

Problem Set 5 for Math 250, Fall 2006.

Due on Wednesday, November 1.

This problem set is a little bit harder, so you get more time to do it.

1. Look up the quadratic reciprocity law in a book if you can't remember it. Let p be an odd prime.
 - (a) Show that the splitting field E of $x^p - 1 \in \mathbb{Q}[x]$ over \mathbb{Q} contains a unique subfield K of degree 2 over \mathbb{Q} , and identify K in the form $\mathbb{Q}[\sqrt{d}]$.
 - (b) Let $\omega \in E$ be a primitive p -th root of unity, and let $q \neq p$ be another odd prime. Study the action of the element $\sigma \in \text{Gal}(E/\mathbb{Q})$ defined by $\sigma(\omega) = \omega^q$. Use this to prove the quadratic reciprocity law (for odd primes). (Hint: compute the action of σ on \sqrt{d} in two ways. It may be useful to first restrict σ to $\mathbb{Z}[\omega]$, and obtain an induced action of σ on $\mathbb{F}_q[\omega]$.)

2. Let G and G' be finite groups, M a G -module and M' a G' -module.

- (a) Suppose $a : G' \rightarrow G$ and $b : M \rightarrow M'$ are two homomorphisms (of groups). We say that a and b are *compatible* if $g \cdot b(m) = b(a(g) \cdot m)$ for all $g \in G'$ and $m \in M$. If $\phi \in C^r(G, M)$ show that $b \circ \phi \circ a^r \in C^r(G', M')$ and that this induces a homomorphism $H^r(G, M) \rightarrow H^r(G', M')$ for each r .

- (b) Suppose $G' = H$ is a subgroup of G and $a : H \hookrightarrow G$ is the inclusion, $b : M \rightarrow M$ the identity map of a G (and hence H)-module. The map $\text{Res} : H^r(G, M) \rightarrow H^r(H, M)$ is the *restriction homomorphism*.

Suppose H is a normal subgroup of G and $a : G \rightarrow G/H$ is the quotient homomorphism. Let M be a G -module and M^H the H -fixed elements, and let $b : M^H \hookrightarrow M$ be the inclusion. The map $\text{Inf} : H^r(G/H, M^H) \rightarrow H^r(G, M)$ is the *inflation homomorphism*.

Show that the sequence

$$0 \rightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M)$$

is exact. (There is a generalization of this for higher r .)

3. Let G be a group and $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ an exact sequence of G -modules.

- (a) Define a *boundary map* $\delta^r : H^r(G, M'') \rightarrow H^{r+1}(G, M')$ as follows. Pick $\phi \in Z^r(G, M'') \subset C^r(G, M'')$ representing some $\gamma \in H^r(G, M'')$ and suppose $\psi \in C^r(G, M)$ maps to ϕ (under the map $M \rightarrow M''$). Define $\delta^r(\gamma) = d^r(\psi)$. Prove that $d^r(\psi)$ can be considered an element in $C^{r+1}(G, M')$ and this definition induces a well-defined map $H^r(G, M'') \rightarrow H^{r+1}(G, M')$.

- (b) Use δ^r to define a long exact sequence

$$0 \rightarrow H^0(G, M') \rightarrow H^0(G, M) \rightarrow H^0(G, M'') \rightarrow H^1(G, M') \rightarrow H^1(G, M) \rightarrow \dots$$

You only have to prove the exactness for the part of the sequence shown, though this sequence goes on indefinitely.

4. (a) If G acts on a non-commutative group M as automorphisms, it is still possible to define $H^1(G, M)$. Define the 1-cocycles $Z^1(G, M)$ to be maps $\phi : G \rightarrow M$ satisfying $\phi(\sigma\tau) = \phi(\sigma)\sigma(\phi(\tau))$. Say that two cocycles $f, g \in Z^1(G, M)$ are *equivalent* if there is $m \in M$ so that $g(\sigma) = m^{-1}f(\sigma)\sigma(m)$ for all $\sigma \in G$. Now define $H^1(G, M)$ to be the equivalence classes. Show that this makes sense (“equivalent” is an equivalence relation, and so on) and that one recovers the definition from the previous problem set when M is abelian.
- (b) Imitate the proof in class to show that $H^1(\text{Gal}(E/F), GL_n(E)) = 0$. (Hint: Let $f \in Z^1(\text{Gal}(E/F), GL_n(E))$. Start by constructing for each $u \in E^n$ a vector $v(u) \in E^n$ satisfying $v(\sigma u) = f(\sigma)\sigma(v(u))$ for every $\sigma \in \text{Gal}(E/F)$.)
5. Let E/F be a finite non-trivial field extension in characteristic 0 and suppose that E is algebraically closed.
- (a) Show that E/F is Galois even without the assumption that the characteristic is 0. (Hint: if F has characteristic $p > 0$ and $a \in F$ but $a \notin F^p$ then $x^{p^n} - a$ is irreducible.)
- (b) Prove that if $[E : F] = p$ for a prime p then $p = 2$. (Hint: write $E = F[\alpha]$ where $\alpha^p \in F$ and then study the Galois action on an element $\beta \notin F$ which satisfies $\beta^p = \alpha$.) In addition show that $E = F[\sqrt{-1}]$.
- (c) Show that $[E : F] \neq 4$.
- (d) Conclude that if E/F is a finite non-trivial field extension in characteristic 0 and if E is algebraically closed then $E = F[\sqrt{-1}]$.
6. (a) Let F be any field not of characteristic 2. Suppose $\sqrt{-1} \notin F$ and that every element of $F[\sqrt{-1}]$ is a square in $F[\sqrt{-1}]$. Show that F has characteristic 0. (Hint: show that a sum of squares in F is itself a square in F .)
- (b) Extend the result of the previous problem to finite characteristic: show that if E/F be a finite field extension in characteristic $p > 0$ such that E is algebraically closed then $E = F$. In particular, finite, non-trivial, algebraically closed extensions necessarily have characteristic 0. (Hint: follow and adjust the steps 5(a), 5(b), 5(c), 5(d) of the previous problem, then use 6(a). A tricky part is to show that if $[E : F] = p$ and E is algebraically closed then F does not have characteristic p – use the classification of these extensions proved in class.)