Topics In Algebra, Homework 6

John Hower, Charlie Scherer, Nathan Wakefield

April 28, 2010

Problem (4)**.** *Let E and F be fields such that $E = F(\sqrt{\alpha})$ for some $\alpha \in F$ and suppose that $G := \mathrm{Gal}(E/F)$ is non-trivial (this happens if and only if α is a non-square in F and E/F is separable).*

1. *$H^2(G, E^*) \cong F^*/N$ where $N = \{u^2 - \alpha v^2 : u, v \in F^*\}$.*
2. *If $E/F = \mathbb{C}/\mathbb{R}$ then $H^2(G, E^*) = \mathbb{Z}_2$.*
3. *If $E/F = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ then $H^2(G, E^*)$ is infinite.*

Proof. For clarity, the action of G on E^* will be denoted by $\cdot$, the multiplication in G will be denoted by $\times$ and the multiplication in E will be denoted by juxtaposition.

1. Clearly $|G| = 2$ so let $G = \{1, \gamma\}$. Recall that $H^2(G, A) \cong Z^2(G, A)/B^2(G, A)$ where $Z^2(G, A)$ is the group of normalized 2-cocycles and $B^2(G, A)$ is the group of normalized 2-coboundaries. Also recall that if $g : G^n \to E^*$ is any n-cochain then g is entirely determined by $g(\gamma, ..., \gamma)$ since applying g to every other tuple gives 1. So let $g_{n,e}$ be the unique n-cochain such that $g_{n,e}(\gamma, ..., \gamma) = e$.

   Consider $g \in Z^2(G, A)$. It must be that for all $x, y, z \in G$ we have

   $$(x \cdot g(y, z))(g(x \times y, z))^{-1} g(x, y \times z)(g(x, y))^{-1} = 1$$

   but the left hand side of this equation always defines a 3-cochain so the only restriction it imposes is

   $$\gamma \cdot g(\gamma, \gamma) = g(\gamma, \gamma)$$

   because $g(\gamma \times \gamma, \gamma) = g(1, \gamma) = 1 = g(\gamma, 1) = g(\gamma, \gamma \times \gamma)$. Thus, $g = g_{2,e}$ for some $e \in E^*$ such that $\gamma e = e$. But then e is fixed by every element of G and since E/F is Galois this means $e \in F$. Ergo, the map $F^* \to Z^2(G, A)$ such that $f \mapsto g_{2,f}$ is surjective. It is also manifestly injective for if $f \neq f'$ then $g_{2,f} \neq g_{2,f'}$ since these two maps take on a different value at (γ, γ). Finally, for any $f, f' \in F$ we have $g_{2,f} g_{2,f'} = g_{2,ff'}$ since $(g_{2,f} g_{2,f'})(\gamma, \gamma) = g_{2,f}(\gamma, \gamma) g_{2,f'}(\gamma), \gamma$. Thus, $F^* \cong Z^2(G, A)$.

   Now take $g \in B^2(G, A)$. We must have $g(x, y) = (x \cdot f(y))(f(x \times y))^{-1} f(x)$ for some normalized 1-cochain $f : G \to G$. But since f is normalized it follows

   $$g(\gamma, \gamma) = (\gamma \cdot f(\gamma)) f(\gamma)$$

   because $f(\gamma \times \gamma) = f(1) = 1$. Now $f(\gamma) = u + \sqrt{\alpha} v$ for some $u, v \in F$ and it must be that $\gamma(\sqrt{\alpha}) = -\sqrt{\alpha}$ so

   $$g(\gamma, \gamma) = (u - \sqrt{\alpha})(u + \sqrt{\alpha}) = u^2 - \alpha v^2$$

   Therefore, $g = g_{2,u^2 - \alpha v^2}$. So as before the map $N \to B^2(G, A)$ is an isomorphism.

   Ergo, $Z^2(G, A)/B^2(G, A) \cong F^*/N$.

2. Note that in the case $E = \mathbb{R}(\sqrt{-1}) = \mathbb{C}$ we have $N = \{u^2 + v^2 : u, v \in \mathbb{R}^*\}$. On the one hand $u^2 + v^2 > 0$ for all $u, v \in R^* = R \setminus \{0\}$. On the other hand if $x > 0$ then $\sqrt{x/2} \neq 0$ so taking $u = v = \sqrt{x/2}$ gives $u^2 + v^2 = x$. Hence, $N = \mathbb{R}^+$. Now for any $x \in \mathbb{R}^*$, $xN = (x/|x|)N$ because $1/|x| \in N$. So $\mathbb{R}^*/N = \{N, -1N\}$.

3. Recall (or find out for the first time) that $x^2 \equiv 2 \pmod{p}$ has no solutions for infinitely many primes p. Therefore, let $P := \{p \in \mathbb{Z}^+ : p \text{ is prime and } x^2 \equiv 2 \pmod{p} \text{ has no solution}\}$. Define a sequence p_k inductively as follows. Let $p_0 = 1$. If p_k has already been defined take $p \in P$ such that $p > p_k$ and put $p_{k+1} = pp_k$. Note that $p_k | p_{k+1}$ for all k and consequently $p_j | p_k$ for all $j \leq k$.

   We want to show that $p_k p_j^{-1} \notin N$ for all $j \neq k$. Once this is done it will follow $\{p_k N : k \in \mathbb{N}\}$ is a collection of infinitely many distinct cosets in $\mathbb{Q}^*/N$. Towards a contradiction suppose that $p_k p_j^{-1} \in N$ for some $j \neq k$. Without loss of generality we may take $j < k$. Then there is some $p \in P$ such that $p_k p_j^{-1} = p\frac{p_{k-1}}{p_j}$ and since $j \leq k-1$ it follows $m := \frac{p_{k-1}}{p_j}$ is an integer satisfying $p > p_{k-1} \geq m \geq 1$. So in particular $(p, m) = 1$. Now the condition that $p_k p_j^{-1} \in N$ means that there are $u, v, x, y \in \mathbb{Z}$ with $(u, v) = (x, y) = 1$ such that

$$pm = (u/v)^2 - 2(x/y)^2$$

   which after rearranging becomes

$$pm(vy)^2 = (uy)^2 - 2(xv)^2 \tag{1}$$

   If $p \nmid xv$ then $(uyx^{-1}v^{-1})^2 \equiv 2 \pmod{p}$ contrary to the choice of p. So either $p|x$ or $p|v$. Now if $p|x$ then since $p|((uy)^2 - 2(xv)^2)$ it follows $p|uy$. As $(x, y) = 1$ this means $p|u$. But also note that $p|x$ and $p|u$ means p^2 divides both sides of (1). Since $(p, m) = 1$ this can only happen if $p|vy$. Then either $p|v$ or $p|y$ but this can not happen because p divides both x and u and $(x, y) = (u, v) = 1$. Hence $p \nmid x$.

   Consider the case $p|v$. Write $v = v'p^a$ where $(v', p) = 1$. Then (1) becomes

$$pm(v'y)^2 p^{2a} = (uy)^2 - 2(xv')^2 p^{2a}$$

   so that $p^{2a}|(uy)^2$. Since $(u, v) = 1$ this can only happen if $p^a|y$. By cancelling a factor of p^{2a} from both sides of (1) we get

$$pm(v'y)^2 = (uy')^2 - 2(xv')^2$$

   But now $p \nmid xv'$ so that $(uy'(xv')^{-1})^a \equiv 2 \pmod{2}$ which is again impossible.

   Ergo $pm = (u/v)^2 - 2(x/y)^2$ has no solutions and it follows $p_k p_j^{-1} = pm \notin N$.

□