

ALGEBRA MID-TERM

CLAY SHONKWILER

1

Suppose I is a principal ideal of the integral domain R . Prove that the R -module $I \otimes_R I$ has no non-zero torsion elements.

Proof. Note, first, that if $I \otimes_R I$ has no non-zero torsion simple tensors, then it will have no non-zero torsion elements. Define $\phi : I \times I \rightarrow I$, given by

$$(m, n) \mapsto mn.$$

This is certainly well-defined. Furthermore, if $m, n, m_1, m_2, n_1, n_2 \in I$ and $r \in R$, then

$$\phi(m_1 + m_2, n) = (m_1 + m_2)n = m_1n + m_2n = \phi(m_1, n) + \phi(m_2, n),$$

$$\phi(m, n_1 + n_2) = m(n_1 + n_2) = mn_1 + mn_2 = \phi(m, n_1) + \phi(m, n_2)$$

and

$$\phi(mr, n) = mrn = \phi(m, rn),$$

so ϕ is a bilinear map. Hence, by the universal property of the tensor product, ϕ induces a homomorphism $\Phi : I \otimes_R I \rightarrow I$ such that

$$m \otimes n = mn.$$

Now, suppose there exists $m \otimes n \in I \otimes_R I$ and non-zero $r \in R$ such that $r(m \otimes n) = 0$. Now, since $m, n \in I$ and I is principal, then $m = r_1a$ and $n = r_2a$ for some $r_1, r_2 \in R$, where a is the generator of the principal ideal I . If $a = 0$, then this proposition is trivially true, since this would imply that I is the zero ideal and so $I \otimes I$ is just the zero module. Therefore, we can assume $a \neq 0$. Since Φ is a homomorphism, this implies

$$0 = \Phi(r(m \otimes n)) = \Phi(r(r_1a \otimes r_2a)) = r(r_1r_2a^2).$$

Since R is an integral domain, this implies that either $r_1 = 0$ or $r_2 = 0$. Hence,

$$m \otimes n = r_1a \otimes r_2a = 0 \otimes r_2a = 0$$

or

$$m \otimes n = r_1a \otimes r_2a = r_1a \otimes 0 = 0.$$

Since our choice of the simple tensor $m \otimes n$ was arbitrary, we see that $I \otimes_R I$ contains no non-zero torsion elements. \square

2

Prove that $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$ as rings.

Proof. We can think of elements of $\mathbb{Z}[i]$ as being of the form $a + bi$ for some $a, b \in \mathbb{Z}$. Now, define a map $\phi : \mathbb{Z}[i] \times \mathbb{R} \rightarrow \mathbb{C}$ given by

$$(a + bi, r) \mapsto r(a + bi).$$

Then, for $a + bi, c + di \in \mathbb{Z}[i]$, $r, r_1, r_2 \in \mathbb{R}$ and $n \in \mathbb{Z}$,

$$\phi(a + bi + c + di, r) = r(a + bi + c + di) = r(a + bi) + r(c + di) = \phi(a + bi, r) + \phi(c + di, r),$$

$$\phi(a + bi, r_1 + r_2) = (r_1 + r_2)(a + bi) = r_1(a + bi) + r_2(a + bi) = \phi(a + bi, r_1) + \phi(a + bi, r_2)$$

and

$$\phi((a + bi)n, r) = r((a + bi)n) = nr(a + bi) = \phi(a + bi, nr),$$

so ϕ is a bilinear map and, hence, induces a \mathbb{Z} -module homomorphism $\Phi : \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \rightarrow \mathbb{C}$. Now, we define the map $\Psi : \mathbb{C} \rightarrow \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R}$ given by

$$z + wi \mapsto 1 \otimes z + i \otimes w$$

and we want to show that Φ and Ψ are inverses. Certainly if $z_1 + w_1i, z_2 + w_2i \in \mathbb{C}$ and $n \in \mathbb{Z}$, then

$$\begin{aligned} \Psi(n(z_1 + w_1i) + z_2 + w_2i) &= \Psi((nz_1 + z_2) + (nw_1 + w_2)i) \\ &= 1 \otimes (nz_1 + z_2) + i \otimes (nw_1 + w_2) \\ &= n(1 \otimes z_1 + i \otimes w_1) + 1 \otimes z_2 + i \otimes w_2 \\ &= n\phi(z_1 + w_1i) + \phi(z_2 + w_2i) \end{aligned}$$

so Ψ is a \mathbb{Z} -module homomorphism. Now, if $(a + bi) \otimes r \in \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R}$, then

$$\begin{aligned} (\Psi \circ \Phi)((a + bi) \otimes r) &= \Psi(\Phi((a + bi) \otimes r)) = \Psi(r(a + bi)) = 1 \otimes ra + i \otimes rb \\ &= a \otimes r + bi \otimes r \\ &= (a + bi) \otimes r. \end{aligned}$$

