erzeugte Untergruppe ist die kleinste Untergruppe, die alle gegebenen Elemente enthält.

```
In [94]: G=S5.subgroup([p1])  
G
```

```
Out[94]: Subgroup generated by [(1,2)(3,4,5)] of (Symmetric group of order 5! as  
a permutation group)
```

```
In [95]: list(G)
```

```
Out[95]: [(), (1,2)(3,4,5), (3,5,4), (1,2), (3,4,5), (1,2)(3,5,4)]
```

```
In [96]: len(G)
```

```
Out[96]: 6
```

Verknüpfungstabelle

```
In [97]: G.cayley_table()
```

```
Out[97]: *  a b c d e f  
      +-----  
      a| a b c d e f  
      b| b c a e f d  
      c| c a b f d e  
      d| d e f a b c  
      e| e f d b c a  
      f| f d e c a b
```

```
In [98]: _.translation()
```

```
Out[98]: {'a': (),
          'b': (3,4,5),
          'c': (3,5,4),
          'd': (1,2),
          'e': (1,2)(3,4,5),
          'f': (1,2)(3,5,4)}
```

```
In [99]: G.cayley_table(names='elements')
```

```
Out[99]:      *          ()      (3,4,5)      (3,5,4)      (1,2) (1,2)
(3,4,5) (1,2)(3,5,4)

+-----+
-----
          ()|          ()      (3,4,5)      (3,5,4)      (1,2) (1,2)
(3,4,5) (1,2)(3,5,4)
          (3,4,5)|          (3,4,5)      (3,5,4)          () (1,2)(3,4,5) (1,2)
(3,5,4)          (1,2)
          (3,5,4)|          (3,5,4)          ()      (3,4,5) (1,2)(3,5,4)
(1,2) (1,2)(3,4,5)
          (1,2)|          (1,2) (1,2)(3,4,5) (1,2)(3,5,4)          ()
(3,4,5)          (3,5,4)
(1,2)(3,4,5)| (1,2)(3,4,5) (1,2)(3,5,4)          (1,2)      (3,4,5)
(3,5,4)          ()
(1,2)(3,5,4)| (1,2)(3,5,4)          (1,2) (1,2)(3,4,5)      (3,5,4)
()          (3,4,5)
```

```
In [100... G.is_abelian()
```

```
Out[100... True
```

```
In [101... S5.is_abelian()
```

```
Out[101... False
```

Liste aller Untergruppen

```
In [102... S5ss=S5.subgroups()
len(S5ss)
```

```
Out[102... 156
```

```
In [103... S5ss
```



Subgroup generated by  $[(1,2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,5)(3,4), (2,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5)(2,4), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4)(2,3), (1,3)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2)(3,5), (1,3)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3)(4,5), (1,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(4,5), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(4,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(4,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2), (1,2)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4), (2,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,5), (1,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3), (1,4)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3), (1,3)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3), (1,3)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,5), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4,5,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),



Subgroup generated by  $[(2,3,4), (3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4), (3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,5), (2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,5), (1,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,3), (2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4), (1,2)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,5), (1,2)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,3), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,4), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,5), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,5), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,5), (1,2)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(4,5), (2,4)(3,5), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2), (1,4)(2,5), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(4,5), (1,4)(3,5), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,5), (2,4)(3,5), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4), (1,3)(2,4), (1,4)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5), (1,4)(3,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,5), (2,3)(4,5), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2), (1,3)(2,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4), (1,5)(3,4), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3), (1,3)(2,4), (1,2)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3), (1,3)(2,5), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5), (1,4)(2,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4), (1,2)(3,4), (1,4)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,5), (1,5)(2,4), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3), (1,5)(2,3), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5,2,3,4), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4,5,2), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,2,4,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4,2,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4,3,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,3,4,5), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,5)(3,4), (2,4)(3,5), (2,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3)(4,5), (1,4)(3,5), (3,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4)(2,3), (1,3)(2,4), (1,2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2)(3,5), (1,3)(2,5), (1,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5)(2,4), (1,4)(2,5), (1,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4,5), (4,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,3), (2,3), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4,5), (1,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,4,5), (4,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,4), (3,4), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,5), (1,2), (1,2)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4), (3,4), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,5), (2,5), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4), (1,2), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,5), (1,5), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,5,2,3,4), (2,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4,5,2), (1,3,5,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,2,4,5), (1,5,2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,3,4,2,5), (1,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,4,3,5), (1,3,5,2)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,2,3,4,5), (2,3,5,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(2,3,4), (4,5), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(3,4,5), (1,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
Subgroup generated by  $[(1,4,5), (1,2), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
Subgroup generated by  $[(1,2,3), (3,4), (1,4)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
Subgroup generated by  $[(1,2,5), (2,3), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
Subgroup generated by  $[(1,5,2,3,4), (2,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
Subgroup generated by  $[(1,5,2,3,4), (2,5)]$  of (Symmetric group of order  $5!$  as a permutation group)]

Wir filtern diese Liste nach Abelschen Untergruppen.

```
In [104... S5ab=[G for G in S5ss if G.is_abelian()]
```

```
In [105... len(S5ab)
```

```
Out[105... 87
```

```
In [106... S5ab
```



Subgroup generated by  $[(1,2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,5)(3,4), (2,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5)(2,4), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4)(2,3), (1,3)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2)(3,5), (1,3)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3)(4,5), (1,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(4,5), (2,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(4,5), (1,2)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(4,5), (1,3)(4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(3,4), (2,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2), (1,2)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(3,4), (1,5)(3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,4), (2,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2), (1,2)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(3,5), (1,4)(3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,3), (1,4)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5), (1,5)(2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3), (1,3)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5), (1,5)(2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3), (1,3)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,5), (1,4)(2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,3,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,4,5,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),

Subgroup generated by  $[(1,4,2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5,2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5,3,2)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4,2)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5,4,2)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,5,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,5,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4,5,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,3,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4,2,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,5,2,3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,4,3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4,5,2)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,2,4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,3), (4,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,5), (3,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(3,4,5), (1,2)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,2,4), (3,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,4,5), (2,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,3,4), (1,5)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,3,5), (1,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,5), (2,4)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(2,4,5), (1,3)]$  of (Symmetric group of order  $5!$  as a permutation group),  
 Subgroup generated by  $[(1,3,4), (2,5)]$  of (Symmetric group of order  $5!$  as a permutation group)]

## Graphen

Ein Graph besteht aus einer Menge von Knoten und einer Menge von Kanten, die

zwischen je zwei Knoten verlaufen.

```
In [107... g=Graph() # leerer Graph
```

```
In [108... g.add_vertex(0)  
g
```

