LECTURE 15.

ALIREZA SALEHI GOLSEFIDY

1. Evaluation map.

Let R be a subring of S. Then for any $s \in S$ and any polynomial $p(x) \in R[x]$ we can evaluate $p(s) \in S$. This gives us a nice homomorphism from $R[x]$ to S.

Q: What is the kernel of the evaluation map?

A: By the definition, kernel consists of polynomials $p(x)$ which vanish at s, i.e. $\{p(x) \in R[x] |\, p(s) = 0\}$.

Example 1. *Let $f : \mathbb{R} \to \mathbb{C}$ be given as $f(p(x)) := p(i)$. Then f is an onto homomorphism and* $\ker(f) = \{p(x)|\, p(i) = 0\}$. *We know that $\mathbb{R}[x]$ is a PID. So* $\ker(f)$ *is a principal ideal. We also know that it is generated by a non-zero polynomial of smallest degree in* $\ker(f)$. *By the definition, $x^2 + 1 \in \ker(f)$ and* $\ker(f)$ *does not contain any degree 0 and degree 1 polynomials. Hence* $\ker(f) = \langle x^2 + 1\rangle$. *Thus by the isomorphism theorem we have*

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \simeq \mathbb{C}.$$

Corollary 2. *The ideal generated by $x^2 + 1$ in $\mathbb{R}[x]$ is a maximal ideal.*

2. Irreducible polynomials.

Definition 3. A non-unit polynomial $f \in R[x]$ is called irreducible if $f(x) = p(x)q(x)$ implies that either $p(x)$ or $q(x)$ is unit.

Example 4. *Any prime element in $\mathbb{Z}$ is an irreducible polynomial in $\mathbb{Z}[x]$.*

Example 5. $x^2 + 1$ *is an irreducible polynomial in $\mathbb{R}[x]$. But it is not irreducible over $\mathbb{C}$.*

Proof. We know that the ideal generated by $x^2 + 1$ is maximal. So if $x^2 + 1 = p(x)q(x)$, then either $p(x)$ or $q(x)$ is a multiple of $x^2 + 1$. So one of them is of degree at least 2, which means the other one is of degree 0. But any degree 0 polynomial in $\mathbb{R}[x]$ is a unit.

Over $\mathbb{C}$, we have $x^2 + 1 = (x + i)(x - i)$ and neither $x + i$ nor $x - i$ are unit. □

Lemma 6. *Le F be a field. $f(x) \in F[x]$ is irreducible if and only if $\langle f(x)\rangle$ is a maximal ideal.*

Proof. Let us assume that $f(x)$ is irreducible and $\langle f(x)\rangle$ is not maximal. So there is a proper ideal I such that

$$\langle f(x)\rangle \subsetneq I \subsetneq F[x].$$

Since $F[x]$ is PID, there is $h(x) \in F[x]$ such that $I = \langle h(x)\rangle$. As $f(x) \in I$, we have that $f(x) = h(x)p(x)$ for some $p(x) \in F[x]$. Since $f(x)$ is irreducible, either $h(x)$ or $p(x)$ is unit.

If $h(x)$ is unit, then $I = F[x]$, which is a contradiction.

If $p(x)$ is unit, then $h(x) \in \langle f(x)\rangle$. This implies $\langle f(x)\rangle = I$ which is a contradiction.

Date: 2/15/2012.

Now assume that $\langle f(x)\rangle$ is a maximal ideal and $f(x) = p(x)q(x)$. So $p(x)q(x) \in \langle f(x)\rangle$. Since $\langle f(x)\rangle$ is a maximal ideal, it is also a prime ideal. Thus either $p(x)$ or $q(x)$ is a multiple of $f(x)$, which means one of them is of the same degree as $f(x)$ and the other one is of degree 0 (Notice that $f(x)$ cannot be zero!). Any degree 0 polynomial in $F[x]$ is unit, which finishes the proof. $\square$

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu