

Handout 16: Back to quotient rings and irreducibility

Let's get back to rings. We're about to use the FHT to prove some pretty neat relationships between fields, quotient rings, and irreducible polynomials. Before we get too deep into those correspondences, let's tack on a definition that will be crucial in later studies:

Definition. Let R be an integral domain (in particular, R could be a field). We define that *characteristic* of R , $\text{char}(R)$, to be the additive order of the multiplicative identity if this order is finite, and 0 otherwise.

Thus $n = \text{char}(R)$ satisfies $n1_R = 0$, and no smaller n gives us this identity.

Examples. What is $\text{char}(R)$ if R is...

(1) \mathbb{Z} ?

(2) \mathbb{Z}_m ?

(3) \mathbb{R} , \mathbb{C} , or \mathbb{Q} ?

Proposition. Let $r \in R$, with R an integral domain. Then the additive order of r is $\text{char}(R)$.

Proof. Just factor nr and use the definition of $\text{char}(R)$:

Proposition. For any integral domain R , $\text{char}(R)$ is either 0 or prime.

Proof. Let $n = \text{char}(R) \neq 0$. Then suppose BWOC that $n = \ell \cdot m$, for $\ell, m < n$...

Your textbook uses the FHT to demonstrate a connection between the characteristic of a ring and its prime field:

Proposition (3.110). The integral domain R has prime field isomorphic to \mathbb{Z}_p if $\text{char}(R) = p$ is prime, and prime field isomorphic to \mathbb{Q} otherwise.

Okay, we're now ready to launch ourselves headlong into a study of quotient rings and finite fields. The first step on our journey is a familiar result which we can obtain in an unfamiliar way:

Proposition (Example 3.111). Let $f : \mathbb{R}[x] \rightarrow \mathbb{C}$ be defined by $f(x) = f(i)$, where $i^2 = -1$. Then $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Proof. Use the FHT, and the fact that in a polynomial PID (like $\mathbb{R}[x]$!), every ideal is generated by the monic polynomial of least degree it contains.

This last result is a special case of a much much much *much* more general

Theorem (3.112). Let k be a field and let $I = (p(x))$ where $p \in k[x]$ is a nonconstant polynomial. The following statements are then equivalent:

- (1) $k[x]/I$ is a field.
- (2) $k[x]/I$ is an integral domain.
- (3) $p(x)$ is irreducible over k .

Proof. Prove (1) \Rightarrow (2) \Rightarrow (3); the first implication is trivial, the second is easily done as a contrapositive proof, and the third requires the fact that if $f \in k[x]$ and $p \nmid f$, then $(p, f) = 1$. Here's some room for you to clean it up:

Notice that this theorem is a nice generalization of the fact that $\mathbb{Z}_m \cong \mathbb{Z}/(m)$ is a field (and an integral domain!) if and only if m is prime. Wow!

As incredible as it might seem, the next results are even cooler:

Proposition (3.113). Let k be a field, and let $p(x) \in k[x]$ be irreducible. Then $k[x]/(p(x))$ is a field containing an isomorphic copy of k and a root, z , of $p(x)$. (That is, p is not irreducible over this new field.) Moreover, if $g \in k[x]$ and $g(z) = 0$, then $p(x)|g(x)$.

Proof. Let $I = (p(x))$. The first claim follows from the facts that $p(x)$ is irreducible and that the natural map from $k[x]$ to $k[x]/I$, when restricted to k , gives an injection from k to $k[x]/I$. That is, what is the image of $a \in k$ in $k[x]/I$?

Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Next we check that $z = x + I$ is a root of the polynomial $p^*(x) = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n$:

Finally, to prove the “Moreover, ...” statement, Note that if $z = x + I$ is a root of g , then $g(x)$ is in the kernel of the natural map to $k[x]/I$. What’s this mean, since $I = (p(x))$?

Theorem (3.114). Let k be a field and let $f \in k[x]$ be a polynomial of degree $n \geq 1$. If $I = (f(x))$ then every element of $k[x]/I$ can be written uniquely as some $b_0 + b_1z + \cdots + b_{n-1}z^{n-1}$ for $b_i \in k$ and $z = x + I$ is a root of f .

Proof. Start out with an arbitrary $h(x) + I$, and use the Division Algorithm to divide h by f . What happens?

Uniqueness isn't hard, either: if you've got two representations, say $r(z)$ and $r'(z)$, take their difference to get a new polynomial with root z and degree $n - 1 < n$. What then?

Notice that this last theorem doesn't require f to be irreducible; when f is irreducible, cool stuff happens, though, as we shall soon see!

Homework. Since I'll be handing out Exam 2 on Wednesday, I'll give you nothing new homework-wise for this week. Nice, aren't I?