Similarly, if $z + wi \in \mathbb{C}$, then

$$(\Phi \circ \Psi)(z + wi) = \Phi(1 \otimes z + i \otimes w) = \Phi(1 \otimes z) + \Phi(i \otimes w) = z + wi.$$

Hence, we see that Φ and Ψ are inverses, so $\Phi : \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \rightarrow \mathbb{C}$ is a \mathbb{Z} -module isomorphism, which is to say an isomorphism of abelian groups. To see that it is, in fact, an isomorphism of rings, we need only show that Φ respects the multiplicative structure. To see this, let $(a + bi) \otimes r_1, (c + di) \otimes r_2 \in \mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R}$. Then

$$\begin{aligned} \Phi([(a + bi) \otimes r_1][(c + di) \otimes r_2]) &= \Phi([(ac - bd) + (ad + bc)i] \otimes r_1 r_2) \\ &= r_1 r_2((ac - bd) + (ad + bc)i) \\ &= r_1 r_2(a + bi)(c + di) \\ &= \Phi((a + bi) \otimes r_1) \Phi((c + di) \otimes r_2). \end{aligned}$$

Therefore, we conclude that $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$ as rings. \square

3

Prove that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$ as rings.

Proof. Let $\phi : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}$ be the identity map. Then ϕ is certainly \mathbb{R} -bilinear, so, by the universal property of the tensor product, it induces an \mathbb{R} -module homomorphism $\Phi : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \rightarrow \mathbb{C} \times \mathbb{C}$. If we define the map $\Psi : \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ given by

$$(z, w) \mapsto z \otimes w.$$

Then we want to show that $\Phi \circ \Psi = Id$ and $\Psi \circ \Phi = Id$, which will mean that Ψ is the inverse of Φ and so Φ is an isomorphism. If $z \otimes w \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, then

$$(\Psi \circ \Phi)(z \otimes w) = \Psi(\Phi(z \otimes w)) = \Psi(z, w) = z \otimes w$$

and if $(z, w) \in \mathbb{C} \times \mathbb{C}$, then

$$(\Phi \circ \Psi)(z, w) = \Phi(\Psi(z, w)) = \Phi(z \otimes w) = (z, w).$$

Hence, we see that the \mathbb{R} -module homomorphism Φ is invertible and so is an isomorphism. To see that it is a ring isomorphism, we must show that it is a ring homomorphism and the bijectivity will follow from what we've just shown. To that end, let $z_1 \otimes w_1, z_2 \otimes w_2 \in \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. Then

$$\begin{aligned} \Phi((z_1 \otimes w_1)(z_2 \otimes w_2)) &= \Phi(z_1 z_2 \otimes w_1 w_2) = (z_1 z_2, w_1 w_2) \\ &= (z_1, w_1)(z_2, w_2) \\ &= \Phi(z_1 \otimes w_1)\Phi(z_2 \otimes w_2). \end{aligned}$$

Hence, we conclude that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$. □

4

Calculate the character table of $S_3 \times S_3$.

Answer: See attached sheet.



5

If ρ is the character of V , show that

$$Ind_H^G(\rho)(g) = \sum_{i=1}^k \rho(g_i^{-1} g g_i)$$

where g_1, \dots, g_k are representatives of the left cosets of H in G , and $\rho(g_i^{-1} g g_i)$ is defined to be 0 if $g_i^{-1} g g_i$ is not in H .

