Pries: M405 - Number Theory, Spring 2018

Week 8 Wednesday: Roots of unity and cyclotomic fields in SAGE
Let p be an odd prime.

1. Getting started:
   (a) Method 1: go to http://sagecell.sagemath.org/
   Method 2: (required for bigger jobs) start a free CoCalc account at http://www.sagemath.org/
   (b) Reference websites
   http://doc.sagemath.org/html/en/reference/number_fields/index.html
   http://doc.sagemath.org/pdf/en/reference/number_fields/number_fields.pdf

2. Polynomial factoring over the rationals
   (a) `R.<x> = QQ[]; R`
   (b) `f3=x^3-1; f3.roots();`
   (c) `plot(f3, -1,1.5);`
   (d) `f3=x^3-1; factor(f3);`
   (e) Repeat step d, replacing $p = 3$ by $p = 5$, then $p = 7$ until you see the pattern.
   (f) Make a conjecture: the factors of $gp = x^p - 1$ in $\mathbb{Q}[x]$ are:

3. The cyclotomic field
   (a) `K.<zeta> = CyclotomicField(3); K.degree();`
   (b) Evaluate these
   `CC(zeta), \zeta^3; \zeta^{3-1}; sum(zeta^i for i in range(0,3));`
   (c) Repeat (a,b), replacing $p = 3$ by $p = 5$, then $p = 7$ until you see the pattern.
   (d) Make a conjecture about ζ^p and $\sum_{i=0}^{p-1} \zeta^n$ and ζ^{p-1} for an arbitrary prime p.

4. Polynomial factoring over the cyclotomic field

   (a) K.<zeta> = CyclotomicField(3); S.<x> = K[];

   (b) f3=x^3-1; f3.roots();

   (c) f3=x^3-1; factor(f3);

   (d) Repeat step c, replacing $p = 3$ by $p = 5$, then $p = 7$ until you see the pattern.

   (e) Make a conjecture: the factors of $fp = x^p - 1$ in $K[x]$ are:

5. For $p = 3, 5, 7, 11$, determine if $\sqrt{p}$ is contained in the cyclotomic field $K. < zeta >$. What about $\sqrt{-p}$? Make a conjecture for all odd primes p. Here are some helpful commands.

```
L.<y> = K.extension(x^2-3); L.absolute\_degree();
```

6. Gauss sums

   (a) Type this:

```
def gauss_sum(a,p):
        K.<zeta> = CyclotomicField(p)
        return sum(legendre_symbol(n,p)*zeta^(a*n) for n in range(1,p))
```

   (b) g=gauss_sum(2,5); g;

   (c) g^2;

   (d) Repeat steps b,c for other choices of a, p (do not change the number 2 in step c).

   (e) Make a conjecture about how g^2 depends on a and p.