Math 612 Homework 3

Paul Hacking

March 1, 2020

Reading: Dummit and Foote, Sections 10.4, 13.1, 13.2, and 13.3.

Please note: We will only consider tensor products of modules over *commutative* rings as in DF 10.4, Corollary 12. I recommend reading Atiyah–MacDonald pp. 24–31 in addition to DF 10.4.

Justify your answers carefully (complete proofs are expected). All rings are assumed commutative with 1.

(1) (a) Let A be a finitely generated abelian group. Prove that if $A \neq \{0\}$ then $A \otimes_{\mathbb{Z}} A \neq \{0\}$.

(b) Show by example that the hypothesis that A is finitely generated in part (a) is necessary.

(2) Recall that for an integral domain R and an R-module M we say $m \in M$ is *torsion* if there exists $0 \neq r \in R$ such that $rm = 0$. The set of all torsion elements forms a submodule $\mathrm{Tors}(M) \subset M$, and we say M is *torsion-free* if $\mathrm{Tors}(M) = \{0\}$. In this exercise we describe an example of an integral domain R and a torsion-free R-module M such that $M \otimes_R M$ is not torsion-free.

Let $R = \mathbb{C}[x, y]$ and $\mathfrak{m} = (x, y) \subset R$. Consider the element $t = x \otimes y - y \otimes x \in \mathfrak{m} \otimes_R \mathfrak{m}$.

(a) Show that $x \cdot t = y \cdot t = 0$.

(b) The evaluation map $R \to \mathbb{C}$, $f \mapsto f(0, 0)$ has kernel $\mathfrak{m}$ and so by the first isomorphism theorem induces an isomorphism of rings $R/\mathfrak{m} \xrightarrow{\sim} \mathbb{C}$. We use this isomorphism to give $\mathbb{C}$ the structure of an R-module (explicitly, we define scalar multiplication by elements of R via $f \cdot \lambda := f(0,0) \cdot \lambda$ for $f \in R$ and $\lambda \in \mathbb{C}$). Show that the map $\varphi\colon \mathfrak{m} \times \mathfrak{m} \to \mathbb{C}$ defined by

$$\varphi(f,g) = \frac{\partial f}{\partial x}(0,0) \cdot \frac{\partial g}{\partial y}(0,0)$$

is R-bilinear.

(c) Using part (b) or otherwise, show that $t \neq 0 \in \mathfrak{m} \otimes_R \mathfrak{m}$.

[Remark: In fact, there is a natural surjective homomorphism

$$\alpha\colon \mathfrak{m} \otimes_R \mathfrak{m} \to \mathfrak{m}^2 = (x^2, xy, y^2) \subset R$$

given by $\alpha(f \otimes g) = f \cdot g$ (why?), and one can show that the kernel of α is generated by t. So $\mathrm{Tors}(\mathfrak{m} \otimes_R \mathfrak{m}) = R \cdot t = \mathbb{C} \cdot t$ (using $x \cdot t = y \cdot t = 0$), and we have a short exact sequence

$$0 \to \mathbb{C} \cdot t \to \mathfrak{m} \otimes_R \mathfrak{m} \to \mathfrak{m}^2 \to 0.$$

]

(3) (Optional) Recall that a (finite) *presentation* of an R-module M is an exact sequence

$$R^n \to R^m \to M \to 0,$$

that is, an expression of M as the cokernel of a homomorphism of free modules $R^n \to R^m$ (which is given by a matrix $A \in R^{m \times n}$).

(a) Let M and N be R-modules and suppose given presentations of M and N. Show how to obtain a presentation of $M \otimes_R N$.

(b) Using part (a) or otherwise, justify the description of $\mathfrak{m} \otimes_R \mathfrak{m}$ in the Remark following Q2.

(4) Let $\varphi\colon R \to S$ be a homomorphism of rings, and let M be an R-module and N an S-module. Recall that $M \otimes_R S$ has the structure of an S-module via $s' \cdot (m \otimes s) := m \otimes s's$ ("extension of scalars") and N may be given the structure of an R-module (denoted ${}_RN$) via $r \cdot n := \varphi(r) \cdot n$ ("restriction of scalars"). Prove that there is an isomorphism of abelian groups

$$F\colon \mathrm{Hom}_S(M \otimes_R S, N) \xrightarrow{\sim} \mathrm{Hom}_R(M, {}_RN)$$

given by

$$F(\theta)(m) = \theta(m \otimes 1)$$

with inverse G given by

$$G(\psi)(m \otimes s) = s \cdot \psi(m).$$

(Check the two maps F and G are well defined and mutually inverse.) We say that the functors

$$(\cdot) \otimes_R S \colon \{R-\text{modules}\} \to \{S-\text{modules}\}$$

and

$${}_R(\cdot) \colon \{S-\text{modules}\} \to \{R-\text{modules}\}$$

are an *adjoint pair* of functors, with $(\cdot) \otimes_R S$ the *left adjoint* of ${}_R(\cdot)$ and ${}_R(\cdot)$ the *right adjoint* of $(\cdot) \otimes_R S$.

