THE UNIVERSITY of ADELAIDE

The University of Adelaide
School of Computer and Mathematical Sciences

Fields and Modules
Diagnostic Quiz

1. Let x be a positive integer and let $[x]$ denote the residue class of x modulo n, where $n \geq 2$. Prove that $[x]$ is a unit in the ring $\mathbb{Z}/n$ if and only if $\gcd(x, n) = 1$. (Here $\mathbb{Z}/n$ denotes the ring of integers modulo n, under addition and multiplication mod n.)

2. Let R be a commutative, unital ring and suppose that the only ideals in R are the trivial ideal $\{0\}$, and R. Prove that R is a field.

3. Which of the following sets I are ideals in the ring $\mathbb{Z}[x]$?

(a) the set I of polynomials in $\mathbb{Z}[x]$ with non-zero constant term;

(b) the set I of polynomials in $\mathbb{Z}[x]$ with constant term equal to zero;

(c) the set I of polynomials in $\mathbb{Z}[x]$ whose constant term is a multiple of 2;

(d) the set I of polynomials in $\mathbb{Z}[x]$ in which only even powers of x appear.

Solutions

1. To say that an element a of a unital ring R is a *unit* is to say that there is an element $b \in R$ such that $ab = 1 = ba$, where $1 \in R$ denotes the unit. Therefore, we must show that there is an integer y such that $[x] \cdot [y] = 1$ in $\mathbb{Z}/n$ if and only if $\gcd(x, n) = 1$.

Let $d = \gcd(x, n)$. We have $[x] \cdot [y] = 1$ if and only if $n|(xy - 1)$, if and only if there is a $k \in \mathbb{Z}$ such that $xy = 1 + kn$. Therefore $d|x$ and $d|n$ and hence $d|(xy - kn)$, i.e. $d|1$. Therefore $d = 1$. Conversely, suppose $d = 1$. Then, by the Euclidean Algorithm, there exist $u, v \in \mathbb{Z}$ such that $1 = xu + vn$ and so $xu = 1 \mod n$, i.e. $[x] \cdot [u] = 1$ in $\mathbb{Z}/n$.

2. Suppose that R is a field. Let $I \subseteq R$ be an ideal. Suppose that $I \neq \{0\}$. We will prove that $I = R$. It suffices to show that $1 \in I$, since then $x = x1 \in I$ for all $x \in R$. Since $I \neq \{0\}$, there exists $x \in I$, $x \neq 0$. Since R is a field, x is a unit and hence there exists $y \in R$ such that $xy = 1$. Therefore $1 \in I$, since $x \in I$ and I is an ideal.

For the converse, suppose that R is a commutative, unital ring whose only ideals are $\{0\}$ and R. We will prove that R is a field. We need to prove that every non-zero $x \in R$ is a unit. Consider the principal ideal (x) generated by x. Since $x \neq 0$, we must have $(x) = R$ by the hypothesis on R. Therefore, $1 \in (x)$ and so there exists $y \in R$ such that $xy = 1$. Hence x is a unit (since R is commutative).

Recall that that if R is a ring and $r \in R$, then the *principal ideal* generated by r is the smallest ideal of R containing r. If R is commutative, then $(r) = \{ ar \mid a \in R \}$.

3. (a) the set I is not an ideal, since it is not an additive subgroup of $\mathbb{Z}[x]$ (it does not contain the additive identity, i.e. the zero polynomial).

(b) the set I is an ideal; for example, I is the kernel of the ring homomorphism $f\colon \mathbb{Z}[x] \to \mathbb{Z}$ defined by $f(a_0 + a_1 x + \cdots + a_n x^n) = a_0$ (recall that the kernel of a ring homomorphism $\phi\colon R \to S$ is always an ideal of R).

(c) the set I is an ideal; for example I is the kernel of the composite ring homomorphism $g \circ f$, where $f\colon \mathbb{Z}[x] \to \mathbb{Z}$ is the homomorphism from (b) and $g\colon \mathbb{Z} \to \mathbb{Z}/2$ is the ring homomorphism given by reduction mod 2, i.e. $g(n) = n \mod 2$.

(d) the set I is not an ideal; while it is an additive subgroup of $\mathbb{Z}[x]$ it is not closed under multiplication by polynomials in $\mathbb{Z}[x]$ — for example $p(x) = x^2 \in I$, but $xp(x) = x^3 \notin I$.