A3: Rings and Modules

Sheet E — HT21

This is a sheet with some extra questions for those who are interested. There is no expectation that these problems be completed. The problems are of quite variable difficulty; many of them are tough, in part because they ask for examples without a hint of what an example should look like. The order of the problems is roughly aligned with the order of the material in the notes, but because a lot of the language of modules is useful for talking about rings (see *e.g.* Exercise E.10) this is not perfectly respected.

E.1. The aim of this question is to identify the group structure of $U(\mathbb{Z}[\sqrt{2}])$. First, show that if $a+b\sqrt{2}$ is a unit then $2b^2-a^2 \in \{-1,1\}$; and then that $1+\sqrt{2}$ is the smallest unit bigger than 1. Hence show that the map

$$\mathbb{Z}\times(\mathbb{Z}/2\mathbb{Z}) \to U(\mathbb{Z}[\sqrt{2}]); (n,v) \mapsto (-1)^v(1+\sqrt{2})^n$$

is a well-defined isomorphism of groups.

E.2. Suppose that R is a ring and write $M_2(R)$ for the set of 2×2 matrices with entries in R and define addition and multiplication on $M_2(R)$ by

$$(A+B)_{i,j} := A_{i,j}+B_{i,j} \text{ and } (AB)_{i,j} := \sum_{k=1}^{2} A_{i,k}B_{k,j} \text{ for } 1 \leq i,j \leq 2.$$

Convince yourself that this is a ring. Write $\det A := A_{1,1}A_{2,2} - A_{1,2}A_{2,1}$. Show that if R is commutative then $A \in U(M_2(R))$ if and only if $\det A \in U(R)$. What if R is not commutative?

[*Hint: It may help to identity a ring R with elements $a,b \in R$ such that $ba = 1$ and $ab \notin U(R)$.*]

E.3. Find a commutative ring R and elements $a,b \in R$ such that $\langle a\rangle = \langle b\rangle$ but there is no $u \in U(R)$ with $a = ub$.

E.4. Show that the ring R is a field in each of the following cases.

(a) $R[X]$ is a PID;

(b) R is a commutative ring in which 0 is irreducible;

(c) R is a non-trivial commutative ring in which every non-unit is prime;

(d) R is an integral domain in which every sequence $(d_n)_{n=0}^{\infty}$ with $d_n \mid d_{n+1}$ (the opposite of the ACCP) has some $N \in \mathbb{N}_0$ such that $d_n \sim d_N$ for all $n \geq N$.

Tom Sanders: tom.sanders@maths.ox.ac.uk

E.5. Show that the set of entire functions $\mathbb{C} \to \mathbb{C}$, denoted $\mathcal{E}(\mathbb{C})$, is an integral domain. Show that the sum of two principal ideals is principal in $\mathcal{E}(\mathbb{C})$ – an integral domain with this property is called a **Bezout domain**. Show that if $f \in \mathcal{E}(\mathbb{C})$ is irredudible then it has at most one root and hence that $\mathcal{E}(\mathbb{C})$ is not a PID.

[*Hint: You may assume a Mittag-Leffler-type result that for any* $A \subset \mathbb{C}$ without *an accumulation point, and* $m : A \to \mathbb{N}^*$, *and any* $w_{n,\alpha} \in \mathbb{C}$ *for* $0 \leq n \leq m(\alpha)$ *there is an entire* f *with* $f^{(n)}(\alpha) = w_{n,\alpha}$ *for all* $\alpha \in A$ *and* $0 \leq n \leq m(\alpha)$.]

E.6. Suppose that R is a Euclidean Domain.

(a) Show that there is a Euclidean function f on R that such that $f(1) = 0$ and $f(ab) \geq f(a)$ for all $a, b \in R^*$.

For the remainder of the question assume that f satisfies the above properties.

(b) Show that if $a \mid b$ and $a \nsim b$ then $f(a) < f(b)$. In particular, $f(au) = f(a)$ iff $u \sim 1$.

Suppose, additionally, that f has unique remainders (and quotients) in the division algorithm, meaning that whenever $a, b \in R^*$ either $b \mid a$; or there is a *unique* pair $(q, r) \in R \times R^*$ such that $b = aq + r$ and $f(r) < f(a)$.