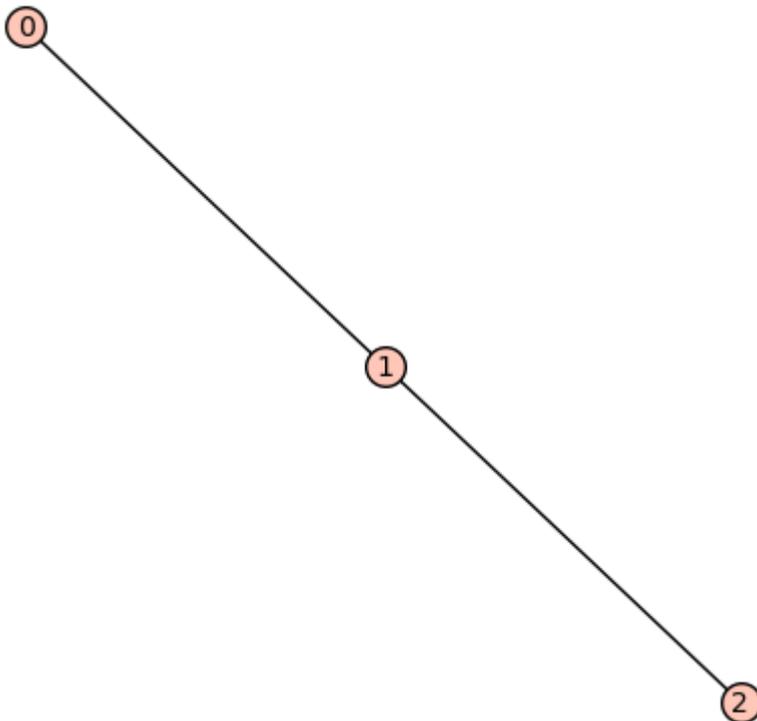
```
Out[108... Graph on 1 vertex
```



```
In [109... g.show()
```



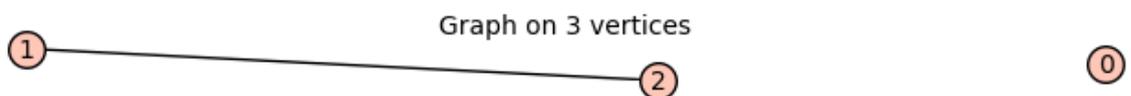
```
In [110... g.add_edge(1,2)  
g.add_edge(1,0)  
g.show()
```



```
In [111... g.delete_edge(1,0)
```

```
In [112... g
```

```
Out[112...
```



Als Bezeichnungen der Knoten können fast beliebige Objekte genommen werden.

Wichtig ist nur, dass die Objekte **immutable**, also unveränderbar sind.

Matrizen sind z.B. standardmäßig nicht immutable, da ihre Einträge verändert werden können.

```
In [113... a=matrix(2,2,[1,x,2,3])  
a
```

```
Out[113... [1 x]  
[2 3]
```

```
In [114... g.add_edge(1,a)
```

```

-----
-
TypeError                                 Traceback (most recent call las
t)
Cell In[114], line 1
----> 1 g.add_edge(Integer(1),a)

File /opt/sagemath/sage-10.7/src/sage/graphs/generic_graph.py:12629, in Ge
nericGraph.add_edge(self, u, v, label)
    12626         except Exception:
    12627             pass
> 12629 self._backend.add_edge(u, v, label, self._directed)

File /opt/sagemath/sage-10.7/src/sage/graphs/base/c_graph.pyx:2334, in sag
e.graphs.base.c_graph.CGraphBackend.add_edge()
    2332         self.add_edge(u, v, l, directed)
    2333
-> 2334 cdef add_edge(self, object u, object v, object l, bint directed):
    2335     """
    2336     Add the edge ``(u,v)`` to ``self``.

File /opt/sagemath/sage-10.7/src/sage/graphs/base/c_graph.pyx:2412, in sag
e.graphs.base.c_graph.CGraphBackend.add_edge()
    2410
    2411         cdef int u_int = self.check_labelled_vertex(u, False)
-> 2412         cdef int v_int = self.check_labelled_vertex(v, False)
    2413
    2414         cdef CGraph cg = self.cg()

File /opt/sagemath/sage-10.7/src/sage/graphs/base/c_graph.pyx:1643, in sag
e.graphs.base.c_graph.CGraphBackend.check_labelled_vertex()
    1641 cdef CGraph G = self.cg()
    1642
-> 1643 cdef int u_int = self.get_vertex(u)
    1644 if u_int != -1:
    1645     if not bitset_in(G.active_vertices, u_int):

File /opt/sagemath/sage-10.7/src/sage/graphs/base/c_graph.pyx:1600, in sag
e.graphs.base.c_graph.CGraphBackend.get_vertex()
    1598 cdef CGraph G = self.cg()
    1599 cdef long u_long
-> 1600 if u in vertex_ints:
    1601     return vertex_ints[u]
    1602 try:

File /opt/sagemath/sage-10.7/src/sage/matrix/matrix0.pyx:6123, in sage.mat
rix.matrix0.Matrix.__hash__()
    6121     """
    6122     if not self._is_immutable:
-> 6123         raise TypeError("mutable matrices are unhashable")
    6124     if self.hash != -1:
    6125         return self.hash

```

**TypeError:** mutable matrices are unhashable

Wir machen die Matrix immutable.

In [115... `a.set_immutable()`

```
In [116.. a[0,0]=2
```

```
-----  
-  
ValueError                                Traceback (most recent call las  
t)  
Cell In[116], line 1  
----> 1 a[Integer(0),Integer(0)]=Integer(2)  
  
File /opt/sagemath/sage-10.7/src/sage/matrix/matrix0.pyx:1460, in sage.mat  
rix.matrix0.Matrix.__setitem__()  
    1458 # If the matrix is immutable, check_mutability will raise an  
    1459 # exception.  
-> 1460 self.check_mutability()  
    1461  
    1462 if type(key) is tuple:  
  
File /opt/sagemath/sage-10.7/src/sage/matrix/matrix0.pyx:422, in sage.matr  
ix.matrix0.Matrix.check_mutability()  
    420 """  
    421 if self._is_immutable:  
--> 422     raise ValueError("matrix is immutable; please change a copy in  
stead (i.e., use copy(M) to change a copy of M).")  
    423 else:  
    424     self._cache = None  
  
ValueError: matrix is immutable; please change a copy instead (i.e., use c  
opy(M) to change a copy of M).
```

```
In [117.. B=a
```

```
In [118.. B[0,0]=2
```

