

IB GROUPS, RINGS AND MODULES

Lent Term 2023

Example Sheet 3 of 4

Rong Zhou

All rings in this course are commutative with a 1.

- (1) Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\omega]$ are Euclidean domains, where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. Show also that the usual Euclidean function $\phi(r) = N(r)$ does not make $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain. Could there be some other Euclidean function ϕ making $\mathbb{Z}[\sqrt{-3}]$ into a Euclidean domain?
- (2) Show that the ideal $(2, 1 + \sqrt{-7})$ in $\mathbb{Z}[\sqrt{-7}]$ is not principal.
- (3) Find an element of $\mathbb{Z}[\sqrt{-17}]$ that is a product of two irreducibles and also a product of three irreducibles.
- (4) Determine whether or not the following rings are fields, PIDs, UFDs, integral domains:
 $\mathbb{Z}[X]$, $\mathbb{Z}[X]/(X^2 + 1)$, $\mathbb{Z}[X]/(2, X^2 + 1)$, $\mathbb{Z}[X]/(2, X^2 + X + 1)$, $\mathbb{Z}[X]/(3, X^3 - X + 1)$.
- (5) Determine which of the following polynomials are irreducible in $\mathbb{Q}[X]$:
 $X^4 + 2X + 2$, $X^4 + 18X^2 + 24$, $X^3 - 9$, $X^3 + X^2 + X + 1$, $X^4 + 1$, $X^4 + 4$.
- (6) Let R be an integral domain. The *greatest common divisor* (gcd) of non-zero elements a and b in R is an element d in R such that d divides both a and b , and if c divides both a and b then c divides d .
 - (i) Show that the gcd of a and b , if it exists, is unique up to multiplication by a unit.
 - (ii) In lectures we have seen that, if R is a UFD, the gcd of two elements exists. Give an example to show that this is not always the case in an integral domain.
 - (iii) Show that if R is a PID, the gcd of elements a and b exists and can be written as $ra + sb$ for some $r, s \in R$. Give an example to show that this is not always the case in a UFD.
 - (iv) Explain briefly how, if R is a Euclidean domain, the Euclidean algorithm can be used to find the gcd of any two non-zero elements. Use the algorithm to find the gcd of $11 + 7i$ and $18 - i$ in $\mathbb{Z}[i]$.
- (7) Find all ways of writing the following integers as sums of two squares: 221 , 209×221 , 121×221 , 5×221 .
- (8) By considering factorisations in $\mathbb{Z}[\sqrt{-2}]$, show that the only integer solutions to the equation $x^2 + 2 = y^3$ are $x = \pm 5$, $y = 3$.

- (9) Let R be any ring.
- (i) Show that the ring $R[X]$ is a principal ideal domain if and only if R is a field.
 - (ii) Show that the ideal (X, Y) in $\mathbb{C}[X, Y]$ is not principal. Can the ideal (X^2, XY, Y^2) be generated by two elements?
- (10) Exhibit an integral domain R and a (non-zero, non-unit) element of R that is not a product of irreducibles.
- (11) Let \mathbb{F}_q be a finite field with q elements.
- (i) Show that the prime subfield K (that is, the smallest subfield) of \mathbb{F}_q has p elements for some prime number p . Show that \mathbb{F}_q is a vector space over K and deduce that $q = p^n$, for some n .
 - (ii) Assuming that a field with p^n elements exists, show that $\text{GL}_n(\mathbb{F}_p)$ contains an element of order $p^n - 1$.

Further Questions

- (12) (a) Consider the polynomial $f = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ in $\mathbb{C}[X, Y]$. Write it as an element of $(\mathbb{C}[X])[Y]$, that is collect together terms in powers of Y , and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X, Y]$.
- (b) Let F be any field. Show that the polynomial $f = X^2 + Y^2 - 1$ is irreducible in $F[X, Y]$, unless F has characteristic 2. What happens in that case?
- (13) Show that the subring $\mathbb{Z}[\sqrt{2}]$ of \mathbb{R} is a Euclidean domain. Show that the units are $\pm(1 \pm \sqrt{2})^n$ for $n \geq 0$.
- (14) If a UFD has at least one irreducible, must it have infinitely many (pairwise non-associate) irreducibles?
- (15) Use your answer to Question 11 to show that if p and ℓ are primes, and ℓ is odd, then every Sylow ℓ -subgroup of $\text{SL}_2(\mathbb{F}_p)$ is cyclic.
- (16) Let $\mathbb{F}_4 = \mathbb{F}_2[\omega]/(\omega^2 + \omega + 1) = \{0, 1, \omega, \omega + 1\}$, a field with four elements.

Show that the groups $\text{SL}_2(\mathbb{F}_4)$ and $\text{PSL}_2(\mathbb{F}_5)$ both have order 60. By exhibiting two Sylow 5-subgroups and using some questions from Example Sheet 1, or otherwise, show that they are both isomorphic to the alternating group A_5 . Show that $\text{SL}_2(\mathbb{F}_5)$ and $\text{PGL}_2(\mathbb{F}_5)$ both have order 120, but that only one of these is isomorphic to S_5 .

[You may find it helpful to show, using the Cayley-Hamilton theorem or otherwise, that the order of an element $I \neq A \in \text{SL}_2(\mathbb{F}_4)$ is uniquely determined by its trace.]

Email address: rz240@dpms.cam.ac.uk