Proof. Let ψ be the representation of H with character ρ . We know that

$$G = \bigsqcup_{i=1}^k g_i H.$$

Hence,

$$\mathbb{C}[G] = \mathbb{C} \left[\bigsqcup_{i=1}^k g_i H \right] = \bigoplus_{i=1}^k g_i \mathbb{C}[H].$$

Therefore,

$$\begin{aligned} \text{Ind}_H^G(V) &= \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V = \left(\bigoplus_{i=1}^k g_i \mathbb{C}[H] \right) \otimes_{\mathbb{C}[H]} V \\ &= \bigoplus_{i=1}^k (g_i \mathbb{C}[H] \otimes_{\mathbb{C}[H]} V) = \bigoplus_{i=1}^k (g_i \otimes_{\mathbb{C}[H]} V). \end{aligned}$$

Now, for each $g \in G$, $gg_i = g_j h$ for a single $j = 1, \dots, k$ and some $h \in H$. This implies that

$$g_j^{-1} gg_i \in H$$

for this value of j and for no other. Since $gg_i = g_j h$,

$$\text{Ind}_H^G(V)(g)(g_i \otimes_{\mathbb{C}[H]} V) = gg_i \otimes_{\mathbb{C}[H]} V = g_j h \otimes_{\mathbb{C}[H]} V = g_j \otimes_{\mathbb{C}[H]} \psi(h)V = g_j \otimes_{\mathbb{C}[H]} V.$$

Hence, if $i \neq j$, which is the same thing as saying that $g_i^{-1} gg_i \notin H$, then there are no eigenvalues of $\text{Ind}_H^G(V)(g)$ in $g_i \otimes_{\mathbb{C}[H]} V$, meaning this piece contributes nothing to $\text{Ind}_H^G(\rho)$.

On the other hand, if $i = j$, then we see that

$$g_i^{-1} gg_i \in H,$$

and so

$$\text{Ind}_H^G(V)(g)(g_i \otimes_{\mathbb{C}[H]} V) = gg_i \otimes_{\mathbb{C}[H]} V = g_i g_i^{-1} gg_i \otimes_{\mathbb{C}[H]} V = g_i \otimes_{\mathbb{C}[H]} \psi(g_i^{-1} gg_i)V.$$

Hence, any eigenvalues in $g_i \otimes V$ of $\text{Ind}_H^G(V)$ are precisely those given by the action of $g_i^{-1} gg_i$ on V .

Therefore, we see that

$$\text{Ind}_H^G(\rho) = \sum_{g_i^{-1} gg_i \in H} \rho(g_i^{-1} gg_i),$$

which we can rewrite as

$$\text{Ind}_H^G(\rho) = \sum_{i=1}^k \rho(g_i^{-1} gg_i)$$

where we follow the convention that $\rho(g_i^{-1} gg_i) = 0$ if $g_i^{-1} gg_i \notin H$. \square

6

Let $H \leq G$ as above, and let ρ be a character of H , and χ a character of G . Prove the following formula, called the Frobenius reciprocity formula:

$$\langle \chi|_H, \rho \rangle_H = \langle \chi, \text{Ind}_H^G(\rho) \rangle_G$$

where $\chi|_H$ denotes the restriction of χ to H .

Proof. Recall, first of all, that

$$\text{Ind}_H^G(\rho)(g) = \sum_{i=1}^k \rho(g_i^{-1}gg_i)$$

as we showed in problem 5 above. Thus,

$$\langle \chi, \text{Ind}_H^G(\rho) \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\text{Ind}_H^G(\rho)(g)} = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\left(\sum_{i=1}^k \rho(g_i^{-1}gg_i) \right)}.$$

Now, since χ is a class function, we can re-arrange the summations like so:

$$\langle \chi, \text{Ind}_H^G(\rho) \rangle_G = \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^k \chi(g_i^{-1}gg_i) \overline{\rho(g_i^{-1}gg_i)}.$$

Since $\rho(g_i^{-1}gg_i) \neq 0$ only when $g_i^{-1}gg_i \in H$, this is the same as

$$\langle \chi, \text{Ind}_H^G(\rho) \rangle_G = \frac{1}{|G|} \sum_{g \in G} \sum_{g_i^{-1}gg_i \in H} \chi(g_i^{-1}gg_i) \overline{\rho(g_i^{-1}gg_i)}.$$