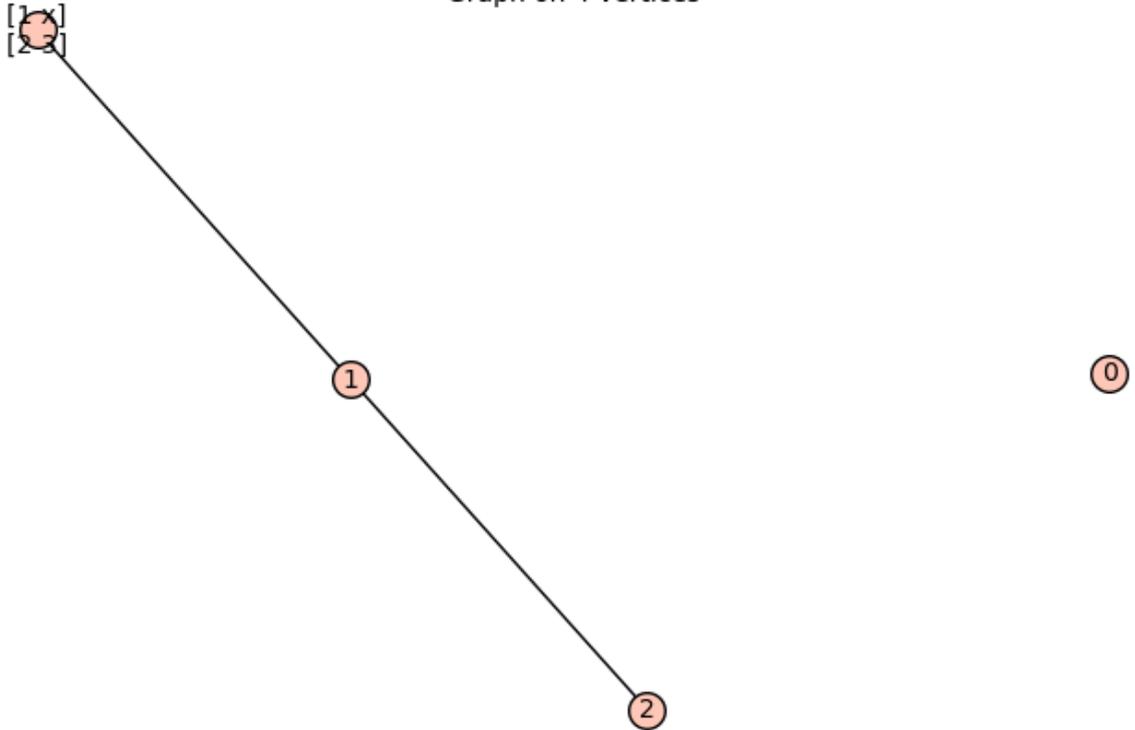
```
-----  
-  
ValueError                                Traceback (most recent call las  
t)  
Cell In[118], line 1  
----> 1 B[Integer(0),Integer(0)]=Integer(2)  
  
File /opt/sagemath/sage-10.7/src/sage/matrix/matrix0.pyx:1460, in sage.mat  
rix.matrix0.Matrix.__setitem__()  
    1458 # If the matrix is immutable, check_mutability will raise an  
    1459 # exception.  
-> 1460 self.check_mutability()  
    1461  
    1462 if type(key) is tuple:  
  
File /opt/sagemath/sage-10.7/src/sage/matrix/matrix0.pyx:422, in sage.matr  
ix.matrix0.Matrix.check_mutability()  
    420 """  
    421 if self._is_immutable:  
--> 422     raise ValueError("matrix is immutable; please change a copy in  
stead (i.e., use copy(M) to change a copy of M).")  
    423 else:  
    424     self._cache = None  
  
ValueError: matrix is immutable; please change a copy instead (i.e., use c  
opy(M) to change a copy of M).
```

```
In [119... g.add_edge(1,a)
```

```
In [120... g
```

```
Out[120...
```

Graph on 4 vertices

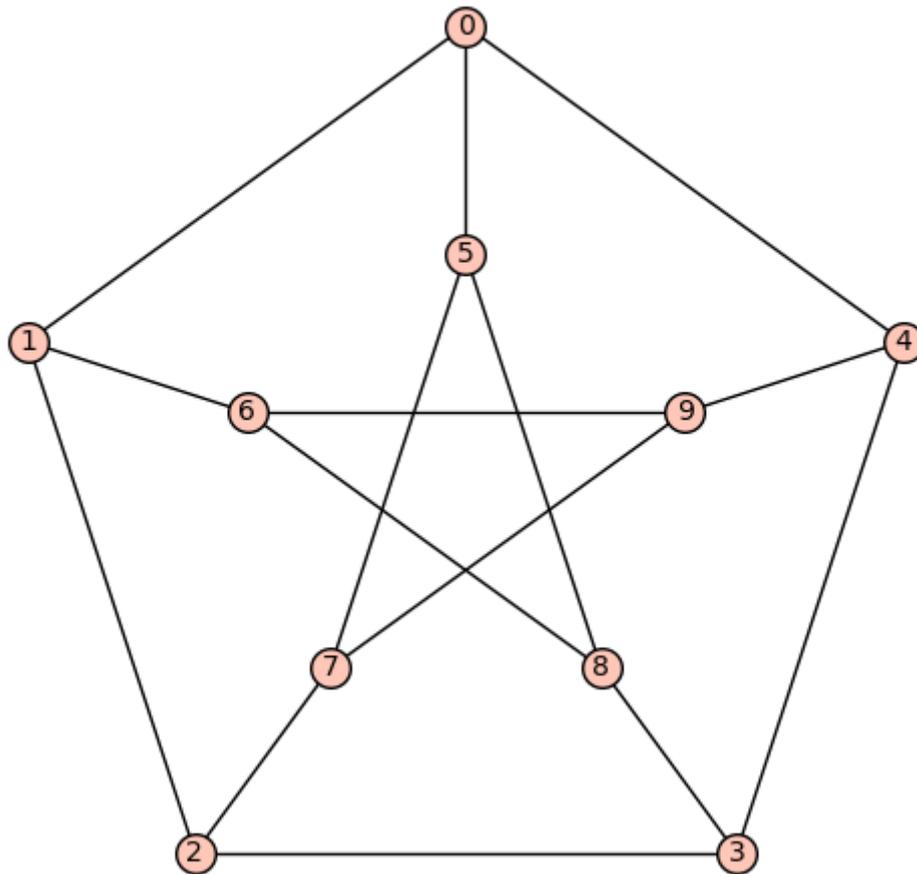


Sage hat eine große Bibliothek an vordefinierten Graphen.

```
In [121... p=graphs.PetersenGraph()  
p
```

Out[121...

Petersen graph: Graph on 10 vertices



Viele Graphentheoretische Algorithmen sind in Sage implementiert. Hier ein paar Beispiele.

