Math 480 - April 16, 2008

Math 480 - April 16, 2008

Introductions...

1. **Who are you? (Name, major, interests).**
2. **Project idea? (Quick summary)**

New crypto seminar:

The seminar meets at 1:30pm on Thursdays in 415L Guggenheim (the Applied Math Building):

April 17, 2008: Reinier Broker -- Modular polynomials for genus 2

Modular polynomials are an important tool in many algorithms involving elliptic curves. In this talk we generalize this concept to the genus 2 case. We give the theoretical framework describing the genus 2 modular polynomials and discuss how to explicitly compute them.

Groups, Rings, and Fields

We are now starting the ``algebraic part" of this course on *Algebraic, Scientific, and Statistical Computing, an Open Source Approach Using Sage*. We will begin with some of the most basic objects in algebra, namely *groups*, *rings*, and *fields*. These are just as basic and important definitions as limit, derivative, and integral in analysis (Calculus), or standard deviation in statistics.

Groups

A **group** is a set G and a map $G \times G \to G$ that we'll denote $(a,b) \to a \cdot b$ such that

1. *Associativity:* For all $a, b, c \in G$ we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. *Identity element:* There exists an element $1_G \in G$ such that $1_G \cdot a = a \cdot 1_G = a$ for every $a \in G$.
3. *Inverse element:* For every $a \in G$ there is an element $b \in G$ such that $ab = 1_G$.

In addition, we say a group is *abelian* if every element commutes, i.e., for every $a, b \in G$ we have $a \cdot b = b \cdot a$. In this case, we often write $a + b$ instead of $a \cdot b$.

Below we give numerous examples of groups in Sage and compute with them, illustrating that they satisfy some of the group axioms.

Symmetric Group: The group of all permutations of 3 objects

```
S = SymmetricGroup(3); S
```

```
Symmetric group of order 3! as a permutation group
```

```
S.list()
```

```
[(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)]
```

Dihedral group D4 = group of symmetries of the square

```
D4 = DihedralGroup(4); D4
```

```
Dihedral group of order 8 as a permutation group
```

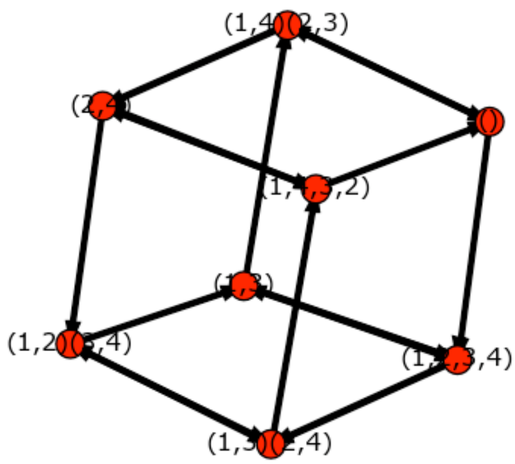
```
D4.list()
```

```
[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2),
(1,4)(2,3)]
```

```
D4.gens()
```

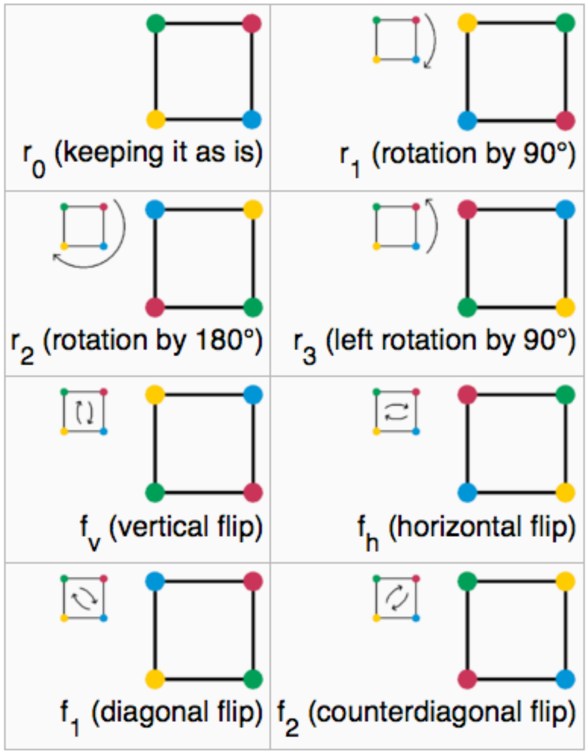
```
((1,2,3,4), (1,4)(2,3))
```

```
D4.cayley_graph().show()
```




```
D4.cayley_table()
```

```
[x0 x1 x2 x3 x4 x5 x6 x7]
[x1 x0 x3 x2 x5 x4 x7 x6]
[x2 x6 x0 x4 x3 x7 x1 x5]
[x3 x7 x1 x5 x2 x6 x0 x4]
[x4 x5 x6 x7 x0 x1 x2 x3]
[x5 x4 x7 x6 x1 x0 x3 x2]
[x6 x2 x4 x0 x7 x3 x5 x1]
[x7 x3 x5 x1 x6 x2 x4 x0]
```