(5) Let R be a ring, $\mathfrak{m} \subset R$ a maximal ideal, and $k = R/\mathfrak{m}$ the associated *residue field*. If M is an R-module, then $M/\mathfrak{m}M = M \otimes_R (R/\mathfrak{m}) = M \otimes_R k$ is a k-vector space (this is an instance of extension of scalars).

Recall that we say a ring R is *local* if it has a unique maximal ideal $\mathfrak{m}$. Nakayama's lemma in commutative algebra is the following assertion (we will prove this later in the course): Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and M a finitely generated R-module. If $\mathfrak{m}M = M$ then $M = 0$.

Now use Nakayama's lemma to prove the following: Let R be a Noetherian local ring and M a finitely generated R-module. Suppose $m_1, \ldots, m_n$ are elements of M such that their images $\bar{m}_1, \ldots, \bar{m}_n$ in $M/\mathfrak{m}M$ span $M/\mathfrak{m}M$ as a k-vector space. Then $m_1, \ldots, m_n$ generate M as an R-module.

(6) Prove that a regular octahedron cannot be dissected by plane cuts and reassembled to form a cube.

(7) Prove that if F is a finite field then $|F| = p^n$ for some prime p and positive integer n.

(8) Give an example of an infinite field of characteristic p.

(9) Let $f = x^3 - x + 1$.

(a) Prove that f is irreducible over $\mathbb{Q}$.

(b) Let $\alpha \in \mathbb{C}$ be a root of f and let $K = \mathbb{Q}(\alpha)$. Then $1, \alpha, \alpha^2$ is a basis for K as a vector space over $\mathbb{Q}$ (why?). Express $(1+\alpha+\alpha^2)^{-1}$ in the form $c_0 + c_1\alpha + c_2\alpha^2$ for $c_0, c_1, c_2 \in \mathbb{Q}$.

(10) Let $\alpha = \sqrt{2} + i$. Compute the minimal polynomial for α over (a) $\mathbb{Q}$, (b) $\mathbb{Q}(\sqrt{2})$, (c) $\mathbb{Q}(i)$, (d) $\mathbb{Q}(\sqrt{-2})$.

(11) Let $\alpha = \sqrt[3]{2}$. Compute the minimal polynomial for $\beta := 1 + \alpha^2$ over $\mathbb{Q}$.

(12) Let $\zeta_n = e^{2\pi i/n}$ for $n \in \mathbb{N}$. Compute the minimal polynomial for ζ_n over $\mathbb{Q}$ for $n = 4, 6, 8, 9, 10, 12$.

(13) Determine whether i is in the following fields (a) $\mathbb{Q}(\sqrt{-2})$, (b) $\mathbb{Q}(\sqrt[4]{-2})$, (c) $\mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is a root of $x^3 + x + 1$.

(14) Let p be a prime, $F \subset K$ a field extension of degree p, and $\alpha \in K \setminus F$. Show that $K = F(\alpha)$.

(15) Let $F \subset K$ be an extension of fields.

(a) Show that if $[K : F] = 1$ then $F = K$.

(b) Suppose $\mathrm{char}(F) \neq 2$. Show that if $[K : F] = 2$ then there exists $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^2 \in F$.

(c) Show by example that the hypothesis $\mathrm{char}(F) \neq 2$ is necessary in part (b).

(16) Let $F \subset K$ be a field extension and $\alpha, \beta \in K$. Let $m = [F(\alpha)\colon F]$, $n = [F(\beta)\colon F]$ and suppose $\gcd(m, n) = 1$. Show that $[F(\alpha, \beta) : F] = mn$ and write down a basis for $F(\alpha, \beta)$ as a vector space over F.

(17) Let $F \subset K$ be a field extension such that $K = F(\alpha)$ for some $\alpha \in K$ and $[K : F]$ is odd. Prove that $K = F(\alpha^2)$.