Kann der Graph gezeichnet werden, ohne dass sich Kanten überkreuzen?

```
In [122... p.is_planar()
```

Out[122... False

```
In [123... p.neighbors(1)
```

Out[123... [0, 2, 6]

Wie viele Farben braucht man, um die Knoten so einzufärben, dass benachbarte Knoten verschiedene Farben haben? (vgl. Vierfarbensatz)

```
In [124... p.chromatic_number()
```

Out[124... 3

Eine konkrete Färbung.

```
In [125... p.coloring()
```

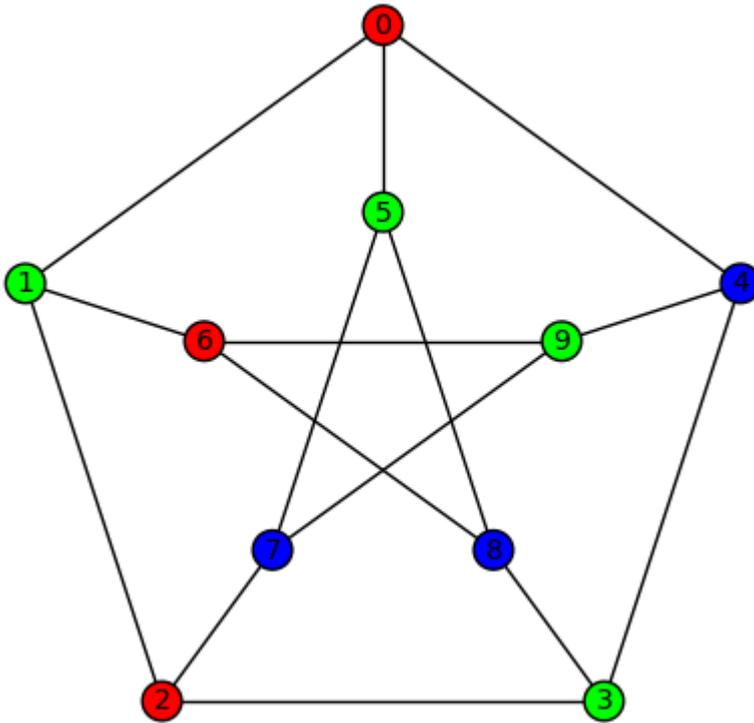
Out[125... [[0, 2, 6], [1, 3, 5, 9], [4, 7, 8]]

Wir wollen die Färbung direkt im Bild des Graphen anzeigen.

```
In [127... c=p.coloring(hex_colors=True)
c
```

```
Out[127... {'#ff0000': [0, 2, 6], '#00ff00': [1, 3, 5, 9], '#0000ff': [4, 7, 8]}
```

```
In [128... p.show(vertex_colors=c)
```



Wir wollen nun die Knoten so umbenennen, dass jeweils die inneren mit den äußeren Knoten Plätze tauschen. Dass können wir über eine Permutation der Knoten erreichen.

```
In [129... S10=SymmetricGroup([0..9])
S10
```

```
Out[129... Symmetric group of order 10! as a permutation group
```

```
In [130... u=S10([5,6,7,8,9,0,1,2,3,4])
u
```

```
Out[130... (0,5)(1,6)(2,7)(3,8)(4,9)
```

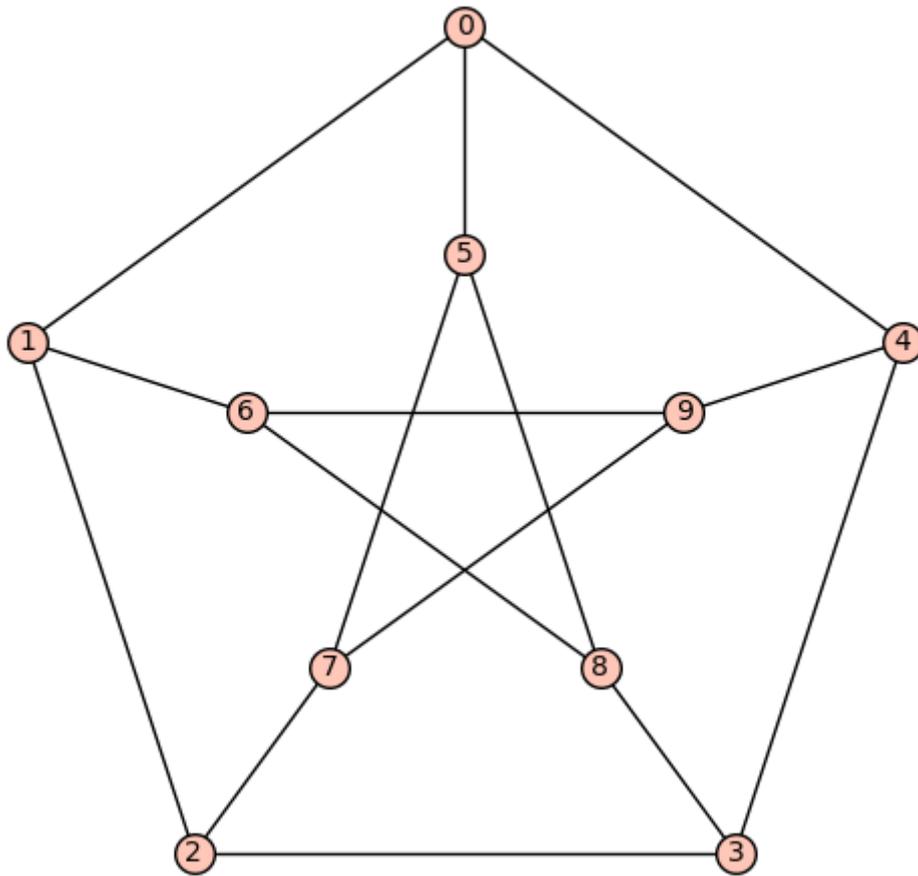
Umbenennen verändert den Graphen, also arbeiten wir lieber mit einer Kopie

```
In [133... p2=p.copy()
```

```
In [134... p2
```

Out[134...

