Sage 快速参考：抽象代数

B. Balof, T. W. Judson, D. Perkinson, R. Potluri

version 1.0, Sage Version 5.0.1
latest version: http://wiki.sagemath.org/quickref

Based on work by P. Jipsen, W. Stein, R. Beezer

基本帮助

com⟨tab⟩ 自动完成 *command*

a.⟨tab⟩ 对象a 的所有方法

<command>? 总结与范例

<command>?? 完整源代码

foo? 列出所有包含 *foo* 的命令

_ 下划线给出前一项输出

www.sagemath.org/doc/reference 在线参考文档

www.sagemath.org/doc/tutorial 在线手册

load foo.sage 载入文件foo.sage 中的命令

attach foo.sage
  自动载入 foo.sage 的变更

列表

`L = [2,17,3,17]` 有序列表

`L[i]` L 的第 i 个元素

注：列表元素索引从 0 开始记

`L.append(x)` L 中添加 x(至末尾)

`L.remove(x)` 从 L 中删除 x

`L[i:j]` L 的第 i 个元素到第 $(j-1)$ 个元素

`range(a)` 从 0 到 $a-1$ 的整数组成的列表

`range(a,b)` 从 a 到 $b-1$ 的整数组成的列表

`[a..b]` 从 a 到 b 的整数组成的列表

`range(a,b,c)`
  从 a 开始相差 c 的所有小于 b 的整数

`len(L)` L 的长度

`M = [i^2 for i in range(13)]`
  整数 0 到 12 的平方组成的列表

`N = [i^2 for i in range(13) if is_prime(i)]`
  0 和 12 之间的素数的平方组成的列表

`M + N` 列表M 和N 的毗连

`sorted(L)` L 的排序版本 (L 不会改变)

`L.sort()` 排序 L (L 会改变)

`set(L)` 每一个元素只出现一次的无序列表 (集合)

程序范例

输出整数 $0,\ldots,14$ 的平方:

```
for i in range(15):
    print i^2
```

输出 $\{0,\ldots,14\}$ 中与 15 互素的整数的平方:

```
for i in range(13):
    if gcd(i,15)==1:
        print i^2
```

基本运算

`a = 3; b = 14`

`gcd(a,b)` a,b 的最大公约数

`xgcd(a,b)`
  三元组 (d,s,t) 其中 $d=sa+tb$, $d=\gcd(a,b)$

`next_prime(a)` a 之后下一个素数

`previous_prime(a)` a 之前的上一个素数

`prime_range(a,b)` 满足 $a\le p<b$ 的素数 p

`is_prime(a)` a 是否是素数?

`b % a` b 被 a 除的余数

`a.divides(b)` a 是否整除 b?

群的构造

置换的乘法从左至右.

`G = PermutationGroup([[(1,2,3),(4,5)],[(3,4)]])`
  生成元为 $(1,2,3)(4,5)$ 与 $(3,4)$ 的置换群

`G = PermutationGroup(["(1,2,3)(4,5)","(3,4)"])`
  定义置换群的另一种语法

`S = SymmetricGroup(4)` 对称群 S_4

`A = AlternatingGroup(4)` 交错群 A_4

`D = DihedralGroup(5)` 10 阶二面体群

`Ab = AbelianGroup([0,2,6])` 交换群 $\mathbb{Z}\times\mathbb{Z}_2\times\mathbb{Z}_6$

`Ab.0, Ab.1, Ab.2` Ab 的生成元

`a,b,c = Ab.gens()`
  `a = Ab.0; b = Ab.1; c = Ab.2` 的缩写

`C = CyclicPermutationGroup(5)`

`Integers(8)` 群 $\mathbb{Z}_8$

`GL(3,QQ)` 3×3 可逆矩阵组成的一般线性群

`m = matrix(QQ,[[1,2],[3,4]])`

`n = matrix(QQ,[[0,1],[1,0]])`

`MatrixGroup([m,n])`
  生成元为 m 和 n 的 (无限) 矩阵群

`u = S([(1,2),(3,4)]);  v = S((2,3,4))` S 中的元素

`S.subgroup([u,v])`
  由 u 和 v 生成的 S 的子群

`S.quotient(A)` 商群 S/A

`A.cartesian_product(D)` 群的乘积 $A\times D$

`A.intersection(D)` 群的交 $A\cap D$

`D.conjugate(v)` 群的共轭 $v^{-1}Dv$

`S.sylow_subgroup(2)` S 的 Sylow 2 子群

`D.center()` D 的中心

`S.centralizer(u)` x 在 S 中的中心化子

`S.centralizer(D)` D 在 S 中的中心化子

`S.normalizer(u)` x 在 S 中的正规化子

`S.normalizer(D)` D 在 S 中的正规化子

`S.stabilizer(3)` 固定 3 的 S 的子群

群的运算

`S = SymmetricGroup(4); A = AlternatingGroup(4)`

`S.order()` S 中元素的个数

`S.gens()` S 的生成元系

`S.list()` S 中的元素

`S.random_element()` S 中随机元

`u*v` S 中 u 和 v 的乘积

`v^(-1)*u^3*v` S 中元 $v^{-1}u^3v$

`u.order()` u 的阶

`S.subgroups()` S 的所有子群

`S.normal_subgroups()` S 的所有正规子群

`A.cayley_table()` A 的乘法表

`u in S` u 是否是 S 中的元素?

`u.word_problem(S.gens())`
  将 u 写成 S 中生成元的乘积

`A.is_abelian()` A 是否交换?

