Graduate Algebra
Homework 11

Due 2015-04-29

1. Let $\mathbb{C}(x^{1/\infty}, y^{1/\infty}) = \cup_{m,n\geq 1}\mathbb{C}(x^{1/m}, y^{1/n})$.

   (a) Show that $\mathbb{C}(x^{1/\infty}, y^{1/\infty})$ is Galois over $\mathbb{C}(x, y)$.

   (b) Compute $\mathrm{Gal}(\mathbb{C}(x^{1/\infty}, y^{1/\infty})/\mathbb{C}(x, y))$.

   Proof. (a): It suffices to show that $\mathbb{C}(x^{1/m}, y^{1/n})$ is Galois over $\mathbb{C}(x, y)$. But it is the splitting field of $(T^m - x)(T^n - y)$ and so is normal. Separability follows from characteristic 0.

   (b): $\sigma \in \mathrm{Gal}(\mathbb{C}(x^{1/\infty}, y^{1/\infty})/\mathbb{C}(x, y))$ takes $x^{1/m}$ to $\zeta_m^a x^{1/m}$ and $y^{1/n}$ to $\zeta_n^b y^{1/n}$ and we see that $\mathrm{Gal}(\mathbb{C}(x^{1/m}, y^{1/n})/\mathbb{C}(x, y)) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Moreover, $\mathbb{C}(x^{1/m}, y^{1/n}) \subset \mathbb{C}(x^{1/M}, y^{1/N})$ iff $m \mid M$ and $n \mid N$ and then the natural projection $\mathrm{Gal}(\mathbb{C}(x^{1/M}, y^{1/N}), \mathbb{C}(x, y)) \to \mathrm{Gal}(\mathbb{C}(x^{1/m}, y^{1/n})/\mathbb{C}(x, y))$ is the natural projection map $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

   Finally,

   $$\mathrm{Gal}(\mathbb{C}(x^{1/\infty}, y^{1/\infty})/\mathbb{C}(x, y)) \cong \varprojlim \mathrm{Gal}(\mathbb{C}(x^{1/m}, y^{1/n})/\mathbb{C}(x, y)) \cong \varprojlim \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}} \times \widehat{\mathbb{Z}}$$

   as the projection maps in the definition of $\widehat{\mathbb{Z}}$ are precisely the natural residue projection maps. □

2. Let L/K be a Galois extension and let $\{M_k | k \in I\}$ be a collection of subextensions $L/M_k/K$ such that M_k/K is finite Galois and $L = \bigcup M_k$. Show that $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(M_k/K)$.

   Proof. Consider the natural projection map

   $$\Phi : \varprojlim_{L/\underbrace{M/K}_{\text{finite Galois}}} \mathrm{Gal}(M/K) \to \varprojlim \mathrm{Gal}(M_k/K)$$

   simply by taking the tuple (σ_M) to the tuple (σ_{M_k}). This is clearly a homomorphism $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(M/K) \to \varprojlim \mathrm{Gal}(M_k/K)$. If $\Phi(\sigma) = 1$ and $\alpha \in L$ let k be such that $\alpha \in M_k$. Then $\Phi(\sigma)(\alpha) = \sigma|_{M_k}(\alpha) = \alpha$ and so $\sigma(\alpha) = \alpha$. We deduce that $\sigma = 1$ and so Φ is injective.

   For surjectivity suppose $(\sigma_k) \in \varprojlim \mathrm{Gal}(M_k/K)$. Let M/K be any finite Galois extension. Then $M = K(\alpha_1, \ldots, \alpha_m)$ and there exists k large enough such that M_k contains $\alpha_1, \ldots, \alpha_m$. Thus $M \subset M_k$ and define $\sigma_M = \sigma_k|_M$. This yields $(\sigma_M) \in \varprojlim \mathrm{Gal}(M/K)$ and clearly $\Phi((\sigma_M)) = (\sigma_k)$. □

3. Suppose $L_1, L_2/K$ are two (possibly infinite) Galois extensions. Show that L_1L_2/K and $L_1 \cap L_2/K$ are Galois and

   $$\mathrm{Gal}(L_1L_2/K) \cong \{(\sigma, \tau) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) | \sigma|_{L_1\cap L_2} = \tau|_{L_1\cap L_2}\}$$

   [Hint: Use the previous problem.]