Petersen graph: Graph on 10 vertices

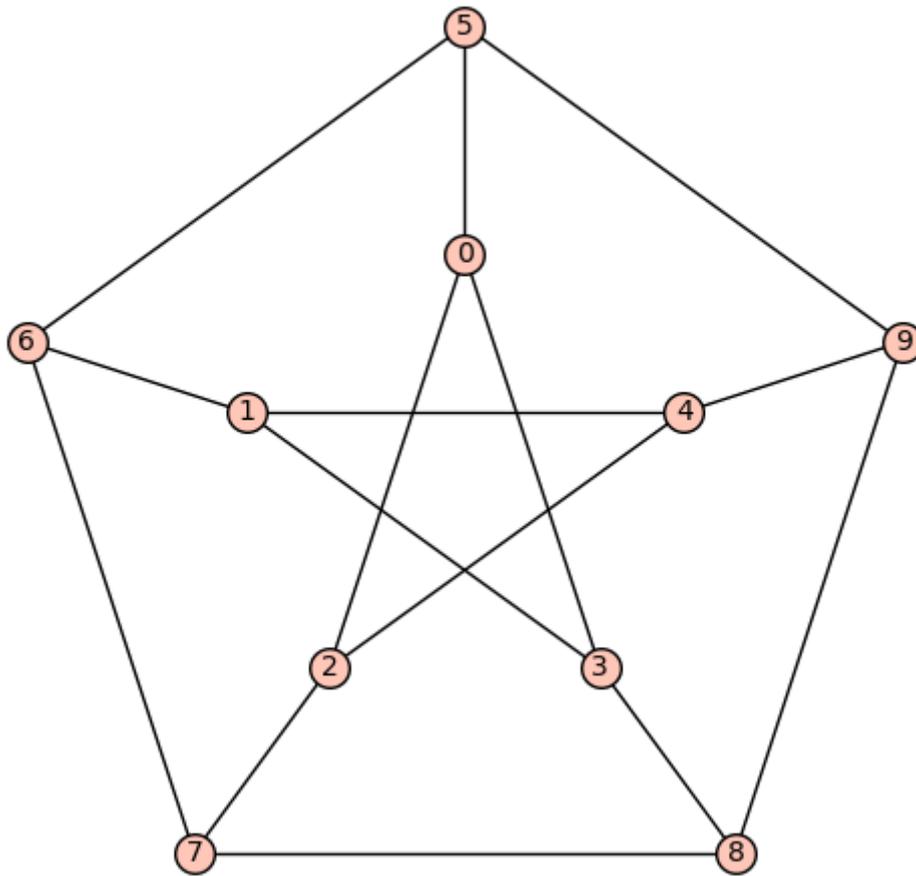


In [135... `p2.relabel(u)`

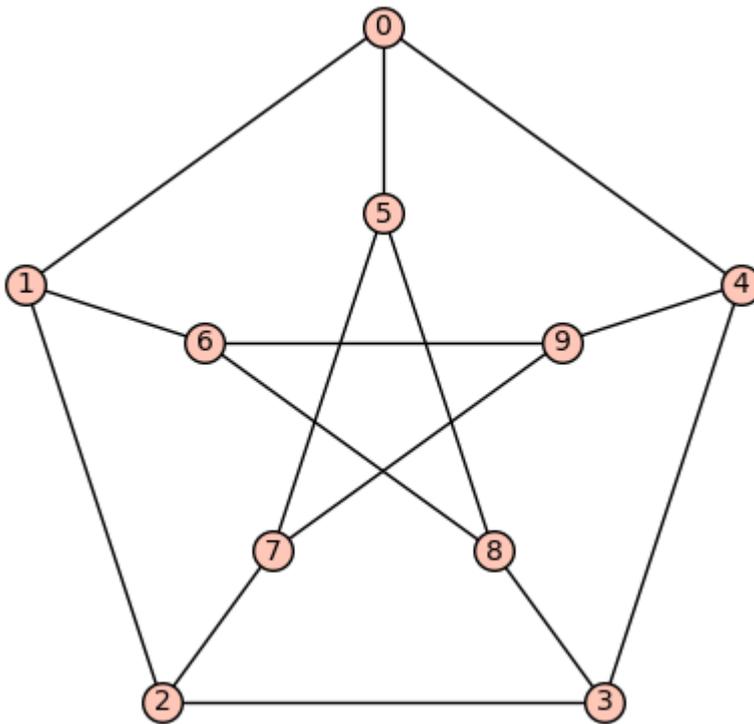
In [136... `p2`

Out[136...

Petersen graph: Graph on 10 vertices



In [137... `p.show()`



Sind zwei Graphen gleich bis auf Umbenennen der Knoten?

In [138... `p.is_isomorphic(p2)`

Out[138... True

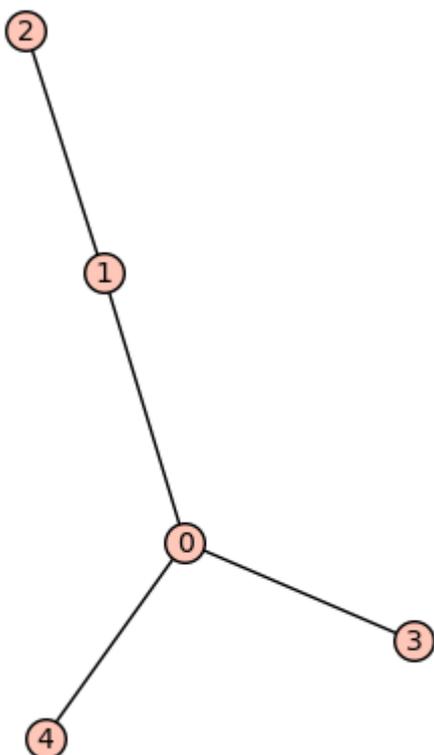
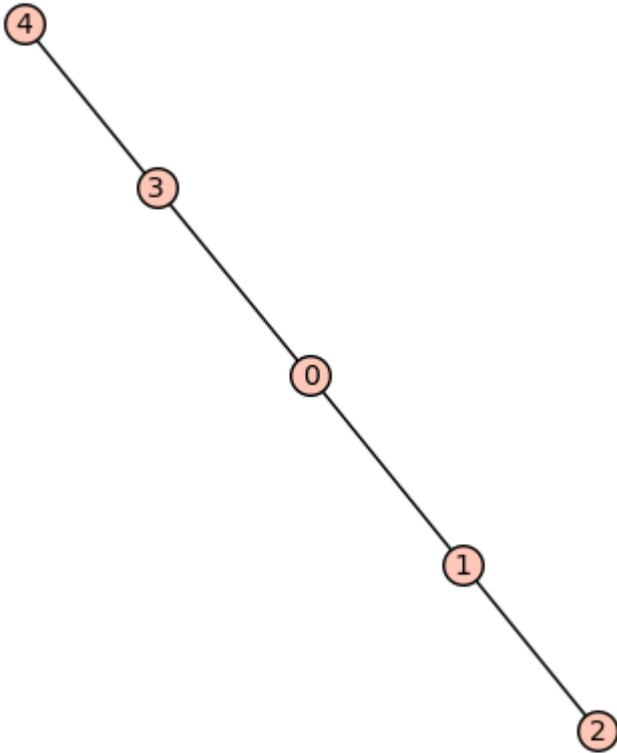
Bäume sind Graphen, die keine Kreise enthalten, also keine Pfade, die im selben Knoten beginnen und enden.

