Homework 5

(due Friday Feb 12, 2016)

February 12, 2016

1 Problem 1

Prove that if $p^j \geq [K : \mathbf{Q}]$ then $I_p/pI_p \subset S/pS$ is the kernel of $x \mapsto x^{p^j}$.

[[If you can't figure it out, the proof is in Cohen's book (page 303). I'm fine if you read the proof, understand it, and write it down here in your own words. It's pretty short. I even scanned the relevant part of Cohen's book in and put it in the directory for the lecture for Feb 5.]]

1.1 proof

Recall we defined $I_p = \{x \in S : x^m \in pS, \quad m \geq 1\}$ so I_p/pI_p in S/pS is the nilradical. The claim follows from a more general lemma.

Lemma 1. *Let A be an n-dimensional k-algebra and $a \in \sqrt{0}$. Then $a^n = 0$.*

Proof. Let $a \in \sqrt{0}$ and consider the map $m_a : A \to A$ given by multiplication by a. This is a k-linear map so defines an element of $End_k(A)$. Moreover, $m_a^r = 0$ for some r by choice of a. Hence the minimal polynomial of m_a must divide X^r. By Cayley-Hamilton, the degree of the minimal polynomial is at most the degree of the characteristic polynomial, n. Hence the minimal polynomial divides X^n. Therefore multiplication by a^n is the zero map which implies $a^n = 0$. □

2 Problem 2

Prove that for any number field $K \neq \mathbf{Q}$ there is an order S in K so that we have to run the round 2 algorithm at least 100 times in order for it to terminate.

2.1 proof

The round 2 algorithm can change the index at p by at most p^n. If we start with an order S of K then the order T given by one run of the algorithm sits between $S \subseteq T \subseteq \frac{1}{p}S$. Therefore

$$[T : S] \leq [\frac{1}{p}S : S] = p^n.$$

The last equality is clear from the fact that $S \approx \mathbb{Z}^n$ as a $\mathbb{Z}$-module so $\frac{1}{p}S/S \approx (\mathbb{Z}/p\mathbb{Z})^n$.

So the claim follows by choosing an order with index at least p^{100n}. For example, in $\mathbb{Z}[i]$, if we choose the order $\mathbb{Z}[5^{200}i]$ then we would need to run at least 100 iterations of round 2. This is always possible. We can choose a primitive element which is integral α, and then take $\mathbb{Z}[p^{100n}\alpha]$.