$x^2+x+1 \in \mathbb{Z}_2[x]$

$$\mathbb{Z}_2[x]/(x^2+x+1) = \underbrace{\{0, 1, x, x+1\}}$$

because dividing by x^2+x+1 leaves a remainder that is degree < 2.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$x + x+1$
$= 2x+1$
$= 1$ in $\mathbb{Z}_2[x]$

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1 inv	x	$x+1$
x	0	x	$x^2 = x+1$	$x^2+x = 1$ inv
$x+1$	0	$x+1$	$x^2+x = 1$ inv	$x^2+2x+1 = x^2+1 = x$

closed under $\times$:)

$$x^2+x+1 \overline{\big)\, x^2} \quad 1$$
$$\frac{-(x^2+x+1)}{x+1}$$

$$x^2+x+1 \overline{\big)\, x^2+x} \quad 1$$
$$\frac{x^2+x+1}{1}$$

$$x^2+x+1 \overline{\big)\, x^2+ \quad 1} \quad 1$$
$$\frac{x^2+x+1}{x}$$

$1 \cdot 1 = 1$
$x(x+1) = 1$
every non-0 element has a multiplicative inverse, so it is a field

HW 5.1 #1, 3,
5.2 # 1, 3, 7, ~~9~~

$x^2-2 \in \mathbb{Q}[x]$

$\mathbb{Q}[x]/(x^2-2) = \{ax+b \mid a,b \in \mathbb{Q}\}$

$(ax+b)+(cx+d) = (a+c)x + (b+d)$

$(ax+b)(cx+d) = acx^2 + adx + cbx + bd$

$$x^2-2 \,\overline{\big)\, acx^2 + (ad+cb)x + bd}\quad ac$$

$$\begin{array}{r} acx^2 + (ad+cb)x + bd \\ acx^2 \qquad\qquad\quad -2ac \\ \hline (ad+bc)x + (bd+2ac) \end{array}$$

so

$(ax+b)(cx+d) = (ad+bc)x + (bd+2ac)$

Show: $ax+b$ has an inverse in $\mathbb{Q}[x]/(x^2-2)$ if $a \neq 0$ or $b \neq 0$

$(ax+b)(cx+d) = 1$ (solve for $cx+d$)

$(ad+bc)x + (bd+2ac) = 1$

$ad+bc=0 \qquad bd+2ac=1$

if $a \neq 0$, we can do:

$ad = -bc \qquad 2ac = 1-bd$

$d = \frac{-bc}{a} \to 2ac = 1 - b\left(\frac{-bc}{a}\right)$

$2a^2c = a + b^2c$

$c(2a^2-b^2) = a$

$c = \frac{a}{2a^2-b^2}$

$d = -\frac{b}{a} \cdot \frac{a}{2a^2-b^2}$

$d = \frac{-b}{2a^2-b^2}$

$(ax+b)^{-1} = cx+d = \frac{ax-b}{2a^2-b^2}$

If $b \neq 0$ then

$bc = -ad \qquad bd = 1-2ac$

$c = -\frac{ad}{b} \to bd = 1 - 2a\left(\frac{-ad}{b}\right)$

$b^2d = b + 2a^2d$

$d(b^2-2a^2) = b$

$d = \frac{b}{b^2-2a}$

$c = -\frac{a}{b} \cdot \frac{b}{b^2-2a^2}$

$c = \frac{-a}{b^2-2a^2}$

$(ax+b)^{-1} = cx+d = \frac{-ax+b}{b^2-2a^2} = \frac{ax-b}{-b^2+2a^2} = \frac{ax-b}{2a^2-b^2}$