

### Answers to Homework 4, Math 5032

1. If  $K \subset L$  is an extension of finite fields, show that the norm map  $N_{L/K} : L^* \rightarrow K^*$  is onto. Deduce Hilbert 90, even though  $K$  may not contain the required roots of unity.

Let  $\#(K) = q$  a power of prime and let  $[L : K] = n$ . Then we know that  $L/K$  is cyclic Galois and the cyclic group is generated by  $\text{Fr}$ , the Frobenius,  $\text{Fr}(x) = x^q$ . Thus we see that  $N(x) = x^{1+q+q^2+\dots+q^{n-1}}$ . We have the following complex of cyclic groups,

$$1 \rightarrow K^* \xrightarrow{i} L^* \xrightarrow{\phi} L^* \xrightarrow{N} K^* \rightarrow 1,$$

where  $i$  is the natural inclusion,  $\phi(x) = \text{Fr}(x)/x$  and  $N$  is the norm. By calculating the orders of the various finite groups involved, it is immediate that Hilbert 90 will follow if  $N$  is surjective. Let  $x \in L^*$  be a generator of this cyclic group. Then let us compute the order of  $N(x) \in K^* \subset L^*$ . By our description above, since  $\text{ord}(x) = q^n - 1$ , it is immediate that  $\text{ord}(N(x)) = q - 1$ . Thus  $N(x)$  is a generator of  $K^*$  and thus  $N$  is surjective.

2. Using the fact that an odd prime  $p$  is a sum of squares if and only if it is  $p \equiv 1 \pmod{4}$ , prove that the cokernel of the norm map  $N : \mathbb{Q}(i)^* \rightarrow \mathbb{Q}^*$  is an infinite dimensional vector space over  $\mathbb{F}_2$ .

Since  $\mathbb{Q}^{*2} \subset N(\mathbb{Q}(i)^*)$ , we see that  $\mathbb{Q}^*/N(\mathbb{Q}(i)^*)$  is an abelian group with all elements of order at most 2 and thus it is an  $\mathbb{F}_2$  vector space. There are infinitely many primes of the form  $p \equiv 3 \pmod{4}$ . So, it suffices to show that for any such  $p_1, p_2, \dots, p_n$ , distinct,  $\prod p_i \notin N(\mathbb{Q}(i)^*)$ . From the assumed fact, this is easy to check.

3. An exact sequence from Galois cohomology. If  $G$  is a group (usually written multiplicatively) and  $A$  is an abelian group (usually written additively), we say that  $A$  is a  $G$ -module to mean that we are given an action of  $G$  on  $A$ , which is same as saying that  $A$  is a module over  $\mathbb{Z}[G]$ , the group ring. A homomorphism  $\phi : A \rightarrow B$  between two  $G$ -modules is a  $G$ -module homomorphism if  $\phi(ga) = g\phi(a)$  for all  $g \in G$  and  $a \in A$ .

- (a) If  $\phi : A \rightarrow B$  is a  $G$ -module homomorphism, show that there are natural induced homomorphisms (of abelian groups)  $\phi^* : H^i(G, A) \rightarrow H^i(G, B)$  for  $i = 0, 1$ .

Let  $x \in H^0(G, A)$ . By definition, then  $x \in A$  such that  $\sigma(x) = x$  for all  $\sigma \in G$ . But then

$$\sigma(\phi(x)) = \phi(\sigma(x)) = \phi(x)$$

and thus  $\phi(x) \in H^0(G, B)$ . We proceed similarly for  $H^1$ . Let  $\eta \in H^1(G, A)$ . Then  $\eta$  can be represented by a cocycle  $\{a_\sigma\}_{\sigma \in G}$ . One checks easily then  $\{\phi(a_\sigma)\}_{\sigma \in G}$  is a 1-cocycle in  $B$ . Next one checks

that if we started with a 1-coboundary in  $A$ , we would get a 1-coboundary in  $B$  and thus everything is well defined.