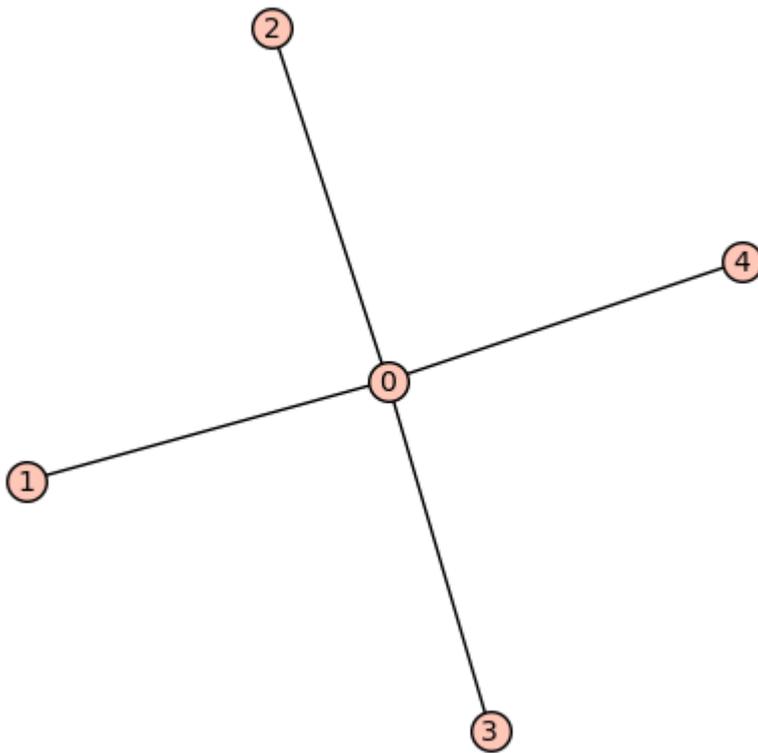
Wir erzeugen hier alle Bäume mit 5 Knoten.

```
In [139... t5=graphs.trees(5)  
t5
```

```
Out[139... <sage.graphs.trees.TreeIterator object at 0x7f8055308bc0>
```

```
In [140... for t in t5:  
t.show()
```

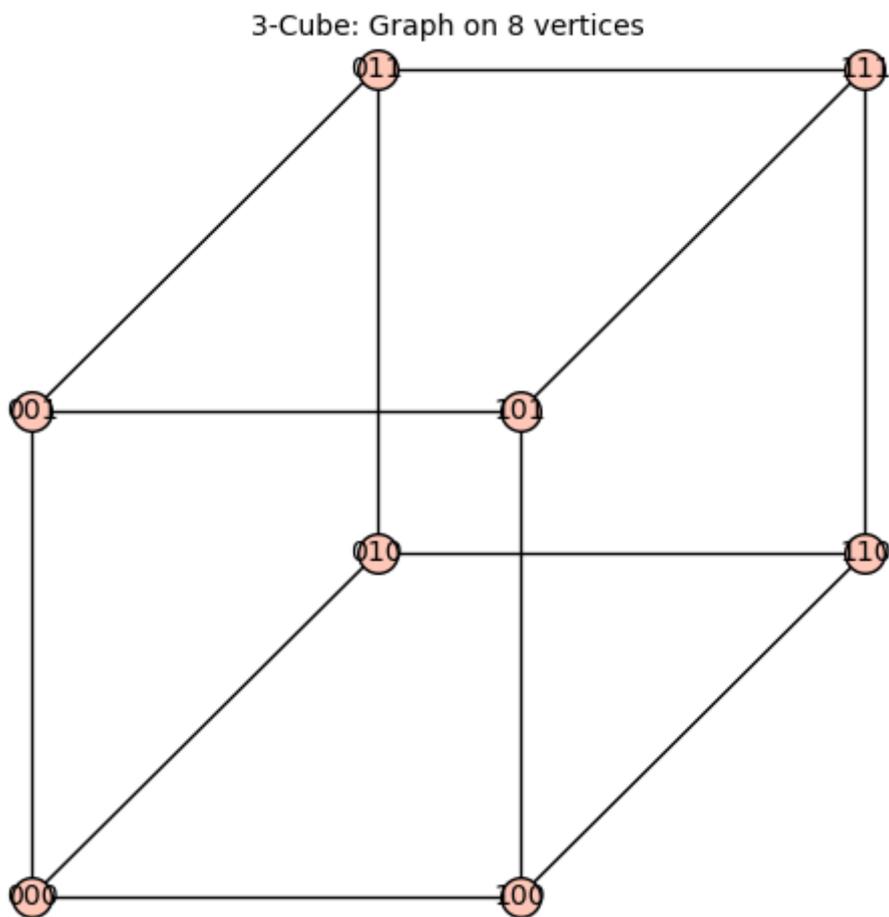




Der Graph bestehend aus Ecken und Kanten eines Würfel.

```
In [243... g6=graphs.CubeGraph(3,embedding=3)
g6
```

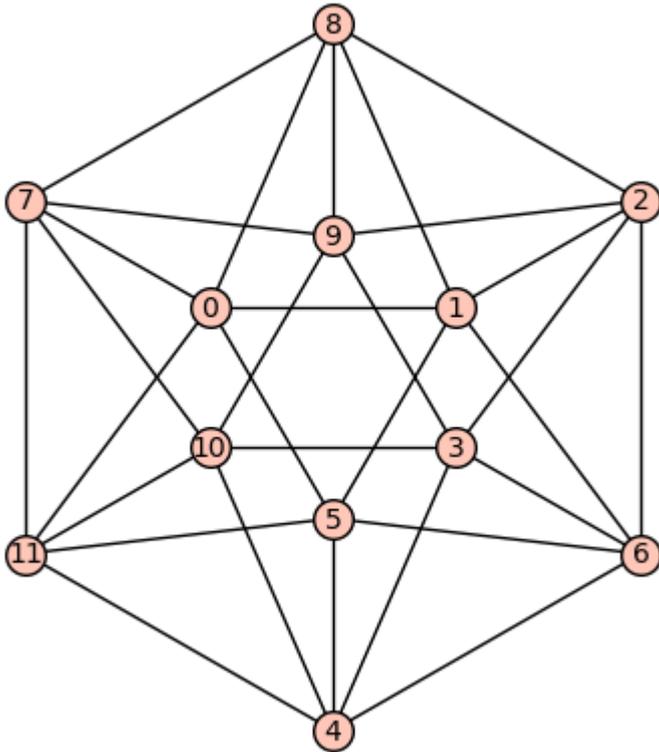
Out[243...



Dasselbe mit einem Icosaeder statt Würfel.

