Rutgers University: Algebra Written Qualifying Exam

January 2018: Problem 5 Solution

Exercise. Let I be a maximal ideal of $\mathbb{Z}[x]$. Prove that $\mathbb{Z}[x]/I$ is a finite field.

Solution.

Theorem: Let R be a commutative ring with unity and I be an ideal of R. Then

$$R/I \text{ is a field} \iff I \text{ is a maximal ideal of } R$$

*To see a detailed proof for why $\mathbb{Z}[x]/I$ is a field, look at the bottom of the document.

$\implies \mathbb{Z}[x]/I$ is a field

$\implies char(\mathbb{Z}[x]/I) = 0$ or p for some prime p

Case 1: $char(\mathbb{Z}[x], I) = p > 0$.

$\implies \mathbb{Z}[x]/I = \mathbb{Z}_p[x]/I'$ where I' is a maximal ideal of $\mathbb{Z}_p[x]$

because if $char(\mathbb{Z}[x]/I) = p$, then $\underbrace{1 + \cdots + 1}_{p \text{ times}} = p \equiv 0$ so $\mathbb{Z}[x]/I \cong \mathbb{Z}_p[x]/I'$

and we know $\mathbb{Z}_p[x]/I'$ must be a field so I' has to be a maximal ideal

$p \equiv 0 \in F \implies p \in I$

$\implies \langle p \rangle \subseteq I$ (since I is an ideal, $\forall r \in R, i \in I$, we have $ir \in I$)

By the **third isomorphism theorem:** If R is a ring, I an ideal and J an ideal s.t. $I \subseteq J \subseteq R$, then

(a) J/I is an ideal of R/I (every ideal has this form)

(b) $(R/I)/(J/I) \cong R/J$

(Note: if we replace J with a subring A then (a) holds resp. subring instead of ideal)

So $I/\langle p \rangle$ is an ideal of $\mathbb{Z}[x]/\langle p \rangle = \mathbb{Z}_p[x]]$

$\langle p \rangle = \{pf(x) : f(x) \in \mathbb{Z}[x]\}$

And $(\mathbb{Z}[x]/\langle p \rangle) \,/\, (I/\langle p \rangle) \cong \mathbb{Z}[x]/I = F$

Theorem: For any field K, $K[x]$ is a principal ideal domain

$\implies \mathbb{Z}_p[x]$ is a PID so I' is a principal ideal

$\implies I' = \langle g(x) \rangle$ for some $g(x) \in \mathbb{Z}_p[x]$

Look at $\deg(g)$: if $\deg(g) = m$, then

$|\mathbb{Z}_p[x]/I'| = |Z_p[x]/\langle a_m x^m + \ldots a_1 x + a_0 \rangle| = \#$ of polys in $\mathbb{Z}_p[x]$ with deg$< m$

(This is because $\mathbb{Z}_p[x]$ is a Euclidean domain) $|\mathbb{Z}[x]/I| = |\mathbb{Z}_p[x]/\langle g \rangle| = p^m$

Case 2: $char(\mathbb{Z}[x]/I) = 0$ (want to get a contradiction)

Choose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in I$ of minimal degree

pick prime p s.t. $p \mid a_n$

Since $\mathbb{Z}[x]/I$ is a field and $p \neq 0$, p has an inverse $h(x) \in \mathbb{Z}[x]/I$

$\implies ph(x) = 1$

$\implies ph(x) - 1 = 0_F \in I$ $\qquad$ (0_F is the elements in I)

$\implies ph(x) - 1 \in I$

(solution continued on next page)

Solution.