Now, for each g_i , there are exactly $|H|$ elements of g_iH , so there are $|H|$ elements $g \in G$ such that $gg_i \in g_iH$. Furthermore, if $g \neq g'$, then $gg_i \neq g'i$, which we can see simply by multiplying both sides of this expression by g_i^{-1} . Hence, if we denote

$$g'g_i = g_i h'_i$$

then the h'_i run over all of H . Hence, for each $h \in H$, we see that $h = g_i^{-1}gg_i$ exactly once for each g_i , so

$$\frac{1}{|G|} \sum_{g \in G} \sum_{g_i^{-1}gg_i \in H} \chi(g_i^{-1}gg_i) \overline{\rho(g_i^{-1}gg_i)} = k \sum_{h \in H} \chi(h) \overline{\rho(h)}.$$

Therefore,

$$\begin{aligned} \langle \chi, \text{Ind}_H^G(\rho) \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \sum_{g_i^{-1}gg_i \in H} \chi(g_i^{-1}gg_i) \overline{\rho(g_i^{-1}gg_i)} \\ &= \frac{1}{|G|} k \sum_{h \in H} \chi(h) \overline{\rho(h)} \\ &= \frac{k}{|G|} \sum_{h \in H} \chi(h) \overline{\rho(h)} \\ &= \frac{1}{|H|} \sum_{h \in H} \chi(h) \overline{\rho(h)} \\ &= \langle \chi|_H, \rho \rangle_H, \end{aligned}$$

giving us the desired result. \square

Suppose that $G = H \times K$. Let V be a representation of H . Prove that $\text{Ind}_H^G(V) = V \otimes R_K$, where R_K denotes the regular representation of K .

Proof. First, note that, by hypothesis, $\mathbb{C}[G] = \mathbb{C}[H \times K]$. Now, we showed in class (February 11) that

$$F[G_1 \times G_2] \simeq F[G_1] \otimes_F F[G_2]$$

for any field F and groups G_1 and G_2 . Hence,

$$\mathbb{C}[G] = \mathbb{C}[H \times K] \simeq \mathbb{C}[H] \otimes_{\mathbb{C}} \mathbb{C}[K]$$

which is, of course, isomorphic to $\mathbb{C}[K] \otimes_{\mathbb{C}} \mathbb{C}[H]$. Therefore, we see that

$$\text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \simeq (\mathbb{C}[K] \otimes_{\mathbb{C}} \mathbb{C}[H]) \otimes_{\mathbb{C}[H]} V.$$

Since $\mathbb{C}[H]$ is a $(\mathbb{C}, \mathbb{C}[H])$ -bimodule, we know that this expression is associative; that is

$$(\mathbb{C}[K] \otimes_{\mathbb{C}} \mathbb{C}[H]) \otimes_{\mathbb{C}[H]} V \simeq \mathbb{C}[K] \otimes_{\mathbb{C}} (\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V).$$

In turn, it is certainly true that $\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \simeq V$, so we see that, when we combine all of the above

$$\text{Ind}_H^G(V) = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \simeq \mathbb{C}[K] \otimes_{\mathbb{C}} (\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V) \simeq \mathbb{C}[K] \otimes_{\mathbb{C}} V.$$

Since $\mathbb{C}[K]$ is R_K , we conclude that

$$\text{Ind}_H^G(V) \simeq R_K \otimes_{\mathbb{C}} V \simeq V \otimes_{\mathbb{C}} R_K.$$

□

(a) Let \mathbb{F}_p denote the finite field with p elements. Suppose that $[K : \mathbb{F}_p] = n$, prove that K has p^n elements.

Proof. Let $a_1, \dots, a_n \in K$ be such that $K = \mathbb{F}_p(a_1, \dots, a_n)$ and $\{a_1, \dots, a_n\}$ forms a basis for K over \mathbb{F}_p . Then each element $\beta \in K$ can be written as

$$\beta = \beta_1 a_1 + \dots + \beta_n a_n$$

where $\beta_k \in \mathbb{F}_p$. Since there are p possible choices for each β_k , we see that K can contain at most p^n distinct elements. Now, suppose there are fewer than p^n distinct elements in K . This means that, for some $\beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n \in \mathbb{F}_p$,

$$\beta_1 a_1 + \dots + \beta_n a_n = \gamma_1 a_1 + \dots + \gamma_n a_n,$$

or

$$(\beta_1 - \gamma_1) a_1 + \dots + (\beta_n - \gamma_n) a_n = 0.$$

Now, since the a_k form a basis for K as a vector space over \mathbb{F}_p , this implies that

$$\beta_k - \gamma_k = 0$$

for all $k = 1, \dots, n$. Hence, $\beta_k = \gamma_k$ and we see that distinct linear combinations of the basis elements correspond to distinct elements of K , meaning that K contains at least p^n elements.