- (b) Let  $0 \rightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \rightarrow 0$  be an exact sequence of  $G$ -modules. Show that there exists a boundary homomorphism of abelian groups  $\partial : H^0(G, C) \rightarrow H^1(G, A)$  giving a long exact sequence,

$$0 \rightarrow H^0(G, A) \xrightarrow{i^*} H^0(G, B) \xrightarrow{\pi^*} H^0(G, C) \xrightarrow{\partial} H^1(G, A) \xrightarrow{i^*} H^1(G, B) \xrightarrow{\pi^*} H^1(G, C)$$

I will check one of these. Rest is similar. Recall the boundary map  $\partial$ . If  $c \in H^0(G, C) \subset C$ , let  $b \in B$  be such that  $\pi(b) = c$ . Then for any  $\sigma \in G$ ,  $\sigma(b) - b \in A$  and thus define  $\partial(c)$  by the 1-cocycle  $\{\sigma(b) - b\}_{\sigma \in G}$ . One easily sees that it is a well defined element in  $H^1(G, A)$ , independent of the choice of  $b$ . Now, let  $\partial(c) = 0$ . This means, the 1-cocycle defined above is a 1-boundary. That is, there exists an  $a \in A$  so that  $\sigma(b) - b = \sigma(a) - a$  for all  $\sigma \in G$ . Now consider  $b' = b - a$ . Then we have  $\sigma(b') = b'$  for all  $\sigma$  and thus  $b' \in H^0(G, B)$ . Further  $\pi(b') = \pi(b) - \pi(a) = c$  since  $\pi(a) = 0$ . Thus we see the exactness at that point.

4. Galois Theory for inseparable extensions: If  $L$  is a field, recall that a derivation  $D$  of  $L$  is an additive map  $D : L \rightarrow L$  with  $D(1) = 0$ , satisfying the Leibniz' rule, namely  $D(ab) = aD(b) + bD(a)$  for all  $a, b \in L$ . If  $K \subset L$  is a field extension, we say that a derivation  $D$  is a  $K$ -derivation, if  $D$  is  $K$ -linear. Let  $\mathfrak{D}_K(L)$  denote the set of all  $K$ -derivations of  $L$ , which is naturally an  $L$ -vector space.

- (a) Let  $L$  be a field of positive characteristic  $p$ . If  $D$  is a derivation of  $L$ , show that  $D(a^p) = 0$  for all  $a \in L$ .

Check by induction (using Leibniz) that  $D(a^n) = na^{n-1}D(a)$  and thus  $D(a^p) = pa^{p-1}D(a) = 0$  since characteristic is  $p$ .

- (b) Let  $\mathfrak{D}_K(L)$  be as above. Show that if  $D_1, D_2 \in \mathfrak{D}_K(L)$ , so is the bracket  $[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$ . (So that  $\mathfrak{D}_K(L)$  is a Lie Algebra over  $K$ ). Show that  $D_1^p \in \mathfrak{D}_K(L)$ . This property is called  $p$ -closedness. Thus  $\mathfrak{D}_K(L)$  is a  $p$ -closed Lie Algebra.

Clearly,  $[D_1, D_2]$  is  $K$ -linear. So, we only need to check that it satisfies the Leibniz rule.

$$\begin{aligned} [D_1, D_2](ab) &= D_1 D_2(ab) - D_2 D_1(ab) \\ &= D_1(aD_2(b) + bD_2(a)) - D_2(aD_1(b) + bD_1(a)) \\ &= aD_1 D_2(b) + D_1(a)D_2(b) + bD_1 D_2(a) + D_1(b)D_2(a) - \\ &\quad - aD_2 D_1(b) - D_2(a)D_1(b) - bD_2 D_1(a) - D_2(b)D_1(a) \\ &= a[D_1, D_2](b) + b[D_1, D_2](a) \end{aligned}$$

For the second part, use induction to check that,

$$D^n(ab) = \sum_{i=0}^n \binom{n}{i} D^i(a)D^{n-i}(b).$$

If  $n = p$ , one sees that  $\binom{p}{i} = 0$  for  $0 < i < p$ , since characteristic is  $p$  and thus we get,  $D^p(ab) = aD^p(b) + bD^p(a)$ , proving that  $D^p$  is a derivation.

- (c) Now assume that  $L^p \subset K$  (in view of the first exercise, derivations can not detect such elements anyway) where  $K \subset L$  is a finite extension. Let  $L = K(a_1, \dots, a_n)$ , where  $n$  is minimal. Show that  $\dim_L \mathfrak{D}_K(L) = n$  and  $[L : K] = p^n$ .