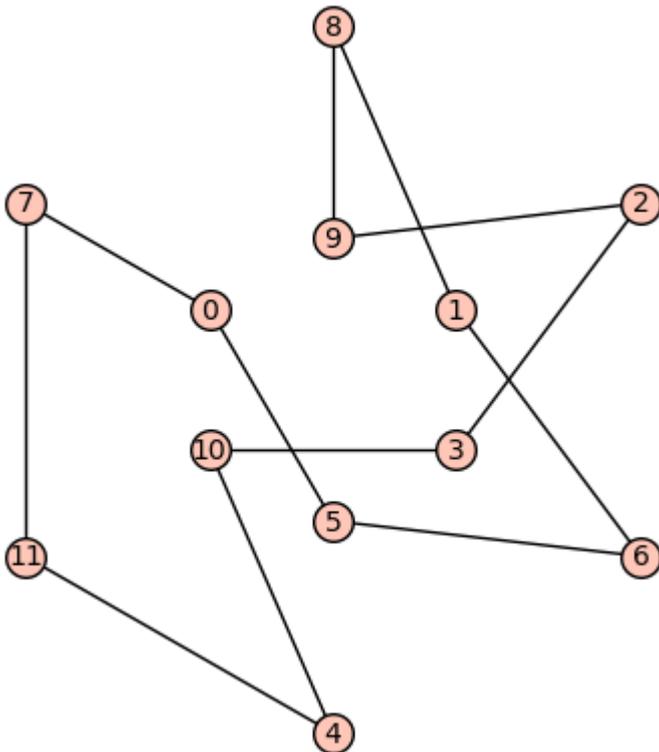
```
In [142... g20=graphs.IcosahedralGraph()
```

```
g20.show()
```



Hamiltonscher Kreis: Ein Kreis, der alle Knoten genau einmal enthält.

```
In [143...] g20.hamiltonian_cycle().show()
```



Eulertour: ein Kreis, der alle Kanten genau einmal durchläuft.

```
In [144...] g20.eulerian_circuit()
```

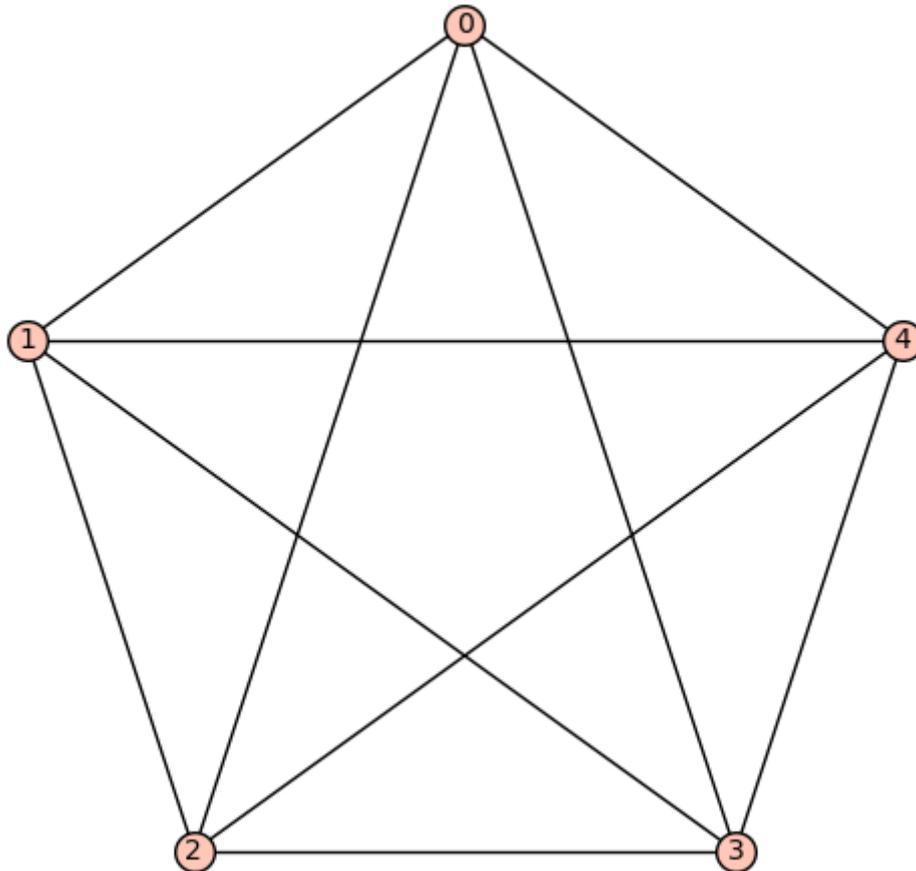
```
Out[144...] False
```

Der Ikosaedergraph hat also keine Eulertour.

Der vollständige Graph mit 5 Knoten. (D.h. alle möglichen Kanten existieren in dem Graphen)

```
In [145... k5=graphs.CompleteGraph(5)
k5
```

```
Out[145... Complete graph: Graph on 5 vertices
```



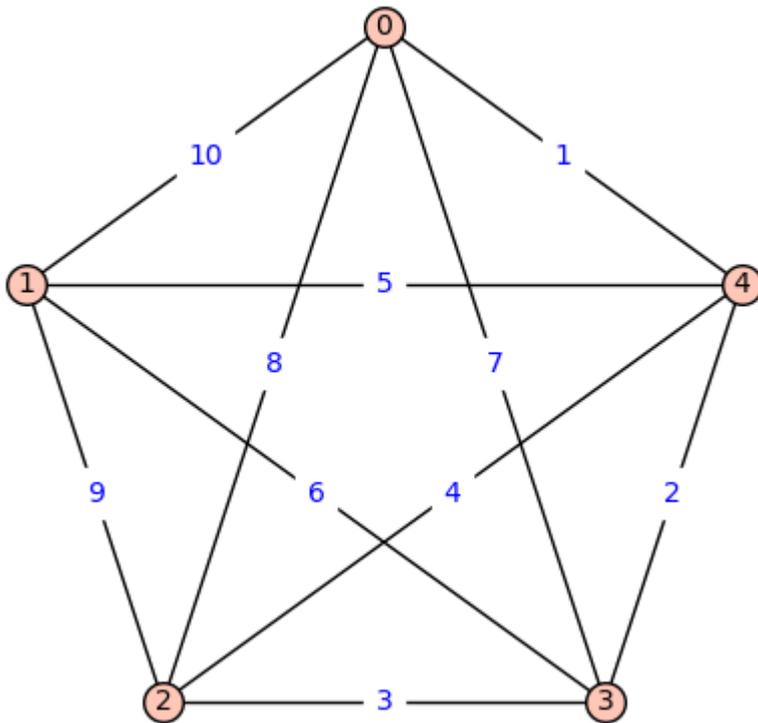
```
In [146... k5.eulerian_circuit()
```

```
Out[146... [(0, 4, None),
(4, 3, None),
(3, 2, None),
(2, 4, None),
(4, 1, None),
(1, 3, None),
(3, 0, None),
(0, 2, None),
(2, 1, None),
(1, 0, None)]
```

Darstellung der Eulertour im Bild des Graphen

```
In [147... for e,i in zip(k5.eulerian_circuit(),(1..)):
    k5.set_edge_label(e[0],e[1],i)
```

```
In [148... k5.show(edge_labels=True)
```