Proof. That $L_1 \cap L_2/K$ is Galois follows as in the finite case, the proof of which did not use finiteness. Every element $x \in L_1L_2$ is a finite rational expression in elements $\alpha_1, \ldots, \alpha_p \in L_1$ and $\beta_1, \ldots, \beta_q \in L_2$. Thus $x \in K(\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q)$ and so x is separable over K. We deduce that L_1L_2/K is separable. Finally, suppose $P(X) \in K[X]$ be irreducible with a root $x \in L_1L_2$. As before this implies that $P(X)$ has a root $x \in K(\alpha_1, \ldots, \alpha_p)K(\beta_1, \ldots, \beta_q)$. Let M/K be the splitting field of the product of the minimal polynomials of $\alpha_1, \ldots, \alpha_p$ and N/K be the splitting field of the product of the minimal polynomials of $\beta_1, \ldots, \beta_q$. This shows that M/K and N/K are normal and since L_1/K and L_2/K are normal we deduce that $M \subset L_1$ and $N \subset L_2$. But then MN/K is normal and MN contains x and $MN \subset L_1L_2$. Since MN/K is normal every root of P is then in MN and therefore in L_1L_2. We deduce that L_1L_2/K is normal and therefore Galois.

Consider the collection $\{M_i\}$ of all subextensions of L_1/K which are finite Galois over K and $\{N_j\}$ of all subextensions of L_2/K which are finite Galois over K. Then $\{M_iN_j\}$ is some collection of subextensions of L_1L_2/K which are finite Galois over K and certainly $L_1L_2 = \bigcup M_iN_j$. Using the previous problem

$$\begin{aligned}
\mathrm{Gal}(L_1L_2/K) &\cong \varprojlim \mathrm{Gal}(M_iN_j/K) \\
&\cong \varprojlim \{(\sigma, \tau) \in \mathrm{Gal}(M_i/K) \times \mathrm{Gal}(N_j/K) | \sigma|_{M_i \cap N_j} = \tau|_{M_i \cap N_j}\} \\
&\subset \varprojlim \mathrm{Gal}(M_i/K) \times \mathrm{Gal}(N_j/K) \\
&\cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)
\end{aligned}$$

But $(\sigma, \tau) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ is in

$$\varprojlim \{(\sigma, \tau) \in \mathrm{Gal}(M_i/K) \times \mathrm{Gal}(N_j/K) | \sigma|_{M_i \cap N_j} = \tau|_{M_i \cap N_j}\}$$

if and only if for each M_i and N_j one has

$$\sigma|_{M_i \cap N_j} = \tau|_{M_i \cap N_j}$$

But $L_1 \cap L_2 = \bigcup M_i \cap N_j$ so this condition is equivalent to $\sigma|_{L_1 \cap L_2} = \tau|_{L_1 \cap L_2}$ and the conclusion follows. $\square$

4. Show that $H^n(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q), \mathbb{F}_{q^d}^\times) = 0$ if $n \geq 1$.

   Proof. Let $\phi(x) = x^q$ be the generator of $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. Write $N = 1 + \phi + \cdots + \phi^{d-1}$ act multiplicatively on $\mathbb{F}_{q^d}^\times$ by $N(x) = x\phi(x)\phi^2(x) \cdots \phi^{d-1}(x) = x^{1+q+\cdots+q^{d-1}}$. Then from class if $n \geq 1$ then

$$H^n(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q), \mathbb{F}_{q^d}^\times) \cong \begin{cases} (\mathbb{F}_{q^d}^\times)^{N=1}/\operatorname{Im}(\phi - 1) & n \text{ odd} \\ (\mathbb{F}_{q^d}^\times)^{\phi=\mathrm{id}}/\operatorname{Im} N & n \text{ even} \end{cases}$$

