Oxford University Department of Mathematics

Rings and Arithmetic 2 (for FHS Part A): Michaelmas Term 2005

More on ideals and quotient rings. Euclidean rings. The Gaussian integers.

Note: the following six problems are offered to give focus to tutorials. The wise and intelligent student will be trying many more exercises, however, from books, past examination papers, and other such sources.

1. Let R be a commutative ring with 1, let $e \in R$ and suppose that $e^2 = e$, $e \neq 0$ and $e \neq 1$. Define $f := 1 - e$ and let A, B be the principal ideals (e), (f) generated by e and f respectively. Show that $A \cap B = \{0\}$ and $A + B = R$ (thus in a natural sense $R = A \oplus B$). Deduce that $R \cong R/A \times R/B$.

2. Let R, S be commutative rings with unity. Prove that if A is an ideal in the direct product $R \times S$ (the ring consisting of all pairs with componentwise addition and multiplication) then there exist ideals X of R and Y of S such that $A = X \times Y$.

3. Let R be a commutative ring with 1. An ideal A in R is said to be *prime* if $A \neq R$ and $ab \in A \Rightarrow a \in A$ **or** $b \in A$.

(i) Show that an ideal A is prime if and only if R/A is an integral domain.

(ii) Show that a maximal ideal is prime.

(iii) Show that if A, B are prime ideals then $A \cap B$ is prime if and only if $A \subseteq B$ or $B \subseteq A$.

(iv) Which ideals are prime in $\mathbb{Z}$?

4. Let F be a field. By an arithmetic operation we mean an operation of addition, subtraction, multiplication or division of two members of F. Given $f, g \in F[x]$, and given that g is not the zero polynomial, division of f by g is the process of finding polynomials $q, r \in F[x]$ (‘quotient’ and ‘remainder’ respectively) such that $f(x) = q(x)g(x) + r(x)$ and either r is the zero polynomial or $\deg r < \deg g$.

(i) Show that if $\deg f = n$ and $\deg g = m$, where $m \leq n$, then division of f by g costs at most $(2m+1)(n-m+1)$ arithmetic operations.

(ii) Hence prove that if $\deg f \leq n$ and $\deg g \leq m$ then the Euclidean Algorithm discovers $\mathrm{hcf}\,(f, g)$ at a cost of no more than $2mn + m + n + 1$ arithmetic operations.

5. Which of the following are euclidean rings? As always, justify your answers.

(i) $\mathbb{Z}[x]$;

(ii) $\mathbb{Q}[x, y]$, the ring of polynomials in two variables with rational coefficients;

(iii) $\mathbb{Z}[\sqrt{2}]$ (defined as $\{\, x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Z} \,\}$);

(iv) $\mathbb{Z}[\sqrt{-5}]$ (defined as $\{\, x + y\sqrt{-5} \in \mathbb{C} \mid x, y \in \mathbb{Z} \,\}$).

6. Let $R := \mathbb{Z}[\mathrm{i}]$, let p be an ordinary integer prime, and let A be the principal ideal (p) generated by p in R. Show that if $p \equiv 3 \pmod 4$ then R/A is a field with p^2 elements. Show also that if $p \equiv 1 \pmod 4$ then $R/A \cong \mathbb{F}_p \times \mathbb{F}_p$. What can you say about R/A when $p = 2$?

ΠMN: Queen’s: 13.x.2005