$\mathbb{Z}[x]$ is not a Euclidean domain but $\mathbb{Q}[x]$ is and $\mathbb{Z}[x] \subset \mathbb{Q}[x]$.
Let $d(x) = \gcd(f(x), ph(x) - 1)$ in $\mathbb{Q}[x]$
$\implies d(x) = u(x)f(x) + v(x)[ph(x) - 1]$ for some $u(x), v(x) \in \mathbb{Q}[x]$
Clear the denominators by multiplying by some $r \in \mathbb{Z}$ to get back to $\mathbb{Z}[x]$
$r \cdot d(x) \in \mathbb{Z}[x]$ and

$$\begin{aligned} r \cdot d(x) &= ru(x)f(x) + rv(x)[ph(x) - 1] \\ &= u'(x)f(x) + v'(x)[ph(x) - 1] \qquad \text{where } u' = ru \in \mathbb{Z}[x] \text{ and } v' = rv \in \mathbb{Z}[x] \end{aligned}$$

Since $u', v' \in \mathbb{Z}[x]$ and $f(x), [ph(x) - 1] \in I$,

$$u'(x)f(x) \in I \qquad \text{and} \qquad v'(x)[ph(x) - 1] \in I$$

$\implies rd(x) = u'f(x) + v'[ph(x) - 1] \in I$

Since $d(x) = \gcd(f(x), ph(x) - 1)$, clearly $d(x) \mid f(x)$
$\implies rd(x) \mid rf(x)$ and $rd(x) \in I$ and $\deg(rf(x)) = \deg(f(x))$ minimal
$\implies \deg(d(x)) = \deg(f(x))$ and $ad(x) = f(x)$ for some $a \in \mathbb{Q} \backslash \{0\}$
$\implies$ In $\mathbb{Q}[x]$, $d(x) \mid [ph(x) - 1]$ so $b(x)d(x) = ph(x) - 1$ for some $b(x) \in \mathbb{Q}[x]$
$\implies \frac{1}{a}b(x)f(x) = ph(x) - 1$
$\implies f(x) \mid [ph(x) - 1]$ in $\mathbb{Q}[x]$
So, $f(x) \mid [ph(x) - 1$ in $\mathbb{Z}[x]$

$$\begin{aligned} &\implies ph(x) - 1 = f(x)g(x) \qquad \text{for some } g \in \mathbb{Z}[x] \\ &\implies -1 \equiv f(x)g(x) \mod p \\ &\implies f(x)(-g(x)) \equiv 1 \mod p \\ &(a_nx^n + \cdots + a_1x + a_0)(b_mx^m + \cdots + b_1x + b_0) \equiv 1 \mod p \\ &\implies \left.\begin{matrix} b_m \equiv 0 \mod p \\ \vdots \\ b_0 \equiv 0 \mod p \end{matrix}\right\} \text{to have zero as a leading coefficient} \\ &\implies g \equiv 0 \mod p \end{aligned}$$

$\implies$ not a unit! this is a contradiction!

Proof that $\mathbb{Z}[x]/I$ is a field

$\mathbb{Z}[x]$ is a commutative ring with unity, and $\mathbb{Z}[x]/I$ is also a commutative ring with unity.
Also if I is a proper ideal of $\mathbb{Z}[x]$ then $\mathbb{Z}[x]/I$ is not the trivial ring.
Therefore, it suffices to prove that every nonzero element in $\mathbb{Z}[x]/I$ has a multiplicative inverse.

Let I be a maximal ideal of $\mathbb{Z}[x]$ and $a \notin I$.
Let J be the ideal $J = \{ab + x | b \in \mathbb{Z}[x], x \in I\}$.
Then, since I is a maximal ideal and $I \subsetneq J$, it follows that $J = \mathbb{Z}[x]$.
$\implies \exists b_0 \in \mathbb{Z}[x]$ and $x_0 \in I$ s.t. $1 = ab_0 + x_0$ and $1 - ab_0 = -x_0 \in I$
i.e. $\forall a \notin I$, $\exists b \in \mathbb{Z}[x]$ s.t.

$$1 - ab \in I.$$

$\implies \forall a \in \mathbb{Z}[x] - I$, $\exists b \in \mathbb{Z}[x]$ s.t.

$$(I + a)(I + b) = I + 1$$

$\implies$ Every nonzero element of $\mathbb{Z}[x]/I$ has a multiplicative inverse.
Thus $\mathbb{Z}[x]/I$ is a field.