From Wikipedia:

Abelian groups

```
A.<a,b> = AbelianGroup([3, 6]); A
```

```
Multiplicative Abelian Group isomorphic to C3 x C6
```

```
A.list()
```

```
[1, b, b^2, b^3, b^4, b^5, a, a*b, a*b^2, a*b^3, a*b^4, a*b^5, a^2,
a^2*b, a^2*b^2, a^2*b^3, a^2*b^4, a^2*b^5]
```

```
a*b*a*b*a
```

```
b^2
```

```
a*b == b*a
```

```
True
```

```
A.permutation_group().cayley_graph().show(vertex_labels=False)
```

```
Traceback (click to the left for traceback)
...
NameError: name 'A' is not defined
```

The Integers under addition are an infinite abelian group:

```
2 + 3 == 3 + 2
```

```
True
```

True

QUESTION: Is the set of integers under multiplication a group?

Integers modulo 12 form a group under addition:

```
R = Integers(12); R
```

```
Ring of integers modulo 12
```

```
R(7) + R(8)
```

```
3
```

```
R.list()
```

```
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11]
```

What about under multiplication? ...

```
R(5)*R(3)
```

```
3
```

The General Linear group of invertible 2×2 matrices with entries in $\{0,1\}$ modulo 2:

```
G = GL(2, GF(2)); G
```

```
General Linear Group of degree 2 over Finite Field of size 2
```

```
for g in G.list(): print g, '\n\n',
```

```
[0 1]
[1 0]

[0 1]
[1 1]

[1 0]
[0 1]

[1 0]
[1 1]

[1 1]
[0 1]

[1 1]
[1 0]
```

```
G = GL(3, GF(3)); G
```

```
General Linear Group of degree 3 over Finite Field of size 3
```

The center is the subgroup of elements that commute with everything else. In this case it is the scalar matrices:

```
G.center()
```

```
Matrix group over Finite Field of size 3 with 1 generators:
[[[2, 0, 0], [0, 2, 0], [0, 0, 2]]]
```

Galois groups motivated the definition of group in the first place

```
K = QQ[2^(1/3)]; K
```

```
Number Field in a with defining polynomial x^3 - 2
```

```
G = K.galois_group(); G
```

```
Galois group PARI group [6, -1, 2, "S3"] of degree 3 of the number
```

```
G.order()
```

```
Galois group PARI group [6, -1, 2, "S3"] of degree 3 of the number field Numbe
6
6
```

There are thousands of interesting and important theorems about groups, numerous invariants of groups that one might want to compute, etc., There are many books about them, courses, articles, and people have devoted their wholes professional lives to studying them. I won't go into any of this here.

```
# The ring of integers is a ring:
ZZ
```

```
Integer Ring
```

```
ZZ(3) * ZZ(7)
```

```
21
21
```

Rings

A **ring** (with unity) is a set R and maps $+ : R \times R \to R$ and $\cdot : R \times R \to R$ such that

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ satisfies all the properties of an abelian group, except possibly the existence of inverses.
3. *Distributive:* We have for every $a, b, c \in R$ that

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Below we give numerous examples of rings in Sage and compute with them, illustrating that they satisfy some of the group axioms.

```
3*(5+7) == 3*5 + 3*7
```

```
True
```

True

Are the set of primes a ring?

```
Primes()
```

```
Set of all prime numbers: 2, 3, 5, 7, ...
```

Set of all prime numbers: 2, 3, 5, 7, ...

Are the set of natural numbers a ring?

```
print '0,1,2,3,4,5, ...'
```

```
0,1,2,3,4,5, ...
```

```
R = Integers(12); R
```

```
Ring of integers modulo 12
```

```
is_Ring(R)
```

```
True
```

```
type(R)
```

```
<class 'sage.rings.integer_mod_ring.IntegerModRing_generic'>
```

```
5
```

```
5
```

```
2011 in Primes()
```

```
True
```

```
for p in Primes():
    if p > 1000: break
    print p
```

```
WARNING: Output truncated!
full_output.txt



2
3
5
7
11
13
17
19
23
29
31
37
41
43
47
53
59
61
67
71
73
79
83
89
97
101
103
107
109
113
127
131
137
139
149
151
157
163
167
173
179
181
191
193
197
199
211
223
227
229
233
239
241
251
257
263
269
271
277

...
```

```
599
601
607
613
617
619
631
641
643
647
653
659
661
673
677
683
691
701
709
719
727
733
739
743
751
757
761
769
773
787
797
809
811
821
823
827
829
839
853
857
859
863
877
881
883
887
907
911
919
929
937
941
947
953
967
971
977
983
991
997
```

