Math 129 HW 10

Bryden Cais

May 2, 2002

Question 2:

1. Since L/K is a Galois extension of degree p, for any prime Q in L above P, we have

$$e(Q|P)f(Q|P)d(Q|P) = p.$$

   Since p is a prime in $\mathbb{Z}$, we see that one of e, f, d is p and the other two are 1. Therefore, P is inert or totally ramified or totally split in L.

2. Let $x = \pi^s y$ with $s \in \mathrm{N}$ and $y \notin P$. Suppose that $p \not| s$. Let Q be a prime above P in L. Then since $(\alpha)^p = P^s(y)$, we see that $Q|(\alpha)^P$ and hence $Q|(\alpha)$. Thus, $Q^p|(\alpha)^p$ so that $Q^p|P^s(y)$. Now since $y \notin P$, we must have $Q \not| y$, for if $y \in Q$ then $y \in R \cap Q = P$, a contradiction. Therefore, we see that $Q^p|P^s$. Since $(s,p) = 1$, we have $Q^p|P$. But then we must have $Q^p = P$ and P is totally ramified.

3. Now suppose that $s = 0$ so that $x = y \notin P$.

   (a) Suppose that $\bar{x} \in R/P^m$ is a p^{th} power but $\bar{x} \in R/P^{m+1}$ is not.

      i. Suppose that $m \leq p-1$ and let $\beta \in R$ be a solution to

$$u^p \equiv x \mod P^m.$$

      Now let $w = \beta - \alpha$, where $\alpha \in L$ is a root of $u^p - x = 0$. Since

$$\mathrm{N}_K^L(w) = \beta^p - x,$$

      we see that $P^m|\,\mathrm{N}_K^L(w)$. Therefore, $\gcd(P, w)$ is a R–ideal distinct from P (since if $P|w$ then $P^p|\,\mathrm{N}_K^L(w)$ and $< p$), that is, P is not prime. We know that if P splits it does so completely. We will show, however, that P splits completely if and only if $\bar{x} \in R/P^{p+1}$ is a p^{th} power, so that in this case, P does not split. Hence, sonce P is not prime and does not split, it must be totally ramified by part 1.

ii. Now suppose that $m = p$. As above, let $\beta \in R$ be a solution to $u^p \equiv x \mod P^m$, and let α be as before. For any $z \in P^{-1} - R$, set $w_z = z(\beta - \alpha)$, and observe that w_z is a root of

$$f(u) = (u - z\beta)^p + z^p x = 0 \tag{1}$$

Using the binomial theorem to expand the above polynomial, we obtain

$$(u - z\beta)^p + z^p x = u^p + \sum_{j=1}^{p-1} \binom{p}{j} u^{p-j} z^j - z^p(\beta^p - x).$$

Since $\binom{p}{j}$ is divisible by p and $P^{p-1} = p$, we see that $\binom{p}{j} z^j$ is integral for $1 \leq j \leq p-1$. Moreover, since $\beta^p - x \equiv 0 \mod P^p$, we see that $z^p(\beta^p - x)$ is integral. Therefore, $f(u) \in R[u]$, and as such, $w_z \in S$. Notice that

$$f'(w_z) = p w_z^{p-1}.$$

Since $P^{p-1} = p$ and $z \in P^{-1}$, we see that $f'(w_z) \notin P$. Since the different $\text{diff}_{L/K}$ is the ideal generated by $f'(\gamma)$ for all $\gamma \in S$, we see that $P \not| \text{diff}_{L/K}$ and hence $P \not| \text{disc}_{L/K}$.

iii. In the next problem, we will show that P splits in L if and only if $\bar{x} \in R/P^{p+1}$ is a p^{th} power. Hence, if $m > p$ then P splits completely since $\bar{x} \in R/P^{p+1}$ is a p^{th} power, so that by the next question, $\bar{x} \in R/P^l$ is a p^{th} power for all $l \geq 1$. This contradicts the assumption that $\bar{x} \in R/P^{m+1}$ is not a p^{th} power. Therefore, $m > p$ never happens.

(b) We show that if P splits in L then $\bar{x} \in R/P^m$ is a p^{th} power for all $m \geq 1$ and that if $\bar{x} \in R/P^{p+1}$ is a p^{th} power, then P splits completely. First suppose that P splits. We know that it must split completely, so we write $P = Q_1 \cdots Q_p$ for distinct primes Q_j of L. Moreover, we have $e(Q_j|P) = f(Q_j|P) = 1$. We show that the rings S/Q_1^m and R/P^m are equal for all $m \geq 1$. To do this, we show that $Q_1^m \cap R = P^m$ for all $m \geq 1$, from which it follows that R/P^m is a subring of S/Q_1^m for all m. Since $f(Q_1|P) = 1$, we have

$$|S/Q_1^m| = |S/Q_1|^m = |R/P|^m = |R/P^m|,$$

from which the equality follows. We proceed by induction. Certainly for $m = 1$ we have $Q_1 \cap R = P$. Now suppose the result holds for $m-1$. Then we have

$$P^m \subset Q_1^m \cap R \subset Q_1^{m-1} \cap R = subset P^{m-1}.$$

If we can show that $Q_1^m \cap R \neq P^{m-1}$ then we will be done since P is a prime ideal. But if $Q_1^m \cap R \neq P^{m-1}$, then $Q_1^m | P^{m-1}$ so that $e(Q_1|P) > 1$, which is false. This gives the claim. Now since S/Q_1^m and R/P^m are equal, there exists $\beta \in R$ with $\alpha \equiv \beta \mod Q_1^m$ for all $m \geq 1$ (where α is as before). Now take norms to obtain

$$\mathrm{N}_K^L(\alpha) \equiv \mathrm{N}_K^L(\beta) \mod \mathrm{N}_K^L(Q_1)^m,$$

that is,

$$\beta^p \equiv x \mod P^m,$$

as required.