(18) In this problem we will prove that it is impossible in general to trisect an angle using ruler and compass. First note that an angle θ can be constructed iff the length $\cos\theta$ can be constructed. Also recall that a length l can be constructed iff there exists a tower of field extensions $\mathbb{Q} = F_0 \subset F_1 \subset \cdot \subset F_n = F$ such that $[F_{i+1} : F_i] = 2$ for each i and $l \in F$.

We consider the angle $\pi/3$. Note that the angle $\pi/3$ can be constructed (why?). So the angle $\pi/3$ cannot be trisected iff the angle $\pi/9$ cannot be constructed, equivalently, the length $\cos(\pi/9)$ cannot be constructed. Find (with proof) the minimal polynomial of $\cos(\pi/9)$ over $\mathbb{Q}$, and deduce that the angle $\pi/3$ cannot be trisected.

(19) A regular n-gon can be constructed iff the angle $2\pi/n$ can be constructed (why?). Prove that a regular pentagon can be constructed by ruler and compass.

(20) Prove that -1 cannot be written as a sum of squares in $\mathbb{Q}(\omega\sqrt[3]{2})$, where $\omega = e^{2\pi i/3}$.

Hints:

1 (a) Use the structure theorem for finitely generated abelian groups. (b) Consider $A = \mathbb{Q}/\mathbb{Z}$.

2 (b) Use the product rule. (c) Use the universal property of the tensor product and part (b) to obtain an R-module homomorphism $\mathfrak{m} \otimes_R \mathfrak{m} \to \mathbb{C}$.

3 (a) Use right exactness of the tensor product and the natural isomorphism $R \otimes_R M \simeq M$, $r \otimes m \mapsto r \cdot m$ for any R-module M. (b) Use the presentation $R \to R^2 \to \mathfrak{m} \to 0$ for $\mathfrak{m}$ described in class and a similar presentation for $\mathfrak{m}^2$.

4 This is straightforward, but note that one has to check that (1) $F(\theta)$ is an R-module homomorphism, (2) $G(\psi)$ is a well defined R-module homomorphism (using the universal property of the tensor product), and (3) $G(\psi)$ is an S-module homomorphism, in addition to checking that $F \circ G = \mathrm{id}$ and $G \circ F = \mathrm{id}$.

5 Consider the exact sequence $R^n \to M \to C \to 0$, where the first homomorphism φ is given by $e_i \mapsto m_i$ and C is the cokernel of φ. Now use right exactness of $(\cdot) \otimes_R k$ and Nakayama's lemma.

6 This is similar to the case of the tetrahedron discussed in class.

7 What is the prime subfield of a field? What is the degree of a field extension?

8 Consider the fraction field $F(t)$ of the ring $F[t]$ of polynomials in a variable t with coefficients in a field F.

9 (a) Since $\deg f \leq 3$, it suffices to check f has no roots in $\mathbb{Q}$. If $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ has a root $\alpha \in \mathbb{Q}$, write $\alpha = a/b$ with $\gcd(a, b) = 1$, then a divides a_0 and b divides a_n. (b) Use the isomorphism $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/(f)$ and the Euclidean algorithm in $\mathbb{Q}[x]$.

10 First determine the minimal polynomial of α over $\mathbb{Q}$ and its factorization in $\mathbb{C}[x]$.

12 Determine the factorization of $x^n - 1$ into irreducibles over $\mathbb{Q}$ in each case.

13 (b) $e^{i\pi/4} = (1+i)/\sqrt{2}$.

14 If $F \subset K \subset L$ is a tower of field extensions, what is the relation between the degrees $[K : F]$, $[L : K]$, and $[L : F]$?

15 (b) If $\alpha \in K \setminus F$ what is the degree of the minimal polynomial of α over F? Complete the square. (c) Consider the finite field of order 4.

17 What are the possible values of $[F(\alpha) : F(\alpha^2)]$?

18 Use the formula for $\cos 3\theta$ in terms of $\cos\theta$ to determine the minimal polynomial of $\cos\pi/9$.

19 $\cos(2\pi/5) = (\zeta + \zeta^{-1})/2$ where $\zeta = e^{2\pi i/5}$. Now find the minimal polynomial of $\cos(2\pi/5)$ using the minimal polynomial of ζ. Alternatively, use the fact that $\theta = 2\pi/5$ is one solution of $\cos 2\theta = \cos 3\theta$.

20 $\mathbb{Q}(\omega\sqrt[3]{2})$ is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$ (why?).