full_output.txt

```
R.<x> = PolynomialRing(QQ); R
```

```
Univariate Polynomial Ring in x over Rational Field
```

```
(x^3 + x + 1/3)^3
```

```
x^9 + 3*x^7 + x^6 + 3*x^5 + 2*x^4 + 4/3*x^3 + x^2 + 1/3*x + 1/27
```

```
R.<x,y,z> = QQ[]; R
```

```
Multivariate Polynomial Ring in x, y, z over Rational Field
```

```
S.<T> = R[]
```

```
S
```

```
Univariate Polynomial Ring in T over Multivariate Polynomial Ring in
x, y, z over Rational Field
```

```
W.<AB, CD, EF> = S[]
```

```
W
```

```
Multivariate Polynomial Ring in AB, CD, EF over Univariate
Polynomial Ring in T over Multivariate Polynomial Ring in x, y, z
over Rational Field
```

```
f = (1+x+y+z)^20; g = f + 1; time h = f*g
```

```
Time: CPU 1.53 s, Wall: 1.61 s
```

```
len(str(h))
```

```
392385
```

```
R.<x,y,z> = QQ[]; R
```

```
Multivariate Polynomial Ring in x, y, z over Rational Field
```

```
S.<xbar,ybar,zbar> = R.quotient(x^2 + y^2 + z^2)
```

```
xbar^2 + ybar^2
```

```
-zbar^2
```

```
# Iterate this construction
T.<W> = R[]; T
```

```
Univariate Polynomial Ring in W over Multivariate Polynomial Ring in
```

```
(W + x - y)^2
```

```
Univariate Polynomial Ring in W over Multivariate Polynomial Ring in x, y, z o
W^2 + (2*x - 2*y)*W + x^2 - 2*x*y + y^2
```

W^2 + (2*x - 2*y)*W + x^2 - 2*x*y + y^2

As with groups, there are thousands of interesting and important theorems about rings, numerous invariants of ring that one might want to compute, etc.,

Fields

A **field** is a ring K such that $(K^*, \cdot)$ is also an abelian group, where K^* is the set of nonzero elements of K. This just means that for every nonzero $a \in K^*$ there is $b \in K^*$ such that $a \cdot b = 1_K$.

QUESTION: Is ZZ a field? .
Is Integers(12) a field? .

```
QQ
```

```
Rational Field
```

```
QQ(5)^(-1)
```

```
1/5
```

```
GF(7)
```

```
Finite Field of size 7
```

```
k.<alpha> = GF(4); k
```

```
Finite Field in alpha of size 2^2
```

In Sage, `CC` "models" the field of complex numbers in the computer. It is *not* really a field though. See the homework.

```
CC
```

```
Complex Field with 53 bits of precision
```

```
ComplexField(200)
```

```
Complex Field with 200 bits of precision
```

```
RR
```

```
Real Field with 53 bits of precision
```

```
RDF
```

```
Real Double Field
```

Real Double Field

The Gaussian rationals as a field:

```
K.<I> = QQ[sqrt(-1)]; K
```

```
Number Field in I with defining polynomial x^2 + 1
```

```
(1+2*I) / (3+4*I)
```

```
2/25*I + 11/25
```

```
R.<x> = QQ[]
K.<alpha> = NumberField(x^5 + 2*x + 1); K
```

```
Number Field in alpha with defining polynomial x^5 + 2*x + 1
```

```
alpha^5
```

```
-2*alpha - 1
```

```
R.<x> = QQ[]
R.is_field()
```

```
False
```

```
F = Frac(R); F
```

```
Fraction Field of Univariate Polynomial Ring in x over Rational
```

```
(2+3*x)/(17*x^3 + 3*x + 5)
```

```
Fraction Field of Univariate Polynomial Ring in x over Rational Field
(3*x + 2)/(17*x^3 + 3*x + 5)
```

Acknowledgement: Magma

The whole idea of really pushing groups, rings, fields, and other abstract often infinite or uncountable mathematical objects to be -- across the board -- **first class objects** in a computer algebr system owes a huge amount to the pioneering work done by John Cannon on the computer algebra systems Cayley and Magma. None of the big commercial systems such as Maple, Mathematica, or Matlab come anywhere close to what has been accomplished in Magma in this direction.

```
%magma
RationalField()
```

```
Rational Field
```

```
%magma
SymmetricGroup(3)
```

```
Symmetric group acting on a set of cardinality 3
```

```
%magma
R<x> := PolynomialRing(RationalField());
S<y,z,w> := PolynomialRing(R,3);
S
```

```
Polynomial ring of rank 3 over Univariate Polynomial Ring in x over
Rational Field
Lexicographical Order
```

```
%magma
(x+y+z+w)^2
```

```
y^2 + 2*y*z + 2*y*w + 2*x*y + z^2 + 2*z*w + 2*x*z + w^2 + 2*x*w +
```

```
%magma
Set(Integers(12))
```

```
{ 0, 11, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 }
```