4.1.6 Let p be a prime integer. Find all roots of $X^{p-1}-1$ in $\mathbb{Z}_p[x]$.

Solution: By Fermat's little theorem $a^{p-1}=1$ for all nonzero $a \in \mathbb{Z}_p$ so the roots are all of $\mathbb{Z}_p^{\times}$:

$$X^{p-1}-1 = \prod_{a \in \mathbb{Z}_p^{\times}} (x-a)$$

4.1.9 Let $a \neq 0$ in a field F. Show $(a^{-1})^{-1}=a$ and $(-a)^{-1}=-(a^{-1})$.

Proof (copied from S. Yealkel)

Since $a^{-1}a=1$, $(a^{-1})^{-1}a^{-1}a=(a^{-1})^{-1}$, i.e. $a=1a=(a^{-1})^{-1}$.

Since $aa^{-1}=1$, $(-a)(-a^{-1})=1$ so

$$(-a)^{-1}(-a)(-a^{-1})=(-a)^{-1} \quad \text{or} \quad -(a^{-1})=(-a)^{-1}. \;//$$

4.1.10 Let $a,b,c \in F$ with $a \neq 0$. Show that $ax+b=c$ has a unique solution in F.

Proof: If $ax+b=c$ then $ax=c-b$ so $x=a^{-1}(c-b)$.

Hence the solution is unique, if there is one. But

$a(a^{-1}(c-b))+b = c-b+b=c$, so $x=a^{-1}(c-b)$ is a solution. //