Student seminar solutions Week 10

1. *Looking at the proof of Lemma* 4.1 *in the book of Childress, construct the function* δ_1*, prove it is well-defined and prove that* $im(\delta_1) = ker(f_0)$*.*

   Proof. We recall that we have a short exact sequence of G-modules

   $$0 \to B \xrightarrow{f} A \xrightarrow{g} C \to 0$$

   We also recall the construction of $\delta_1 : H^1(C) \to H^0(B)$ as in the book of Childress. Let $c \in ker_C\ s(G)$. Since g is surjective, there exists $a_1 \in A$ such that $g(a_1) = c$. But since $c \in ker_C\ s(G)$, we have

   $$0 = s(G)(g(a_1)) = g(s(G)(a_1))$$

   so that $s(G)(a_1) \in ker(g) = im(f)$. Then there exists $b_1 \in B$ with $f(b_1) = s(G)(a_1)$. Now

   $$\begin{aligned} 0 &= (\sigma - 1)s(G)(a_1) \\ &= (\sigma - 1)f(b_1) \\ &= f((\sigma - 1)(b_1)) \end{aligned}$$

   Hence, by injectivity of f we get $(\sigma - 1)(b_1) = 0$ so that $b_1 \in ker_B\ (\sigma - 1)$. So we may define

   $$\delta_1(c + (\sigma - 1)C) = b_1 + s(G)B$$

   Let's check that δ_1 is well-defined. Suppose $c + (\sigma - 1)C = c' + (\sigma - 1)C$ in $H^1(C)$. Repeating the abovee for c', we obtain

   $$\begin{aligned} &a_1' \in A \text{ with } g(a_1') = c', \text{ and} \\ &b_1' \in B \text{ with } f(b_1') = s(G)(a_1') \end{aligned}$$

   It suffices to show that

   $$b_1 - b_1' \in s(G)B$$

   We have that $c - c' \in (\sigma - 1)C$ and since g is surjective, there exists $a \in A$ such that

   $$c - c' = (\sigma - 1)(g(a)) = g((\sigma - 1)(a))$$

   Also

   $$c - c' = g(a_1) - g(a_1') = g(a_1 - a_1')$$

Thus

$$g(a_1 - a_1' - (\sigma - 1)(a)) = 0$$

So that $a_1 - a_1' - (\sigma - 1)(a) \in ker(g) = im(f)$. But now there exists $b \in B$ with

$$f(b) = a_1 - a_1' - (\sigma - 1)(a)$$

Hence

$$\begin{aligned} s(G)f(b) &= s(G)(a_1 - a_1' - (\sigma - 1)(a)) \\ &= f(b_1) - f(b_1') \end{aligned}$$

So that

$$f(s(G)(b)) = f(b_1 - b_1')$$

And by injectivity of f we get that

$$b_1 - b_1' \in s(G)B$$

as wanted.
Now that we know that δ_1 is well-defined, let's show that $im(\delta_1) = ker(f_0)$. First let $c \in ker_c\ s(G)$, we have

$$\begin{aligned} f_0(\delta_1(c + (\sigma - 1)C)) &= f_0(b_1 + s(G)B) \\ &= f(b_1) + s(G)A \\ &= s(G)a_1 + s(G)A \\ &= s(G)A \end{aligned}$$

So $im(\delta_1) \subseteq ker(f_0)$. Now let $b + s(G)B \in ker(f_0)$, it means that $f(b) \in s(G)A$. Hence there exists $a \in A$ suvh that $f(b) = s(G)(a)$. Define $c = g(a) \in C$, and oberve that

$$s(G)(c) = s(G)(g(a)) = g(s(G)(a)) = g(f(b)) = 0$$

so that $c \in ker_C\ (\sigma - 1)$, and by definition

$$\delta_1(c + (\sigma - 1)C) = b + s(G)B$$

So $ker(f_0) \subseteq im(\delta_1)$ and then

$$im(\delta_1) = ker(f_0)$$

□

2. If A, B are G-modules such that their Herbrand quotient exist, show that

$$\mathcal{Q}_G(A \times B) = \mathcal{Q}_G(A)\mathcal{Q}_G(B)$$

Proof. Let $x \in \mathbb{Z}[G]$, and denote also by x the left multiplication by x in either A, B or $A \times B$, which is G-module map. Obseve that

$$\begin{aligned} ker_{A\times B}(x) &= \{(a,b) \in A \times B \mid x(a,b) = (0,0)\} \\ &= \{(a,b) \in A \times B \mid xa = 0,\ xb = 0\} \\ &= ker_A(x) \times ker_B(x) \end{aligned}$$

Similarly

$$\begin{aligned} im_{A\times B}(x) &= \{x(a,b) \mid (a,b) \in A \times B\} \\ &= \{(xa, xb) \mid (a,b) \in A \times B\} \\ &= im_A(x) \times im_B(x) \end{aligned}$$

