

Handout 17: Quotient rings and finite fields, II

Let's pick up right where we left off. Our last result (Theorem 3.114) essentially gave us the following

Corollary (3.115). If $f(x) \in \mathbb{Z}_p[x]$ is irreducible and $\deg(f) = n$, then $\mathbb{Z}_p[x]/(f(x))$ is a finite field of order p^n .

There's more:

Fact. Let k be a finite field. Then there exists a prime p and positive integer n such that $|k| = p^n$.

The proof of this last fact requires a bit of group theory we haven't discussed. If you're interested, check out Theorem 2.147 in the text and see if you can piece together a rough proof of the fact above using that theorem.

We've seen now that $k[x]/(p(x))$ is a field if p is irreducible over k , and this new field contains a root, z , of p (which couldn't have existed in k since p was irreducible).

Definition. If E is a field, k is a subfield of E , and $z \in E$, then $k(z)$ (read " k adjoin z ") is the smallest subfield of E containing both k and z . That is,

$$k(z) = \bigcap \{F \leq E \mid k \cup \{z\} \subseteq F\}.$$

Examples.

(1) What's $\mathbb{R}(i)$?

(2) Describe $\mathbb{Q}(\sqrt{2})$ as a set.

(3) What's $k(z)$, if $z \in k$?

Notice that we've shown $k[x]/(p(x)) \cong k(z)$, for $z = x + (p(x))$.

The interplay between various quotient rings is rich:

Proposition (3.116). Let k be a subfield of K and let $z \in K$.

- (i) If $f(z) = 0$ for some polynomial $f \in k[x]$, then $p(z) = 0$ for some *irreducible* $p \in k[x]$.
- (ii) If $p \in k[x]$ is irreducible and $p(z) = 0$, then there is an isomorphism $\phi : k[x]/(p(x)) \rightarrow k(z) \leq K$ satisfying $\phi(x + (p(x))) = z$ and $\phi(a) = a$ for all $a \in k$.
- (iii) If z and z' are both roots of p in K , then there is an isomorphism $\theta : k(z) \rightarrow k(z')$ with $\theta(z) = z'$ and $\theta(a) = a$ for all $a \in k$.
- (iv) Each element of $k(z)$ can be uniquely written as $b_0 + b_1z + \cdots + b_{n-1}z^{n-1}$ for some $b_i \in k$, provided $\deg(p) = n$.

Personally I think (iii) is the coolest part of this proposition. Here's room for a picture that gives us an idea of what's going on there:

Proof of Proposition 3.116. For (i), factor f into irreducibles and use the evaluation map, plugging in z . What happens?

For (ii), first show that $\text{im}(\phi)$ is a subfield of K containing both k and z . Then argue that $\text{im}(\phi) \subseteq k(z)$ holds as well:

For (iii), find the right composition of the maps you obtain from (ii) applied to both z and z' . A picture says it best:

Finally, for (iv), use the decomposition of elements of $k[x]/(p(x))$ given by Theorem 3.114; why is this decomposition unique?

Your text gives a short proof of the following nice

Corollary (3.117). If k is a field and $p \in k[x]$ is irreducible, then if $\alpha \in k[x]/(p(x))$ is a root of some nonzero polynomial in $k[x]$, there is a unique monic irreducible polynomial $h \in k[x]$ having root α .

Existence follows from the previous theorem, and uniqueness follows a by-now-standard greatest-common-divisor argument.

Notice that if we start with an irreducible $p \in k[x]$ and we manage to find a root z in a larger field $K \geq k$, we *can* factor p over K . If we keep tearing off roots, extracting linear terms, maybe we can eventually factor p completely:

Definition. We say that the polynomial $f(x) \in k[x]$ *splits* over the larger field K if p can be written as a product of linear factors in $K[x]$.

Examples. Find the smallest field over which $x^3 - 2 \in \mathbb{Q}[x]$ splits.

What do you suppose is the smallest field over which any $f(x) \in \mathbb{C}[x]$ splits?

Theorem (3.118; due to Kronecker). If k is a field and $f(x) \in k[x]$ is a nonconstant polynomial, then there is a field $K \geq k$ such that f splits over K .

Proof. Induct on the degree of f ! You'll want to modify the statement of the theorem in order to grant us a little more flexibility: we'll allow ourselves to consider $f(x)$ as an element of any larger polynomial ring $E[x]$ where E an *intermediate* field, $k \leq E \leq K$.

Here's some room to wrap things up, considering two cases (f is irreducible, and f is not irreducible):

Your text now includes a proof that for any prime p and any q there is a field with exactly p^n elements; we'll hold off on that for now and pick up next time with some basic Galois theory. We'll begin by experimenting with isomorphisms between various quotients of finite-field polynomial rings.