(c) Show that if $a, b, a+b \in R^*$ then $f(a+b) \leq \max\{f(a), f(b)\}$, and hence that $U(R) \cup \{0\}$ is a field; call it $\mathbb{F}$.

(d) Finally, show that if $R \neq \mathbb{F}$ then there is $a \in R^*$ such that for all $b \in R^*$ there is a unique $k \in \mathbb{N}_0$ and elements $q_0, \ldots, q_k \in \mathbb{F}$ with $q_k \neq 0$ such that $b = q_k a^k + \cdots + q_1 a + q_0$. Hence conclude that $R \cong \mathbb{F}[X]$.

E.7. Show that $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbb{F}_p[X]$ when p is a prime with $p \equiv 3 \pmod 7$ or $p \equiv 5 \pmod 7$.

E.8. Show that if $f \in \mathbb{Z}[X]$ is monic and $f \pmod p$ is irreducible for some prime p then f is irreducible. (When $f(X) = a_d X^d + \cdots + a_0$ then $f \pmod p$ is the polynomial in $\mathbb{F}_p[X]$ with coefficient of X^n being $a_n \pmod p$ for $0 \leq n \leq d$.) Show that $X^4 + 1$ is *not* irreducible in $\mathbb{F}_p[X]$ for any prime p. On the other hand show that $X^4 + 1$ *is* irreducible in $\mathbb{Z}[X]$. Is $X^4 + 1$ irreducible in $\mathbb{R}[X]$?

[*Hint: You may assume that if* $\mathbb{F}$ *is a finite field then* $U(\mathbb{F})$ *is cyclic, which is proved in Exercise IV.5; and also that for every odd prime* p *there is a field extension of* $\mathbb{F}_p$ *of degree* 2, *which follows from Exercise II.9.*]

E.9. Show that $X^p - X - 1$ is irreducible in $\mathbb{Z}[X]$ for p a prime.

Tom Sanders: tom.sanders@maths.ox.ac.uk

E.10. Write $\overline{\mathbb{Z}}$ for the set of $z \in \mathbb{C}$ for which there is a monic $p \in \mathbb{Z}[X]$ such that $p(z) = 0$. Show that $\alpha \in \overline{\mathbb{Z}}$ if and only if $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module, and hence that $\overline{\mathbb{Z}}$ is a ring. Show that $\overline{\mathbb{Z}}$ has no irreducible elements.

E.11. Suppose that $\phi : M \to N$ is R-linear map and every submodule of N is finitely generated, and every submodule of $\ker \phi$ is finitely generated. Show that every submodule of M is finitely generated. Hence show that if R is a PID then every submodule of R^n is finitely generated.

E.12. Suppose that $\mathbb{F}$ is a field. Use the Chinese Remainder Theorem to show that if $\lambda_1, \dots, \lambda_k \in \mathbb{F}$ are pairwise distinct and $a_1, \dots, a_k \in \mathbb{F}$, then there is a polynomial $p \in \mathbb{F}[X]$ of degree at most $k-1$ such that $p(\lambda_i) = a_i$ for all $1 \le i \le k$. What happens if $\mathbb{F}$ is replaced by $\mathbb{Z}$?

E.13. Suppose that M and N are R-modules for which there is an R-linear injection $M \to N$ and an R-linear surjection $M \to N$. Is there necessarily an R-linear bijection $M \to N$?

E.14. The set of integer-valued sequences (*i.e.* functions $\mathbb{N}_0 \to \mathbb{Z}$) has the structure of a $\mathbb{Z}$-module. Show that it is *not* free.

E.15. Suppose that R is a commutative ring and $\phi, \psi : R^n \to R^n$ are R-linear maps such that $\ker \phi = \ker \psi$ and $\mathrm{Im}\phi = \mathrm{Im}\psi$. Is it necessarily the case that there are R-linear isomorphisms $\sigma, \tau : R^n \to R^n$ such that $\phi = \sigma \circ \psi \circ \tau$?

[*Hint: It may help to reflect on rings with the properties described in Exercise E.3.*]

E.16. Show that if M is a finitely presented R-module, then *any* surjective R-linear map $\phi : R^m \to M$ has a finitely generated kernel. Hence give an example of a finitely generated module that is not finitely presented.

[*Hint: It may help to recall Exercise III.6.*]

Mathematical Institute, University of Oxford
Tom Sanders: tom.sanders@maths.ox.ac.uk