`A.is_cyclic()` A 是否循环?

`A.is_simple()` A 是否为单群?

`A.is_transitive()` A 是否可迁?

`A.is_subgroup(S)` A 是否是 S 的子群?

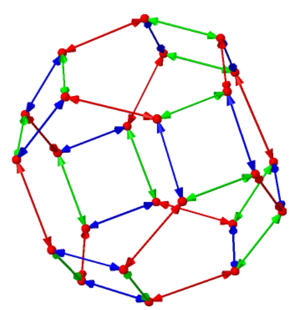
`A.is_normal(S)` A 是否是 S 的正规子群?

`S.cosets(A)` A 在 S 中的右陪集

`S.cosets(A,'left')` A 在 S 中的左陪集

`g = S.cayley_graph()` S 的 Cayley 图

`g.show3d(color_by_label=True, edge_size=0.01, vertex_size=0.03)` 如下:



环和域的构造

`ZZ` 整数 (整) 环, $\mathbb{Z}$
`Integers(7)` 整数模 7 剩余类环, $\mathbb{Z}_7$
`QQ` 有理数域, $\mathbb{Q}$
`RR` 实数域, $\mathbb{R}$
`CC` 复数域, $\mathbb{C}$
`RDF` 双精度域, 不精确
`CDF` 复双精度域, 不精确
`RR` 53-位实数, 不精确, 与`RDF`不同
`RealField(400)` 400-位实数, 不精确
`ComplexField(400)` 同上, 400-位复数
`ZZ[I]` Gaussian 整数环
`QuadraticField(7)` 二次域, $\mathbb{Q}(\sqrt{7})$
`CyclotomicField(7)`
包含 $\mathbb{Q}$ 和 x^7-1 的根的最小域
`AA, QQbar` 代数数域, $\overline{\mathbb{Q}}$
`FiniteField(7)` 有限域 $\mathbb{Z}_7$
`F.<a> = FiniteField(7^3)`
包含 7^3 个元素的有限域 (以 a 为本原元素), GF(7^3)
`SR` ring of symbolic expressions
`M.<a>=QQ[sqrt(3)]` 域 $\mathbb{Q}[\sqrt{3}]$, 其中 $a=\sqrt{3}$.
`A.<a,b>=QQ[sqrt(3),sqrt(5)]`
域 $\mathbb{Q}[\sqrt{3},\sqrt{5}]$, 其中 $a=\sqrt{3}$, $b=\sqrt{5}$.
`z = polygen(QQ,'z'); K = NumberField(x^2 - 2,'S')`
由多项式 x^2-2 定义的数域 (s 为该多项式的根)
`s = K.0` 令 s 为 K 的生成元
`D = ZZ[sqrt(3)]`
`D.fraction_field()`
整环 D 的分式域

环的运算

注: 运算取决于环的选择
`A = ZZ[I]; D = ZZ[sqrt(3)]` 环
`A.is_ring()` A 是否是环?
`A.is_field()` A 是否是域?
`A.is_commutative()` A 是否交换?
`A.is_integral_domain()`
`True` A 是否是整环?
`A.is_finite()` A 是否有限?
`A.is_subring(D)` A 是否是 D 的子环?
`A.order()` A 中元素的个数
`A.characteristic()` A 的特征
`A.zero()` A 的加法单位元
`A.one()` A 的乘法单位元
`A.is_exact()`
`False` 若 A 使用浮点表示
`a, b = D.gens(); r = a + b`
`r.parent()` r 属于哪个环 (这里是 D)
`r.is_unit()` r 是否为单位?

多项式

`R.<x> = ZZ[ ]` R 是多项式环 $\mathbb{Z}[x]$
`R.<x> = QQ[ ]; R = PolynomialRing(QQ,'x'); R = QQ['x']`
R 是多项式环 $\mathbb{Q}[x]$
`S.<z> = Integers(8)[ ]` S 是多项式环 $\mathbb{Z}_8[z]$
`S.<s, t> = QQ[ ]` S 是多项式环 $\mathbb{Q}[s,t]$
`p = 4*x^3 + 8*x^2 - 20*x - 24`
R $(=\mathbb{Q}[x])$ 中的多项式
`p.is_irreducible()` p 在 $\mathbb{Q}[x]$ 上是否不可约?
`q = p.factor()` 因式分解 p
`q.expand()` 展开 q
`p.subs(x=3)` 计算 p 在 $x=3$ 处的值
`R.ideal(p)` R 中由 p 生成的理想
`R.cyclotomic_polynomial(7)`
分圆多项式 $x^6+x^5+x^4+x^3+x^2+x+1$
`q = x^2-1`
`p.divides(q)` p 是否整除 q?
`p.quo_rem(q)`
p 除以 q 的商和余数
`gcd(p, q)` p 和 q 的最大公因式
`p.xgcd(q)` p 和 q 的扩充最大公因式
`I = S.ideal([s*t+2,s^3-t^2])`
S $(=\mathbb{Q}[s,t])$ 中的理想 $(st+2, s^3-t^2)$
`S.quotient(I)` 商环 S/I

域的运算

`A.<a,b>=QQ[sqrt(3),sqrt(5)]`
`C.<c> = A.absolute_field()`
"flattens" a relative field extension
`A.relative_degree()`
相对域扩张的次数
`A.absolute_degree()`
绝对扩张的次数
r = a + b; `r.minpoly()`
域中元素 r 的极小多项式
`C.is_galois()` C 是否是 Q 的 Galois 扩张?