So we get

$$\begin{aligned} \mathcal{Q}_G(A \times B) &= \frac{\big[ker_{A\times B}(\sigma - 1) : im_{A\times B}s(G)\big]}{\big[ker_{A\times B}s(G) : im_{A\times B}(\sigma - 1)\big]} \\ &= \frac{\big[ker_A(\sigma - 1) \times ker_B(\sigma - 1) : im_As(G) \times im_Bs(G)\big]}{\big[ker_As(G) \times ker_Bs(G) : im_A(\sigma - 1) \times im_B(\sigma - 1)\big]} \\ &= \frac{\big[ker_A(\sigma - 1) : im_As(G)\big]\ \big[ker_B(\sigma - 1) : im_Bs(G)\big]}{\big[ker_As(G) : im_A(\sigma - 1)\big]\ \big[ker_Bs(G) : im_B(\sigma - 1)\big]} \\ &= \mathcal{Q}_G(A)\, \mathcal{Q}_G(B). \end{aligned}$$

□

3. Let K/F be a Galois extension of number fields with Galois group G.

   (a) Let $v \in V_F$ be a place of F. Prove that G acts transitively on the set $\{w \mid v\}$ of places of K lying above v.

   (b) Check that the action of G on J_K coincides with the usual action of G on $K^\times$.

   (c) Let $v \in V_F$ and fix a place $w \mid v$. Show that the map

   $$Gal(K_w/F_v) \longrightarrow G, \qquad \sigma \longmapsto \sigma|_K$$

   is an isomorphism onto the subgroup $G_w = \{\tau \in G \mid \tau(w) = w\}$ of G.

Proof. (a) Assume for contradiction that the action is not transitive. Then there exist two places $w, w' \mid v$ lying in distinct G-orbits. Thus the sets

$$\{\sigma(w) : \sigma \in G\}, \qquad \{\sigma(w') : \sigma \in G\}$$

are disjoint.

By the Approximation Theorem, we may choose an element $\alpha \in K^\times$ satisfying

$$||\sigma(\alpha)||_w < 1 \qquad \text{and} \qquad ||\sigma(\alpha)||_{w'} > 1 \qquad \text{for all } \sigma \in G.$$

But then

$$||N_{K/F}(\alpha)||_w < 1 < ||N_{K/F}(\alpha)||_{w'}$$

which is absurd because $N_{K/F}(\alpha) \in F$ and $w|_F = v = w'|_F$. Therefore, the assumption that w and w' lie in distinct orbits is impossible, and the action of G on the places above v must be transitive.

(b) Let $\iota : K^\times \to J_K$ be the inclusion given by $\iota(\alpha) = (\alpha)_{w \in V_K}$. Then for $v \in V_F$ $\iota(\alpha)_{w|v} = (\alpha)_{w|v}$ and the action by $\sigma \in G$ is given by

$$\sigma \cdot (\alpha)_{w|v} = (\sigma(\alpha))_{w|v}$$

So we get

$$\sigma \cdot \iota(\alpha) = \iota(\sigma(\alpha))$$

as wanted.

(c) Let $v \in V_F$ and fix a place $w \mid v$ of K. Consider the map

$$Gal(K_w/F_v) \longrightarrow G, \qquad \tau \longmapsto \tau|_K,$$

where $Gal(K_w/F_v)$ denotes the group of F_v-automorphisms of the local field K_w. By definition, these automorphisms fix F_v. Moreover, since K_w/F_v is a finite extension of complete fields, every automorphism is automatically continuous with respect to the w-adic topology: this is because any field automorphism fixing the base field F_v is F_v-linear and linear maps on finite-dimensional normed vector spaces are continuous.

If $\tau \in Gal(K_w/F_v)$, then $\tau|_K$ is an automorphism of K fixing F, hence an element of $G = Gal(K/F)$. Since τ is continuous and preserves the w-adic valuation, we have

$$w(\tau(x)) = w(x) \qquad \text{for all } x \in K_w^\times.$$

This shows that $\tau|_K$ fixes the place w, because a place is determined by the valuation it induces. Hence

$$\tau|_K \in G_w := \{\sigma \in G : \sigma(w) = w\},$$

and the restriction map lands in G_w.

Suppose $\tau \in Gal(K_w/F_v)$ restricts to the identity on K. Since K is dense in K_w and τ is continuous, τ must act trivially on all of K_w. Hence $\tau = id$, so the map is injective.

Let $\sigma \in G_w$. Then σ is a field automorphism of K fixing F and satisfying $\sigma(w) = w$. Because σ preserves the valuation corresponding to w, it is continuous for the w-adic topology on K. Since K is dense in K_w, any continuous map from K extends uniquely to a continuous automorphism of the completion K_w. Thus σ extends to an element $\widetilde{\sigma} \in Gal(K_w/F_v)$ whose restriction to K is σ, which proves surjectivity.
Since the map is injective with image G_w, we conclude that

$$Gal(K_w/F_v) \;\cong\; G_w.$$

□

4. Recall Hilbert's Theorem 90 from class: For any cyclic Galois extension of fields K/F with Galois group G and any map $f : G \to K^\times$ satisfying

$$f(\tau\sigma) = \tau(f(\sigma))\, f(\tau),$$

there exists some $\alpha \in K^\times$ such that

$$f(\sigma) = \frac{\sigma(\alpha)}{\alpha}, \qquad \text{for all } \sigma \in G.$$

Use this to show:

(a) There is an exact sequence of abelian groups

$$1 \longrightarrow F^\times \longrightarrow K^\times \longrightarrow ker(N_{K/F}) \longrightarrow 1.$$

(b) Deduce that the norm map is surjective for an extension of finite fields.

