Groups Rings and Fields, Example Sheet 2

Dr Alessio Corti a.corti@dpmms.cam.ac.uk

February, 2003

(1)

1. Suppose that $f\colon R \to S$ is a ring homomorphism. Show that if $J \subset S$ is an ideal in S, then $f^{-1}(J) = \{a \in R \mid f(a) \in J\}$ is an ideal in R.
2. What are the ideals in the ring $\mathbb{Z}$? What are the ideals in the quotient ring $\mathbb{Z}/(n)$?
3. For which values of n and m is there a homomorphism $\phi\colon \mathbb{Z}/(n) \to \mathbb{Z}/(m)$? Is the homomorphism unique?

(2) Let R, S be rings. Persuade yourselves that $R\times S$ is naturally a ring (as an additive group $R \times S$ is the direct product of $R, +$ with $S, +$; the multiplication is defined as $(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$).

1. Suppose that $f\colon R \to S$ and $g\colon R \to T$ are ring homomorphisms. Show that $(f, g)\colon R \to S \times T$ defined by $(f, g)(r) = (f(r), g(r))$ is a ring homomorphism.
2. Suppose that $f\colon R \to T$ and $g\colon S \to T$ are ring homomorphisms. Is $f + g\colon R\times S \to T$ defined by $(f+g)(r, s) = f(r)+g(s)$ a ring homomorphism?

(3) Show that if I and J are ideals in R, then so is $I \cap J$. Show that the quotient $R/(I \cap J)$ is isomorphic to a subring of the product $R/I \times R/J$.

(4) Let k be a field, and let $R = k[X, Y]$ be the polynomial ring in two variables.

1. Let I be the principal ideal generated by the element $X - Y$ in R. Show that $R/I \cong k[X]$.
2. What can you say about R/I when I is the principal ideal generated by $X^2 + Y$?
3. Let $I \subset R$ be the principal ideal generated by $X^2 - Y^2$. Show that R/I is not an integral domain. Exhibit an injective ring homomorphism $R/I \to k[x] \times k[y]$ and determine its image. Interpret these results geometrically in terms of polynomial functions on the "coordinate axes" in k^2.

(5) An ideal $I \subset R$ is *prime* if $ab \in I$ implies $a \in I$ or $b \in I$. Show that I is prime if and only if R/I is an integral domain.

(6) Find an irreducible polynomial $f(X) \in \mathbb{F}_3[X]$ of degree 3. Show that $\mathbb{F}_3[X]/(f)$ is a field with 27 elements.

(7) What are the units in $\mathbb{Z}/(12)$? What are the ideals in $\mathbb{Z}/(12)$? Is $\mathbb{Z}/(12)$ a PID? (I am not sure I said it clearly in the lectures but, by definition, a principal ideal domain is an integral domain.)

(8) In this question we work in the ring $R = \mathbb{Z}[i]$ of Gaussian integers.

1. Show that the units in the ring are ± 1 and $\pm i$.
2. Show that, up to multiplication by a unit, the primes in the ring the integer primes $p \equiv 3 \mod 4$, and the $a \pm ib$ where $p = 2$ or $p = a^2 + b^2 \equiv 1 \mod 4$ is an integer prime. (Recall from quadratic mathematics that an integer prime p is the sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$).
3. What is the greatest common divisor in $\mathbb{Z}[i]$ of the elements $3 - 4i$ and $4 + 3i$?
4. What is the greatest common divisor in $\mathbb{Z}[i]$ of the elements $11 + 7i$ and $18 - i$?

(9)

1. Show that $X^4 + 2X + 2$ and $X^4 + 18X^2 + 24$ are irreducible in $\mathbb{Q}[X]$.
2. Are $X^3 - 9$ and $X^4 - 8$ irreducible in $\mathbb{Q}[X]$? (You better approach this question with "bare hands").
3. Show that $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbb{Q}[X]$.
4. Are $X^3 + X^2 + X + 1$ and $X^4 + X^3 + X + 1$ irreducible in $\mathbb{Q}[X]$?
5. Show that $X^4 + 1$ is irreducible in $\mathbb{Q}[X]$.
6. Show that $X^4 + 4$ factorizes in $\mathbb{Q}[X]$ into irreducible quadratic factors.

(10) Consider the polynomial $f(X, Y) = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ 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 hence show, using the Eisenstein criterion for polynomials with coefficients in $\mathbb{C}[X]$, that f is prime in $\mathbb{C}[X, Y]$. Do the same for $f(X, Y) = X^3Y + X^2Y^2 + Y^3 - Y^2 + X + Y + 1$.

(11) Following the outline given in the lectures, show that if p is prime then $X^{p-1} + \cdots + X + 1$ is irreducible in $\mathbb{Z}[X]$. Factorize $X^3 + X^2 + X + 1$ and $X^5 + X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$. Suppose $X^{n-1} + \cdots + X + 1$ is irreducible in $\mathbb{Z}[X]$. Does it follow that n is prime?