

Math 654
Homework #3

April 15, 2007

Due Wednesday, April 25.

Instructions: Do problems 1, 2, 4, and 5. Problem 3 is extra credit.

1. Let G be a finite group, and let $\mathbb{Z}[G] := \left\{ \sum_{t \in G} a_t \cdot t \mid a_t \in \mathbb{Z} \right\}$ be the group ring of G . Let M be a $\mathbb{Z}[G]$ -module. We set

$$M^G := \{m \in M \mid \forall t \in G, tm = m\}.$$

- (a) Show that M^G is an abelian group.
 (b) Show that if $\phi : M \rightarrow N$ is a homomorphism of $\mathbb{Z}[G]$ -modules, then the restriction $\phi' := \phi|_{M^G} : M^G \rightarrow N^G$ is a group homomorphism.
 (c) Suppose $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is an exact sequence of $\mathbb{Z}[G]$ -modules. Prove that the induced sequence of abelian groups $0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$ is exact.
2. As in the previous problem, let G be a finite group. Let A be a $\mathbb{Z}[G]$ -module and define sets of functions,

$$Z(A) := \{c : G \rightarrow A \mid \forall s, t \in G, c(st) = sc(t) + c(s)\},$$

$$B(A) := \{c : G \rightarrow A \mid \exists a \in A, \forall t \in G, c(t) = ta - a\}.$$

- (a) Using the structure of A as an abelian group, we can define an addition law on $Z(A)$ by setting $(c + d)(a) := c(a) + d(a)$ for $c, d \in Z(A)$. Similarly for $B(A)$. Show that these addition laws are well-defined, and under them that $Z(A)$ and $B(A)$ are abelian groups and that $B(A)$ is a subgroup of $Z(A)$. In this way we can define,

$$H(A) := Z(A)/B(A),$$

which is an abelian group.

- (b) Suppose $\phi : A \rightarrow B$ is a homomorphism of $\mathbb{Z}[G]$ -modules. Show that there is a natural group homomorphism $\bar{\phi} : H(A) \rightarrow H(B)$ in the following way: suppose $\bar{c} \in H(A)$ represents the class of $c \in Z(A)$ in $H(A)$. Then show that the function $d : G \rightarrow B$ defined by

$$d(t) := \phi(c(t))$$

is an element of $Z(B)$. Set $\bar{\phi}(\bar{c}) := \bar{d}$. Show that $\bar{\phi}$ is a well-defined group homomorphism. (In other words, $\bar{\phi}(\bar{c}) = \overline{\phi \circ c}$.)

- (c) Suppose

$$0 \rightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \rightarrow 0$$

is an exact sequence of $\mathbb{Z}[G]$ -modules. Show that there is a natural group homomorphism $\delta : C^G \rightarrow H(A)$ such that

$$0 \rightarrow A^G \xrightarrow{\phi'} B^G \xrightarrow{\psi'} C^G \xrightarrow{\delta} H(A) \xrightarrow{\bar{\phi}} H(B) \xrightarrow{\bar{\psi}} H(C)$$

is exact.

3. (Extra Credit) Let E/k be a finite Galois extension with Galois group G .

(a) Let $f : E \rightarrow E$ be defined by

$$f(\alpha) := \sum_{\sigma \in G} \beta_{\sigma} \sigma(\alpha), \quad \beta_{\sigma} \in E.$$

Suppose that for at least one $\sigma \in G$ that $\beta_{\sigma} \neq 0$. Show that f is not identically 0.

(b) Show that both the additive group E and the multiplicative group E^{\times} are $\mathbb{Z}[G]$ -modules. (Note that \mathbb{Z} operates on E^{\times} by exponentiation: $n \cdot e := e^n$ for $n \in \mathbb{Z}$ and $e \in E^{\times}$.)

(c) Show that $H(E) = \{0\}$ and $H(E^{\times}) = \{1\}$.

(d) Suppose now that G is cyclic of prime order p and that k contains all p -th roots of unity. Show that E is a pure radical extension of k . That is, show that there is an $\alpha \in E$ with $E = k(\alpha)$ and $\alpha^p \in k$. (This statement remains true even if $[E : k]$ is not prime.)

4. Let $R = \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$. Let $I = (2, \sqrt{-6})$ be the ideal of R generated by 2 and $\sqrt{-6}$.

(a) Show that a non-zero ideal J of R is free as an R -module if and only if it is a principal ideal. Show that I is not free as an R -module.

(b) Show that $I \oplus I \cong R \oplus R$ as R -modules. (Hint: consider the natural R -module homomorphism $(r, s) \mapsto 2r + s\sqrt{-6} : R \oplus R \rightarrow I$. Show that it splits.)

Thus I is not free, but $I \oplus I$ is free.

5. Let V be a finite dimensional vector space over a field k , $A : V \rightarrow V$ a linear transformation. For $f \in k[x]$ and $v \in V$, define

$$f(x) \cdot v = (f(A))(v).$$

That is, substitute A into f and evaluate the resulting transformation on v .

(a) Verify that V is a $k[x]$ -module via the above definition.

(b) Show that V is a torsion $k[x]$ -module.

(c) Let the *minimal polynomial* of A be the unique monic polynomial $q_A \in k[x]$ of least degree for which $q_A(A) = 0$. Determine q_A in terms of the elementary divisors of the $k[x]$ -module V .

(d) Let $p_A(x) = \det(xI - A) \in k[x]$ be the characteristic polynomial of A , where $I : A \rightarrow A$ is the identity transformation. Relate p_A to the elementary divisors of V .

(e) *Cayley-Hamilton Theorem*: Show that $p_A(A) = 0$. I.e., A linear transformation satisfies its own characteristic polynomial.