Math 5211 - Abstract Algebra II — Due by email

Problem Set 2 — 2/17/14 at 5 PM

Often the significance of a mathematical theorem becomes clear only when looked at from above – that is to say, from the standpoint of a more advanced theory. But the meaning is always there. This is a vitally important point. Were it not for this, mathematics would degenerate into a collection of unrelated formalisms and parlor tricks.

E. Beckenbach and R. Bellman

Read §10.1–10.3 (skip pp. 421-422) and handouts on Noetherian modules and dual modules.
To be handed in: 1, 2, 3, 4

1. Let d be a nonsquare integer. In $\mathbf{Z}[\sqrt{d}]$, let $\mathfrak{a}$ be the ideal $(a, b + c\sqrt{d})$, where a, b, and c are integers and a and c are not 0. So as a $\mathbf{Z}[\sqrt{d}]$-module,

$$\mathfrak{a} = \mathbf{Z}[\sqrt{d}]a + \mathbf{Z}[\sqrt{d}](b + c\sqrt{d}),$$

while as a $\mathbf{Z}$-module

$$\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}a\sqrt{d} + \mathbf{Z}(b + c\sqrt{d}) + \mathbf{Z}(cd + b\sqrt{d}).$$

There are two $\mathbf{Z}[\sqrt{d}]$-module generators (by definition) and four $\mathbf{Z}$-module generators. It is natural to ask: when does $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b + c\sqrt{d})$? That is, when are the given $\mathbf{Z}[\sqrt{d}]$-module generators also $\mathbf{Z}$-module generators?

a) Show $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b + c\sqrt{d})$ if and only if the following three conditions are all satisfied:

- $c|a$,
- $c|b$,
- $d \equiv (b/c)^2 \bmod a/c$.

(In particular, when $\mathfrak{a} = (a, b \pm \sqrt{d})$ then $\mathfrak{a} = \mathbf{Z}a + \mathbf{Z}(b + \sqrt{d})$ if and only if $d \equiv b^2 \bmod a$.)

b) Let's put part a to work. In $\mathbf{Z}[\sqrt{-5}]$, find an element of the ideal $(3, 1 + 2\sqrt{-5})$ that is not a $\mathbf{Z}$-linear combination of 3 and $1 + 2\sqrt{-5}$. (So 3 and $1 + 2\sqrt{-5}$ span the ideal as a $\mathbf{Z}[\sqrt{-5}]$-module but not as a $\mathbf{Z}$-module.) Then find a pair of elements that generates the ideal $(3, 1 + 2\sqrt{-5})$ as both a $\mathbf{Z}[\sqrt{-5}]$-module and as a $\mathbf{Z}$-module.

c) Show the ideal $(7, 2 + 3\sqrt{-5})$ is not generated as a $\mathbf{Z}$-module by 7 and $2 + 3\sqrt{-5}$ by finding an explicit element of the ideal that is not in their $\mathbf{Z}$-span, and then find a pair of elements in the ideal that generate it as both a $\mathbf{Z}$-module and a $\mathbf{Z}[\sqrt{-5}]$-module.

2. Let R be an integral domain with fraction field K, and I and J be nonzero ideals in R.

a) Show every R-linear map $f\colon I \to J$ has the form $f(x) = cx$ where $c \in K$ such that $cI \subset J$.

b) Use the work in part a to show $\mathrm{Hom}_R(I, J) \cong \{c \in K : cI \subset J\}$ as R-modules.

3. Let V be a finite-dimensional vector space over a field F and $A\colon V \to V$ be an F-linear operator on V. Treat V as an $F[T]$-module by setting $f(T)(v) = f(A)v$ for all $f(T) \in F[T]$ and $v \in V$. For each $v \in V$, set the annihilator ideal of v to be $I(v) = \{f(T) \in F[T] : f(T)v = 0\}$, so $F[T]v \cong F[T]/I(v)$ as $F[T]$-modules. The ideal $I(v)$ has a generator, and its relation to v is analogous to the order of an element in an abelian group.

   a) Let $F = \mathbf{R}$, $V = \mathbf{R}^2$, and $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 2 \end{smallmatrix}\right)$. Compute the ideal $I(v)$ for $v = \binom{1}{0}$ and $\binom{2}{3}$.

   b) If $I(v) = (n)$, show for any factor d of n in $F[T]$ that $I(dv) = (n/d)$. This is the analogue of g^d having order n/d in an abelian group if g has order n and d is a positive factor of n.

   c) If $I(v) = (n)$ and m is relatively prime to n in $F[T]$, show $I(mv) = I(v)$. This is the analogue of g^m having order n in an abelian group if g has order n and m is relatively prime to n.

   d) Set $I(v) = (m)$ and $I(w) = (n)$. If m and n are relatively prime in $F[T]$, show $I(v + w) = (mn)$. This is the analogue of the order of the product being the product of the orders in a finite abelian group when the orders are relatively prime.