Since we've shown that $|K| \geq p^n$ and $|K| \leq p^n$, we conclude that K contains exactly p^n elements. \square

(b) Prove that $f(x) = x^5 - ax - 1 \in \mathbb{Z}[x]$ is irreducible unless $a = 0, 2, -1$.

Proof. If f is not irreducible, then there are two cases to consider: it has a linear factor, or it is the product of an irreducible cubic polynomial with an irreducible quadratic. If f has a linear factor, then this implies that f has a root $r \in \mathbb{Z}$, i.e.,

$$r^5 - ar - 1 = 0.$$

This implies that

$$1 = r^5 - ar = r(r^4 - a),$$

so it must be true that r divides 1; that is, $r = \pm 1$. If $r = 1$ is a root of f , then

$$0 = f(r) = f(1) = 1^5 - a(1) - 1 = 1 - a - 1 = -a,$$

so it must be the case that $a = 0$. On the other hand, if $r = -1$ is a root of f , then

$$0 = f(r) = f(-1) = (-1)^5 - a(-1) - 1 = -1 + a - 1 = a - 2,$$

so it must be the case that $a = 2$. Since these are the only possible integer roots of f , we conclude that f is irreducible or only reduces into factors with degree greater than 1 unless $a = 0, 2$. Now, suppose

$$x^5 - ax - 1 = f(x) = (hx^2 + bx + c)(jx^3 + dx^2 + ex + g).$$

Then either $h = j = 1$ or $h = j = -1$; without loss of generality, we may assume that $h = j = 1$, so

$$\begin{aligned} x^5 - ax - 1 &= (x^2 + bx + c)(x^3 + dx^2 + ex + g) \\ &= x^5 + (b+d)x^4 + (c+bd+e)x^3 + (cd+be+g)x^2 + (ce+bg)x + cg. \end{aligned}$$

This gives us the following system of equations:

$$\begin{aligned} b+d &= 0 \\ c+bd+e &= 0 \\ cd+be+g &= 0 \\ ce+bg &= -a \\ cg &= -1. \end{aligned}$$

Hence, we can conclude immediately that $d = -b$ and $c = \pm 1$. Now, suppose $c = 1$. Then $g = -1$ and the system above reduces to:

$$\begin{aligned} 1 - b^2 + e &= 0 \\ -b + be - 1 &= 0 \\ e - b &= -a. \end{aligned}$$

Hence, by the second line,

$$b(e-1) = 1 \quad \Leftrightarrow \quad b = \frac{1}{e-1}.$$

Since b must be an integer, this implies $e = 0, 2$. If $e = 2$, then $b = 1$ and so, by the first equation,

$$0 = 1 - b^2 + e = 1 - 1 + 2 = 2$$

which is certainly not true. If $e = 0$, then $b = -1$ and so, by the third equation in our revised system, $a = -1$.

On the other hand, suppose $c = -1$. Then $g = 1$ and the original system of equations reduces to:

$$\begin{aligned} -1 - b^2 + e &= 0 \\ b + be + 1 &= 0 \\ b - e &= -a \end{aligned}$$

Hence, by the second line,

$$b(e+1) = -1 \quad \Leftrightarrow \quad b = \frac{-1}{e+1}.$$

Since b is an integer, this implies that $b = \pm 1$, which means that $b^2 = 1$. By the first equation, then

$$0 = -1 - b^2 + e = -1 - 1 + e = e - 2 \quad \Leftrightarrow \quad e = 2.$$

However, if $e = 2$, then

$$b = \frac{-1}{e+1} = \frac{-1}{2+1} = \frac{-1}{3} \notin \mathbb{Z}.$$

Hence, we conclude that $c \neq -1$. Therefore, we see that f can only be factored into the product of a cubic and a quadratic if $a = -1$. Combined with our other two possible values of a that make f reducible, 0 and 2, we conclude that f is irreducible unless $a = 0, 2, -1$. \square