   But $(\mathbb{F}_{q^d}^\times)^{\phi=\mathrm{id}} = (\mathbb{F}_{q^d}^\times)^{\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)} = \mathbb{F}_q^\times$ from the main theorem of Galois theory. Also, $\operatorname{Im} N = \{x^{1+q+\cdots+q^{d-1}} | x \in \mathbb{F}_{q^d}^\times\}$. Let g be a generator of the cyclic group $\mathbb{F}_{q^d}^\times$. Then $\operatorname{Im} N = \langle g^{1+q+\cdots+q^{d-1}} \rangle$. Since $\mathrm{ord}(g^{1+q+\cdots+q^{d-1}}) = (q^d - 1)/(1 + q + \cdots + q^{d-1}) = q - 1$ it follows that $\langle g^{1+q+\cdots+q^{d-1}} \rangle \cong \mathbb{F}_q^\times$ and thus $\operatorname{Im} N = \mathbb{F}_q^\times$. Immediately we deduce that $H^n = 0$ when n is even.

   Also if $N(x) = 1$ then $x^{1+q+\cdots+q^{d-1}} = 1$ and so $x \in \langle g^{q-1} \rangle$. Note that $(\phi - 1)(x) = x^{q-1}$ whose image is clearly $\langle g^{q-1} \rangle$. We deduce that $H^n = 0$ when n is odd as well. $\square$

5. Let $H \subset G$ be finite groups and N an H-module.

   (a) Let $\mathrm{Ind}_H^G N = \{f : G \to N | f(hg) = h(f(g)), \forall g \in G, h \in H\}$. For $g \in G$ and $f \in \mathrm{Ind}_H^G N$ define $g(f) : G \to N$ by $g(f)(x) = f(xg)$. Show that this yields an action on $\mathrm{Ind}_H^G N$ which turns $\mathrm{Ind}_H^G N$ into a G-module.

(b) Thinking of N as a $\mathbb{Z}[H]$-module and $\mathrm{Ind}_H^G N$ as a $\mathbb{Z}[G]$-module show that $\mathrm{Ind}_H^G N \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$ as $\mathbb{Z}[G]$-modules. Here $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$ is a $\mathbb{Z}[G]$-module via the scalar multiplication $[g]([h] \otimes n) = [gh] \otimes n$. [Hint: Show that the map $f \mapsto \sum_{g \in H\backslash G} [g^{-1}] \otimes f(g)$ is well-defined and yields the isomorphism.]

(c) If M is a G-module show that $\mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathrm{Ind}_H^G N) \cong \mathrm{Hom}_{\mathbb{Z}[H]}(M, N)$. [Hint: Take $f : M \to \mathrm{Ind}_H^G N$ to $m \mapsto f(m)(1)$ and $\phi : M \to N$ to $m \mapsto (g \mapsto \phi(g(m)))$.]

Proof. (a): We need to check that $g(h(f)) = (gh)(f)$. But $g(h(f))(x) = g(f)(xh) = f(xgh) = (gh)(f)(x)$. The action clearly commutes with the natural abelian group structure on the space of functions in $\mathrm{Ind}_H^G N$.

(b): For $f \in \mathrm{Ind}_H^G N$ let $\Phi(f) = \sum_{g \in H\backslash G} [g^{-1}] \otimes f(g)$. To show that $\Phi(f)$ is well-defined we need only show that it is independent of choices of representatives of $H\backslash G$ in G. But if $g' = hg$ are representatives for the same coset in $H\backslash G$ then $[(g')^{-1}] \otimes f(g') = [g^{-1}h^{-1}] \otimes f(hg) = [g^{-1}][h^{-1}] \otimes h(f(g)) = [g^{-1}] \otimes f(g)$ as $[h^{-1}] \in \mathbb{Z}[H]$. Finally, Φ is additive trivially and so Φ is a homomorphism $\mathrm{Ind}_H^G N \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$.