4. Let R be a PID with fraction field K. A finitely generated torsion R-module M is an analogue of a finite abelian group (it is precisely a finite abelian group when $R = \mathbf{Z}$), and we want to look at an analogue for such modules of characters for finite abelian groups. The R-module K/R will be our substitute for the roots of unity in $\mathbf{C}^\times$. When $R = \mathbf{Z}$ we have $K/R = \mathbf{Q}/\mathbf{Z}$, which is isomorphic to the complex roots of unity using the function $e^{2\pi i z}$.

   a) Show every finitely generated R-submodule of K/R is isomorphic to $(1/r)I/I$ for some nonzero $r \in R$. This is analogous to every finite subgroup of $\mathbf{R}/\mathbf{Z}$ being $(1/n)\mathbf{Z}/\mathbf{Z}$ for some nonzero integer n.

   b) Use part a to show every finitely generated R-submodule of K/R is isomorphic to R/I for a unique nonzero ideal I in R, and for every nonzero ideal I in R show K/R contains a *unique* R-submodule isomorphic to R/I. This is analogous to all finite subgroups of $\mathbf{C}^\times$ being cyclic and $\mathbf{C}^\times$ containing a unique cyclic group of order n for all $n \geq 1$.

   c) For any finitely generated torsion R-module M, define a *character* of M to be an R-linear map $\chi\colon M \to K/R$ and set $\widehat{M} = \mathrm{Hom}_R(M, K/R)$.[1] For nonzero ideals I in R, show $\widehat{R/I} \cong R/I$ as R-modules. This is analogous to finite cyclic groups being isomorphic to their dual groups.

   d) For any finitely generated torsion R-module M, show $\widehat{M}$ is a finitely generated torsion R-module. (Hint: An R-linear map out of M is determined by its values on a spanning set.)

   e) Let M be a finitely generated torsion R-module and N be a submodule of M. Show every character of N can be extended to a character of M. The key point is figuring out, if $N \neq M$ and $m \in M - N$, how to extend a character of N to a character of $N + Rm$ (*i.e.*, how to extend an R-linear map $N \to K/R$ to an R-linear map $N + Rm \to K/R$).

5. Let V be a vector space over a field K and let $\varphi_1, \ldots, \varphi_r$ lie in the dual space $V^\vee$.

[1] This is different from the dual module of M, which is $\mathrm{Hom}_R(M, R)$ and equals 0 for torsion-modules; it's like $\mathrm{Hom}_{\mathbf{Z}}(A, \mathbf{Z})$ being 0 when A is a torsion abelian group.

a) If V is finite-dimensional, show an element ψ in $V^\vee$ lies in the span of $\varphi_1, \ldots, \varphi_r$ if and only if $\bigcap_{i=1}^r \ker \varphi_i \subset \ker \psi$. (You might first try the case when $\varphi_1, \ldots, \varphi_r$ are linearly independent in $V^\vee$, but the result is true without such a restriction.)

b) Show part a is true even without the assumption that V is finite-dimensional: an element ψ in $V^\vee$ lies in the span of $\varphi_1, \ldots, \varphi_r$ if and only if $\bigcap_{i=1}^r \ker \varphi_i \subset \ker \psi$.

6. Let G be a finite group, possibly nonabelian. We will see how to interpret the group homomorphisms $G \to \mathbf{C}^\times$ as the "normalized" simultaneous eigenvectors in a space of functions.

Let $V = \mathrm{Map}(G, \mathbf{C})$ be the set of all functions $f \colon G \to \mathbf{C}$. Under addition of functions and $\mathbf{C}$-scaling, this is a complex vector space:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (cf)(x) = c \cdot f(x).$$

One basis of V is the delta-functions δ_g, where $\delta_g(g) = 1$ and $\delta_g(h) = 0$ for $h \neq g$, so $\dim_{\mathbf{C}} V = |G|$.

For $g \in G$, let $L_g \colon V \to V$ be interior scaling by g on the left: for $f \in V$, $L_g f$ is the function in V given by $(L_g f)(x) = f(gx)$ for all $x \in G$.

a) Prove each $L_g \colon V \to V$ is $\mathbf{C}$-linear.

b) Prove a group homomorphism $f \colon G \to \mathbf{C}^\times$, regarded as an element of V, is an eigenvector ("eigenfunction") of *every* L_g. Remember that, by definition, the zero function in V is not considered to be an eigenvector.

c) Let $G = S_3$. Listing the elements of G in the order $(1), (12), (13), (23), (123), (132)$, express $L_{(12)}$ and $L_{(123)}$ as 6×6 matrices with respect to the basis $\{\delta_g : g \in S_3\}$ and check these matrices have order 2 and 3, respectively.

d) Express the sign homomorphism $S_3 \to \{\pm 1\}$ as a column vector in the basis of V from part c and check it is an eigenvector of $L_{(12)}$ and $L_{(123)}$, as it must be by part b.

e) Here is a converse to part b: if $f \in V$ is an eigenvector of *every* L_g, prove $f(e) \neq 0$ (e denotes the identity in G) and that if we rescale f so that $f(e) = 1$ then f is a group homomorphism $G \to \mathbf{C}^\times$.