If  $E \subset E(a)$ , an extension of fields in characteristic  $p$  with  $a \notin E$  but  $a^p \in E$ , one easily checks that the irreducible polynomial of  $a$  over  $E$  is of the form  $X^p - a^p$ , since this polynomial has only one root in the algebraic closure, namely  $a$ . Thus it follows that  $E(a) \cong E[X]/(X^p - a^p)$  and in particular  $[E(a) : E] = p$ . Now, by induction it is clear that  $[L : K] = p^n$  where  $L, K, n$  are as above. Also  $L \cong K[X_1, \dots, X_n]/I$  where  $I$  is the ideal generated by the polynomials  $X_i^p - a_i^p$ . Thus any element in  $L$  can be expressed as  $f(a_1, \dots, a_n)$  where  $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ . Given any  $n$  elements  $b_1, \dots, b_n \in L$ , one can define an element  $D = D_{b_1, \dots, b_n} \in \mathfrak{D}_K(L)$  by

$$D(f(a_1, \dots, a_n)) = \sum \frac{\partial f}{\partial X_i}(a_1, \dots, a_n) \cdot b_i.$$

One checks that this is well defined. Thus one has  $\dim_L \mathfrak{D}_K(L) \geq n$ . Further, if  $T \in \mathfrak{D}_K(L)$ , then one easily checks that  $T = D_{b_1, \dots, b_n}$  where  $b_i = T(a_i)$  and thus we get the equality.

- (d) Conversely, let  $\mathfrak{D}$  be a finite dimensional (over  $L$ ) vector space of  $p$ -closed Lie algebra of derivations of  $L$ . Show that if we define  $K = \{a \in L \mid D(a) = 0 \forall D \in \mathfrak{D}\}$  then  $K \subset L$  is a subfield and it is a finite extension,  $L^p \subset K$  and  $\mathfrak{D} = \mathfrak{D}_K(L)$ .

If we define  $K$  as above and  $x, y \in K$ , clearly  $x + y \in K$  since for any  $D \in \mathfrak{D}$ ,  $D(x + y) = Dx + Dy = 0$ . Similarly,  $D(xy) = xDy + yDx = 0$  and thus  $xy \in K$ . If  $x \neq 0$ , then  $D(x^{-1}) = -\frac{Dx}{x^2} = 0$ . Thus  $K$  is a subfield of  $L$ . Also, for any  $x \in L$  and  $D \in \mathfrak{D}$ ,  $D(x^p) = 0$  and so  $L^p \subset K$ .

The last part is more delicate. I suggest you look up Jacobson's book Basic Algebra, vol 2, page 534 (Jacobson's theorem).

5. We have seen in class that if  $K$  is a field and  $n$  a positive integer which is not divisible by the characteristic of  $K$  and  $\omega$  is a primitive  $n^{\text{th}}$  root of 1, then  $K(\omega)$  is an abelian extension of  $K$  with Galois group a subgroup of  $(\mathbb{Z}/n\mathbb{Z})^*$ .

- (a) In the above assume that  $n = p$  is a prime. Show that the Galois group is cyclic.

This is obvious, since then the Galois group is a subgroup of the cyclic group  $(\mathbb{Z}/p\mathbb{Z})^*$ .

- (b) Let  $K$  be any field,  $p$  any prime and  $a \in K$ . Show that if the polynomial  $X^p - a$  is not irreducible over  $K$  then it has a root in  $K$ . (Hint: If  $p =$  the characteristic of  $K$ , this is trivial. If not, use the previous part.)

In characteristic  $p$ , we have already seen this in the previous problem, since  $X^p - a$  has only one root in the algebraic closure. So, let us assume that  $p$  is not the characteristic, so that if  $a \neq 0$  (which we can assume),  $X^p - a$  is a separable polynomial. Let  $b$  be a root of  $f(X) = X^p - a$  and  $\omega$  a primitive  $p^{\text{th}}$  root of 1. Then the splitting field of  $f$  is  $K(\omega, b)$ . If  $f$  is not irreducible over  $K$ , surely it is not irreducible over  $L = K(\omega)$ . Since  $f = \prod_{i=0}^{p-1} (X - \omega^i b)$ , if it is not irreducible, the constant term of this factor must be  $\prod \omega^{i_k} b$  for some integers  $0 \leq i_k < p$ , but not all. Thus we see that  $\omega^l b^m \in L$  for some  $l$  and  $1 \leq m < p$ . Since  $\omega^l \in L$ , we see that  $b^m \in L$ . But  $b^p = a \in L$  and since  $p, m$  are relatively prime, we see that  $b \in L$ .

$L/K$  is a cyclic extension of degree  $m$  dividing  $p-1$ . For any  $\sigma$  in the Galois group of  $L/K$ , we must have  $\sigma(b) = \omega^r b$  and thus we see that  $N(b) = \omega^l b^m \in K$  for some  $l$ . Since  $m, p$  are relatively prime, we can write  $1 = am + cp$  for some integers  $a, c$ . So, we have  $\omega^{al} b^{am} \in K$  and  $b^{pc} = a^c \in K$ . Multiplying, we get,  $\omega^{al} b \in K$ . But this is a root of  $f$ .