Algebraic number theory (Spring 2013), Homework 4

Frank Thorne, thornef@webmail.sc.edu

Due Wednesday, February 27

Recall that starred (*) exercises may involve background beyond what is assumed in this course.

Here crossed (+) exercises involve computer computations. Feel free to use any software you wish, but SAGE and PARI/GP are particularly well suited to doing computations in algebraic number theory. If you aren't familiar with either of these programs, now is a great time to learn them!

1. (5 points) Recall from HW 2, problem 8, we had the ideal factorization

$$(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

   Determine the norm of each of these ideals. Conclude, using multiplicativity of norms, that this is the unique factorization of (3) into prime ideals.

2. (5 points) By the Chinese Remainder Theorem, it is possible to find $x \in \mathbb{Z}[i]$ with $x \equiv 3 \pmod 7$, $x \equiv 1 \pmod{1+i}$, and $x \equiv i \pmod{2+i}$. Do so!

3. (5 points) In lecture we proved that, for $D \equiv 3 \pmod 4$, the *extremely important fact* that splitting of primes in quadratic extensions $\mathbb{Q}(\sqrt{D})$ is governed by whether or not p is a quadratic residue.

   What, if anything changes, when we remove the condition $D \equiv 3 \pmod 4$?

4. (+ 10 points) *If you would like to learn PARI/GP or SAGE, here are a few easy warmups:*

   Get an installation of PARI/GP, SAGE, or other software working, and compute:

   (a) The sum of the first hundred primes;

   (b) The average value of all the quadratic residues mod 97;

   (c) The number of roots of $x^{101} + x + 1$ mod 103.

5. (3 points) Suppose $K/\mathbb{Q}$ is a sextic field (i.e., it has degree 6 over $\mathbb{Q}$). Determine all possible splittings of primes p in $\mathcal{O}_K$.

   For example, you might have $(p) = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3$, where $f(\mathfrak{p}_1|p) = f(\mathfrak{p}_2|p) = 1$ and $f(\mathfrak{p}_3|p) = 1$. You could abbreviate this to $(1^2 1^2 2)$, where each exponent indicates the ramification index, and each base indicates the inertial degree.

   (You will have a long list.)

6. (5 points) Let K be the cubic field of discriminant -31 given by $x^3 + x - 1 = 0$. Either using a computer or by hand, find primes p which are inert (still prime), totally split (type (111)), partially split (type (21)), and ramified (type $(1^2 1)$).

7. (+: up to 25 points if done solo; or work in teams and credit will be divided.) This one is fun.

   In a previous exercise you enumerated all possible splitting types for sextic fields.

   Do they all actually occur? The e-f-g theorem rules everything out, but it doesn't tell you that every possible splitting type occurs.

   Determine, as best as you can, which of the splitting types occur in actual sextic fields. This is likely to require extensive trial and error using a computer program.

   Please be careful that you only look at sextic *fields*; don't take *reducible* sextic polynomials, factor them mod p, and expect this to tell you something interesting. Note that PARI/GP and SAGE can handle a lot of this automatically – there is functionality built in to handle number fields, to find their discriminants, and so on.

   In addition, observe which splitting types are the most common.

8. (+: up to 25 points; same rules as previous problem)

   Fun with cubic fields.

   Take a ton of cubic fields, sorted by discriminant. (You can download a data file from `http://hobbes.la.asu.edu/NFDB` which can be directly imported into a program.)

   (a) Pick your favorite prime, not 2 or 3. Then, find cubic fields in which this prime is totally split, inert, partially split, and ramified. (Note that this is sort of dual to a previous question.)

   (b) Pick any cubic field which does not have a square discriminant. Count the number of primes $p \leq X$, where X is some reasonably big number, for which p is totally split, inert, partially split, and ramified. What do the proportions look like?

   (c) Now pick a cubic field which *does* have a square discriminant. How does your calculation change? Can you explain why?

   (d) One simple thing you can do with these tables is to count all the cubic fields K with $|Disc(K)| < X$. Davenport and Heilbronn (1971) proved that the number of such fields is asymptotic to $\frac{1}{3\zeta(3)}X$, where $\zeta(3) = 1.202\cdots$ Does this match your data well?

   (e) Once again, picking some prime > 3, compute counts of cubic fields with $|Disc(K)| < X$ where this prime is totally split, inert, partially split, and ramified. Describe your data. Can you guess the relative proportions?