Next, every element of $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$ is of the form $\sum_{g \in G} [g^{-1}] \otimes n_g$ as $\mathbb{Z}[G]$ is free over $\mathbb{Z}$. Fix once and for all representatives in G of the cosets $H\backslash G$. Rewrite this as

$$\sum_{g \in G} [g^{-1}] \otimes n_g = \sum_{g \in H\backslash G} \sum_{h \in H} [(hg)^{-1}] \otimes n_{hg} = \sum_{g \in H\backslash G} [g^{-1}] \otimes (\sum_{h \in H} h(n_g)) = \sum_{g \in H\backslash G} [g^{-1}] \otimes f_g$$

Note that $\mathbb{Z}[G] \cong \oplus_{g \in H\backslash G} g^{-1}\mathbb{Z}[H]$ is a free $\mathbb{Z}[H]$-module. Thus $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N \cong \oplus_{g \in H\backslash G} g^{-1}\mathbb{Z}[H] \otimes_{\mathbb{Z}[H]} N$ and so the expression $\sum_{g \in H\backslash G} [g^{-1}] \otimes f_g$ uniquely determines the f_g.

Since the f_g are uniquely determined we may define $f : G \to N$ by $f(g) = f_g$. Again this is a homomorphism of abelian groups and clearly it is the inverse of Φ. Thus $\Phi : \mathrm{Ind}_H^G N \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$ is an isomorphism of $\mathbb{Z}$-modules. To check that it is an isomorphism of $\mathbb{Z}[G]$-modules it suffices to show that for $h \in G$, $\Phi(hf) = h\Phi(f)$.

$$\Phi(hf) = \sum_{g \in H\backslash G} [g^{-1}] \otimes (hf)(g) = \sum_{g \in H\backslash G} [g^{-1}] \otimes f(gh) = \sum_{g' = gh \in H\backslash G} [h(g')^{-1}] \otimes f(g') = h\Phi(f)$$

as multiplication by h permutes $H\backslash G$.

(c): Suppose $f : M \to \mathrm{Ind}_H^G N$ is $\mathbb{Z}[G]$-linear. Let $\Phi(f) = (m \mapsto f(m)(1))$. This is a map $M \to N$ that is clearly $\mathbb{Z}$-linear. Suppose $h \in H$. We need to check that it is h-linear, i.e., that $\Phi(f)(h(m)) = h(\Phi(f)(m))$. But f is h-linear so

$$\Phi(f)(h(m)) = f(h(m))(1) = h(f(m))(1) = f(m)(h) = h(f(m)(1))$$

as $h \in H$ and $f(m) \in \mathrm{Ind}_H^G N$. Thus we get a map $\Psi : \mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathrm{Ind}_H^G N) \to \mathrm{Hom}_{\mathbb{Z}[H]}(M, N)$. From definitions it is linear in f and thus Φ is a homomorphism.

Now suppose $\phi : M \to N$ is H-linear and define $\Psi(\phi) = (m \mapsto (g \mapsto \phi(g(m))))$. Note that for $h \in H, g \in G$

$$\Psi(\phi)(m)(hg) = \phi(hg(m)) = h(\phi(g(m))) = h(\Psi(\phi(m)(g)))$$

as ϕ is h-linear. Thus $\Psi(\phi)(m) \in \mathrm{Ind}_H^G N$. The map $\Psi(\phi)$ is linear in m and thus we get a $\mathbb{Z}$-linear homomorphism $\Psi(\phi) : M \to \mathrm{Ind}_H^G N$. We need to heck that $\Psi(\phi)$ is G-linear. Suppose $h \in G$.

$$\Psi(\phi)(h(m))(g) = \phi(g(h(m))) = \phi((gh)(m)) = \Psi(\phi)(m)(gh) = h(\Psi(\phi)(m))(g)$$

Finally, note that Ψ is linear in ϕ and so $\Psi : \mathrm{Hom}_{\mathbb{Z}[H]}(M, N) \to \mathrm{Hom}_{\mathbb{Z}[G]}(M, \mathrm{Ind}_H^G N)$ is a homomorphism.

Note that $\Psi(\Phi(f))(m)(g) = \Phi(f)(g(m)) = f(g(m))(1) = g(f(m))(1) = f(m)(g)$ and $\Phi(\Psi(\phi))(m) = \Psi(\phi)(m)(1) = \phi(m)$ and so Φ and Ψ are mutual inverses yielding an isomorphism.

$\square$