Now suppose that we have a solution β to $u^p \equiv x \mod P^{p+1}$. As before, for any $z \in P^{-1} - R$, set $w = z(\beta - \alpha)$. Then w is a root of

$$f(u) = (u - z\beta)^p + z^p x = 0. \tag{2}$$

as are $w_j = z(\beta - \zeta^j \alpha)$ for $j = 1, 2, \ldots, p-1$ and $\zeta = e^{2\pi i/p}$. As before, $f(u) \in R[u]$ so that $w_j \in S$ for each j. Now set

$$Q_j = \gcd(PS, w_j S).$$

Certainly $Q_j \neq S$ for $0 \leq j \leq p-1$ since $\mathrm{N}_K^L(w_j) = z^p(\beta^p - x)$ is divisible by P by hypothesis. We claim that $Q_1 \cdots Q_p = P$. To see this, notice that from the definition of Q_j we have $P \subset Q_j$ for each j so that $Q_1 \cdots Q_p \supset P$. Moreover, since we can write

$$Q_j = \gamma_j + \delta_j w_j$$

for some $\gamma_j \in PS$ and $\delta_j \in S$, every element of $Q_1 \cdots Q_p$ is a sum of elements of the form

$$\prod_{j=0}^{p-1}(\gamma_j + \delta_j z(\beta - \zeta^j \alpha)) = \gamma + \delta z^p(\beta^p - x),$$

where $\gamma \in P$ and $\delta \in S$. Since $z^p(\beta^p - x) \in P$ by hypothesis, it follows that $Q_1 \cdots Q_p \subset P$, so that $Q_1 \cdots Q_p = P$ as claimed. Finally, the Q_j are either all distinct or all equal by part 1. But the latter possibility cannot hold since we showed above that $P \not| \operatorname{disc}_{L/K}$. Therefore, P splits completely.

4. We can now easily determine the behaviour of P in L. We know that P either totally splits or ramifies or it is inert. Moreover, we know that P splits completely if and only if $u^p \equiv x \mod P^{p+1}$ has a solution in R. Also, if P is not totally split but the congruence $u^p \equiv x \mod P^p$ has a solution in R then P is inert. If The above congruence $u^p \equiv x \mod P^p$ has no solution then P is totally ramified.

5. Suppose that $x \in R^*$.

   (a) Recall that $\operatorname{disc}_{L/K}$ divides $\operatorname{disc}(\alpha) = \mathrm{N}_K^L(p\alpha^{p-1}) = p^p x^{p-1}$. Since $x \in R^*$, the only primes dividing $\operatorname{disc}_{L/K}$ are those above p, that is, those primes of L above P (since P is the unique prime in K above P). Therefore, the extension L/K is unramified outside P.

   (b) If $L/\mathbb{Q}$ is Galois, then it is not difficult to see that we in fact have

   $$L = MK,$$

   where M is a degree p Galois extension of $\mathbb{Q}$ (this follows from the Galois correspondence, for example). Let P, π, Q be primes of K, M, L above p. Now we know that p totally ramifies in K so that $e(P|p) = p - 1$. We have shown that L/K is unramified outside of P and that $K/\mathbb{Q}$ is unramified outside of p. Consequently,

$L/\mathbb{Q}$ is unramified outside of p. If a prime $q \in \mathbb{Z}$ distinct from p ramified in M, it would ramify in L so that the only possible ramification in $M/\mathbb{Q}$ occurs at p. But *some* prime must ramify, so that p ramifies in L. Moreover, since $e(\pi|p)f(\pi|p)d(\pi|p) = p$, we see that $e(\pi|p) = p$ and p totally ramifies in L. Now $e(Q|p) = e(Q|P)e(P|p) = e(Q|\pi)e(\pi|p)$ so that $e(Q|p)$ is divisible by p and $p-1$. Since $(p, p-1) = 1$, we see that $e(Q|p) = p(p-1)$ and p is totally ramified in L so that P is totally ramified in L.

(c) If $x = \zeta$, then $L = \mathbb{Q}(\zeta^{1/p})$ is a cyclotomic field and hence Galois. Therefore, P ramifies in L so that $m \leq p-1$.

Question 3:

Suppose that there exists $x \in R^*$ that is conruent to a p^{th} power modulo P^p but is not a p^{th} power in R^*. Then $L = K(\sqrt[p]{x})$ is a nontrivial Galois field extension of degree p. Moreover, we know from question 2 part 3 that P does not ramify in L. By part 5 of question 2, L/K is unramified outside of P and is therefore an everywhere unramified Galois extension of degree p. If K has no such extensions, then we colclude that there can be no such x and hence that every $x \in R^*$ that is congruent to a p^{th} power in R^* modulo P^p is in fact a p^{th} power in R^*.