ACE Algebraic Number Theory – Pre-Quiz

Questions

1. Determine the unit group of the ring $\mathbb{Z}/12\mathbb{Z}$ of integers modulo 12.
2. Let R be a commutative ring with identity. Explain why every maximal ideal in R is prime. Is the converse true?
3. Show that the rings $\mathbb{R}[x]/\langle x^2 + 1\rangle$ and $\mathbb{C}$ are isomorphic.

Solutions

1. An element $[x] \in \mathbb{Z}/12\mathbb{Z}$ is invertible iff $\gcd(x, 12) = 1$. Thus the set of units is $U = \{[1], [5], [7], [11]\}$. To understand the group structure of U, notice that

$$5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \bmod 12.$$

   Thus every element of U is its own inverse. The only four element group with this property is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. Let $M \subset R$ be a maximal ideal. Then R/M is a field, which is thus also an integral domain, which implies that M is a prime ideal.

   The converse is false, however, since $\{0\} \subset R$ is a prime ideal which is not maximal.

3. Consider the map $e : \mathbb{R}[x] \to \mathbb{C}$, $e : f(x) \mapsto f(i) \in \mathbb{C}$, which evaluates polynomials at i. It is easy to see that this map is a ring homomorphism and is surjective. It thus remains to show that $\ker e = \langle x^2 + 1 \rangle$ and then the result follows from the First Isomorphism Theorem.

   To show $\ker e = \langle x^2 + 1 \rangle$, we note that the minimal polynomial of i over $\mathbb{R}$ is $x^2 + 1$, and so any polynomial $f(x) \in \mathbb{R}[x]$ has root i iff f is divisible by $x^2 + 1$.

   For those not familiar with minimial polynomials, we can also show this directly.

   First, if $f(x) \in \langle x^2 + 1 \rangle$, then clearly $f(i) = 0$, so $f \in \ker e$.

   Conversely, suppose that $f \in \ker e$, so $f(i) = 0$. Now since the coefficients of f are real, it follows that

$$0 = \overline{0} = \overline{f(i)} = \overline{f}(\overline{i}) = f(-i),$$

   where $\bar{\cdot}$ denotes complex conjugation. So $f(x)$ is divisible by both $x - i$ and $x + i$ in $\mathbb{C}[x]$. Hence $f(x)$ is divisible by $(x - i)(x + i) = x^2 + 1$, which means that $f(x) \in \langle x^2 + 1 \rangle$, as required.