## Elliptische Kurven

```
In [149... 191.is_prime()
```

```
Out[149... True
```

```
In [150... E=EllipticCurve(GF(191),[-1,-1])
E
```

```
Out[150... Elliptic Curve defined by  $y^2 = x^3 + 190x + 190$  over Finite Field of size 191
```

```
In [151... E.order()
```

```
Out[151... 194
```

```
In [152... E.order().factor()
```

```
Out[152... 2 * 97
```

```
In [153... E.abelian_group()
```

```
Out[153... Additive abelian group isomorphic to  $Z/194$  embedded in Abelian group of points on Elliptic Curve defined by  $y^2 = x^3 + 190x + 190$  over Finite Field of size 191
```

```
In [154... P=E.random_element()
Q=E.random_element()
P,Q
```

```
Out[154... ((189 : 152 : 1), (115 : 50 : 1))
```

```
In [155... P+Q
```

Out[155... (22 : 104 : 1)

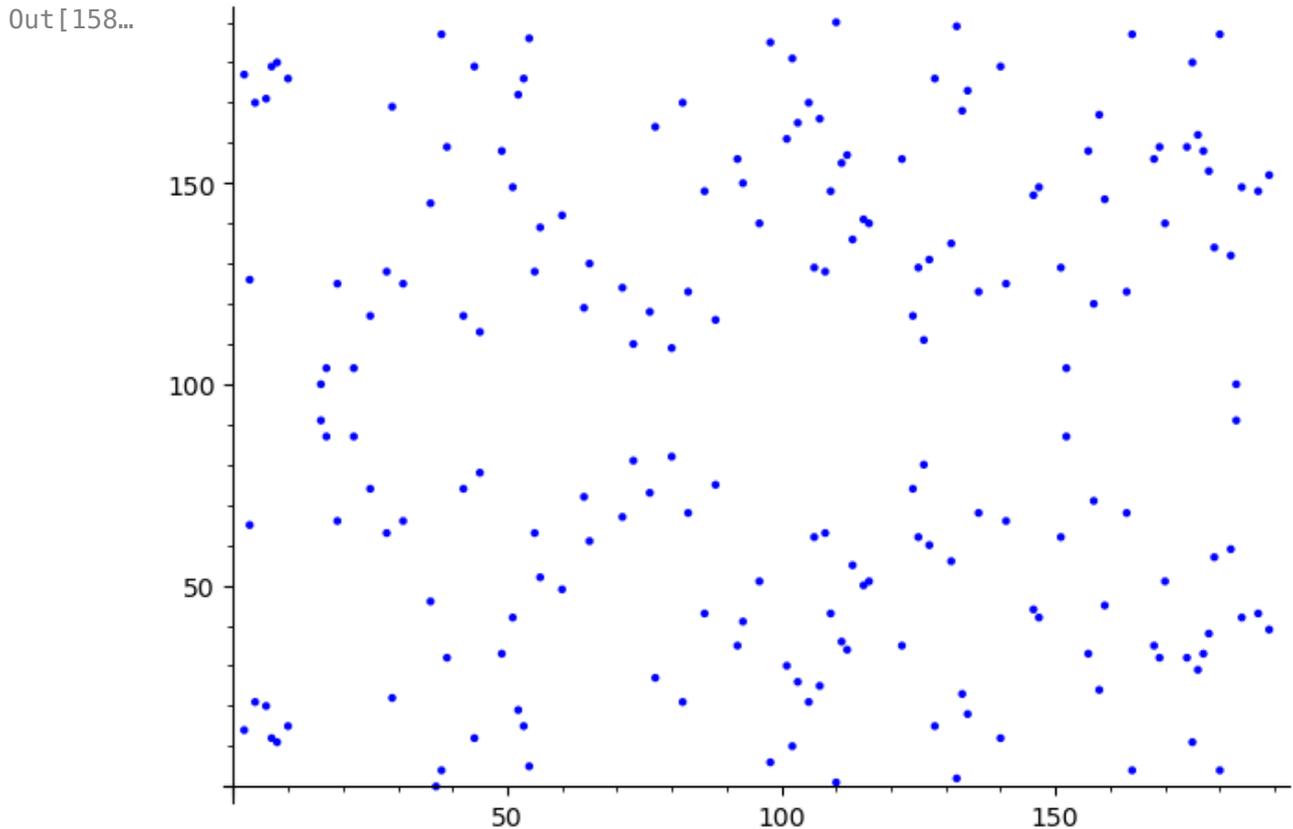
```
In [156... 2*P
```

Out[156... (102 : 181 : 1)

```
In [157... g=E.random_element()  
g, g.order()
```

Out[157... ((108 : 128 : 1), 194)

```
In [158... cp=E.plot()  
cp
```



```
In [159... @cached_function  
def ntimesg(n):  
    return cp + point([ZZ(c) for c in (n*g).xy()],pointsize=100,rgbcolor=
```

```
In [160... @interact  
def _(n=slider(1,g.order()-1,step_size=1)):  
    show(ntimesg(n),xmin=0,xmax=191,ymin=0,ymax=191)
```

Interactive function <function \_ at 0x7f80549dc900> with 1 widget  
n: TransformIntSlider(value=1, description='n', max=193, min=1)

```
In [161... # Hier ist ein Beispiel einer derzeit tatsächlich in der Kryptographie ve  
# Curve25519
```

```
In [162... p=2^255-19  
p.is_prime(), p
```

Out[162... (True,  
57896044618658097711785492504343953926634992332820282019728792003956564  
819949)

```
In [163... C=EllipticCurve(GF(p), [0, 486662, 0, 1, 0])  
C
```

Out[163... Elliptic Curve defined by  $y^2 = x^3 + 486662x^2 + x$  over Finite Field o  
f size 57896044618658097711785492504343953926634992332820282019728792003  
956564819949

```
In [164... C.order().factor()
```

Out[164...  $2^3 * 723700557733226221397318656304299424085711635937990760600195093828$   
5454250989

```
In [165... (C.order()).log(2).n()
```

Out[165... 255.0000000000000

```
In [168... P=C.lift_x(9)  
P
```

Out[168... (9 : 1478161944758954479102059356840998688726460613461647528896488183775  
5586237401 : 1)

```
In [169... ord=P.order()  
ord
```

Out[169... 723700557733226221397318656304299424085711635937990760600195093828545425  
0989

```
In [170... ord.is_prime()
```

Out[170... True

```
In [171... ord.log(2).n()
```

Out[171... 252.0000000000000

```
In [172... 2*P
```

Out[172... (14847277145635483483963372537557091634710985132825781088887140890597596  
352251 : 891461309122914783127793547204864306688006789925184041885518179  
3938505594211 : 1)

```
In [173... 4563452*P
```

Out[173... (31371633939913154697052398904246762625499846936057095673751569546807932  
907353 : 203913171366309912158989149084974831561902944060405335699927988  
3853399749039 : 1)