Proof. (a) Assume K/F is cyclic with generator $\sigma \in Gal(K/F)$ of order n. Observe firstly that $F^\times \to K^\times$ is clearly injective since it is just the inclusion of $F^\times$ into $K^\times$. We define

$$\varphi : K^\times \to ker(N_{K/F}), \quad \varphi(\alpha) = \frac{\alpha}{\sigma(\alpha)}$$

We have for any $\alpha \in K^\times$ that

$$N_{K/F}\left(\frac{\alpha}{\sigma(\alpha)}\right) = \prod_{i=0}^{n-1} \sigma^i\left(\frac{\alpha}{\sigma(\alpha)}\right) = \frac{\prod_{i=0}^{n-1} \sigma^i(\alpha)}{\prod_{i=0}^{n-1} \sigma^{i+1}(\alpha)} = 1$$

because G is cyclic. So φ is well defined, and clearly it is a group morphism because σ is a group morphism.
It remains to show that $ker(\varphi) = F^\times$ and that φ is surjective.
If $\varphi(\alpha) = 1$ it means that $\alpha = \sigma(\alpha)$, so α is fixed by σ and hence by

the whole Galois group since it is a generator, so $\alpha \in F^\times$. Conversely any $\alpha \in F^\times$ is fixed by σ, so $\varphi(\alpha) = 1$. Thus $ker(\varphi) = F^\times$.
Let $b \in K^\times$ such that $N_{K/F}(b) = 1$. Define a map

$$f : G \longrightarrow K^\times, \qquad f(\sigma^i) = \prod_{j=0}^{i-1} \sigma^j(b),$$

with the convention that the empty product $f(1)$ is equal to 1. We check that f is a 1-cocycle. For any $i, k \in \{0, \ldots, n-1\}$ we have

$$f(\sigma^{i+k}) = \prod_{j=0}^{i+k-1} \sigma^j(b) = \Big(\prod_{j=0}^{i-1} \sigma^j(b)\Big)\Big(\prod_{j=i}^{i+k-1} \sigma^j(b)\Big) = f(\sigma^i)\,\sigma^i\big(f(\sigma^k)\big)\,,$$

so $f(\tau\sigma) = \tau(f(\sigma))\, f(\tau)$ for all $\tau, \sigma \in G$. Thus Hilbert's Theorem 90 applies, and there exists $\alpha \in K^\times$ such that

$$f(\tau) = \frac{\tau(\alpha)}{\alpha}, \qquad \text{for all } \tau \in G.$$

But $f(\sigma) = b$, so $b = \sigma(\alpha)/\alpha = \varphi(\alpha^{-1})$. Therefore b lies in the image of φ, proving that φ is surjective.
We have shown that $\ker(\varphi) = F^\times$ and that φ is surjective onto $\ker(N_{K/F})$. This yields the desired short exact sequence

$$1 \longrightarrow F^\times \longrightarrow K^\times \xrightarrow{\varphi} ker(N_{K/F}) \longrightarrow 1.$$

(b) Let $\mathbb{F}_{q^n}/\mathbb{F}_q$ be a finite extension of finite fields. This extension is Galois with cyclic Galois group generated by the Frobenius automorphism

$$\sigma : x \mapsto x^q.$$

By the previous result, for any cyclic Galois extension K/F we have the short exact sequence

$$1 \longrightarrow F^\times \longrightarrow K^\times \xrightarrow{\varphi} ker(N_{K/F}) \longrightarrow 1,$$

where $\varphi(\alpha) = \alpha/\sigma(\alpha)$ and $N_{K/F}$ is the field norm.
Applying this to $K = \mathbb{F}_{q^n}$ and $F = \mathbb{F}_q$, we obtain that φ is surjective onto $\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})$. Since $K^\times$ is a finite group, the exactness of the sequence implies

$$|\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| = \frac{|K^\times|}{|F^\times|} = \frac{q^n - 1}{q - 1}.$$

But the image of the norm is a subgroup of $F^\times$, and we have

$$|F^\times| = q - 1.$$

Since $|K^\times| = |ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| \cdot |im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})|$, we obtain

$$|im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})| = \frac{q^n - 1}{|\ker(N_{\mathbb{F}_{q^n}/\mathbb{F}_q})|} = q - 1 = |F^\times|.$$

Hence $im(N_{\mathbb{F}_{q^n}/\mathbb{F}_q}) = F^\times$. In other words, the norm map

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$$

is surjective.

□