Algebra III: Rings and Modules
Problem Sheet 3, Autumn Term 2022-23

John Nicholson

1. Prove that the two definitions of ring localisation given in lectures are equivalent. That is, let R be a commutative ring and let $S \subseteq R$ be a multiplicative submonoid. Show that there is a unique ring R' such that there exists a map $\iota : R \to R'$ with the following two properties:

   (i) $\iota(S) \subseteq (R')^\times$, i.e. everything in S gets mapped to a unit in R'.

   (ii) For all commutative rings A and maps $\varphi : R \to A$ with $\varphi(S) \subseteq A^\times$, there exists a unique $\widetilde{\varphi} : R' \to A$ such that $\varphi = \widetilde{\varphi} \circ \iota$.

   [First prove this in the case where R is an integral domain. The general case is more difficult.]

2. Let R be a unique factorisation domain, let F denote its field of fractions and let

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X].$$

   Show that, if $\frac{p}{q} \in F$ is a root of f for $p, q \in R$ with $\gcd(p,q) = 1$, then $p \mid a_0$ and $q \mid a_n$ in R. [This is a generalisation of the Rational Root theorem.]

3. Show that the following polynomials are irreducible in $\mathbb{Q}[X,Y]$:

$$3X^3Y^3 + 7X^2Y^2 + Y^4 + 2XY + 4X, \qquad 2X^2Y^3 + Y^4 + 4Y^2 + 2XY + 6.$$

4. We say a polynomial in $\mathbb{Z}[X,Y]$ is *primitive* if the greatest common divisor of its (integer) coefficients is one. Show that:

   (i) If $f, g \in \mathbb{Z}[X,Y]$ are primitive, then fg is primitive.

   (ii) If $f \in \mathbb{Z}[X,Y]$ is primitive, then $f \in \mathbb{Z}[X,Y]$ is irreducible if and only if $f \in \mathbb{Q}[X,Y]$ is irreducible. [This is the analogue of Gauss' lemma for multivariate polynomials.]

5. For each of the following elements $\alpha \in \mathbb{C}$ determine whether α is an algebraic integer and, if so, compute its minimal polynomial f_α.

$$(1+\sqrt{3})/2, \quad 2\cos(2\pi/7), \quad (1+i)\sqrt{3}, \quad \sqrt{5}/\sqrt{7}, \quad i + \sqrt{3}.$$

6. Let R be a commutative ring. Show that R is Noetherian if and only if every ideal $I \subseteq R$ is finitely generated.

7. Let R be a commutative ring. Give a proof or counterexample to each of the following statements:

   (i) If R is Noetherian, then R is an integral domain.

   (ii) If $R[X]$ is Noetherian, then R is Noetherian. [The converse to Hilbert's basis theorem.]

   (iii) Let $S \subseteq R$ be a multiplicative submonoid. If R is Noetherian, then $S^{-1}R$ is Noetherian.

8. Let R and S be rings. Show that every $R \times S$ module M is isomorphic to a product $M_1 \times M_2$, where M_1 is an R-module and M_2 is an S module, and the $R \times S$-module structure on $M_1 \times M_2$ is given by $(r, s) \cdot (m_1, m_2) = (rm_1, sm_2)$.

9. Let R be a ring. An R-module is M said to be *cyclic* if M it is generated by one element, and *simple* if M has no R-submodules other than 0 and M.

   (i) Show that any cyclic R module is isomorphic to R/I for some ideal I of R.

   (ii) Show that any simple R-module is cyclic.

   (iii) Show that M is a simple R-module if and only if M is isomorphic to R/I for some maximal ideal I of R.

10. Let R be a ring and M an R-module. Define the *endomorphism ring* of M to be set $\mathrm{End}_R(M) := \{f : M \to M \mid f \text{ is an } R\text{-module homomorphism}\}$ with pointwise addition and multiplication given by function composition. The *automorphism group* of M, denoted by $\mathrm{Aut}_R(M)$, is defined to be the group of units of $\mathrm{End}_R(M)$.

    (i) Show that a $\mathbb{Z}$-module is the same thing as an abelian group. Deduce that, for for an abelian group M, we have $\mathrm{End}(M) \cong \mathrm{End}_{\mathbb{Z}}(M)$ and $\mathrm{Aut}(M) \cong \mathrm{Aut}_{\mathbb{Z}}(M)$.

    (ii) Show that the two definitions of R-module given in lectures are equivalent. That is, for an abelian group M, show that the structure $\cdot : R \times M \to M$ of a left R-module on M is the same information as a ring homomorphism $\varphi : R \to \mathrm{End}(M)$.

    (iii) Let G be a group and M an abelian group. Show that an $R[G]$-module structure on M is equivalently an R-module structure on M and a homomorphism $\varphi : G \to \mathrm{Aut}_R(M)$.

    (iv) Let G be a group. Show that a $\mathbb{Z}[G]$-module is equivalently an abelian group M with a G-action, i.e. group homomorphism $G \to \mathrm{Aut}(M)$. [We often call this a G-module.]

    [Hint: To show that two definitions are equivalent, we need to establish a one-to-one correspondence. For example, you could show that (a) for every abelian group A, there exists a $\mathbb{Z}$-module M_A, (b) For every $\mathbb{Z}$-module M, there exists an abelian group $A(M)$, (c) $A(M_A) \cong A$ as abelian groups and $M_{A(M)} \cong M$ as $\mathbb{Z}$-modules.]

+11. If R is a ring, the *formal power series ring* $R[[X]]$ is the ring with elements

$$f = a_0 + a_1 X + a_2 X^2 + \cdots ,$$

where each $a_i \in R$. This has addition and multiplication the same as for polynomials, but without upper limits. Show that, if R is Noetherian, then $R[[X]]$ is Noetherian.