Question 13.44.

Proof. This is a hands on, elementary proof of the question. A much quicker proof that uses the theory learnt in lectures is to notice that \( \mathbb{Z}_7[\sqrt{3}] \) is a subring of \( \mathbb{R} \) (a field, and in particular an integral domain) so it is also an integral domain.

And \( |\mathbb{Z}_7[\sqrt{3}]| = 49 \), so it is a finite integral domain... what result can we now use to solve the question?

If you want to see how to solve this directly:

Fix a non-zero element \( a + b\sqrt{3} \) in \( \mathbb{Z}_7[\sqrt{3}] \) and we want to find some \( x + y\sqrt{3} \) such that

\[(x + y\sqrt{3})(a + b\sqrt{3}) = 1\]

If \( b = 0 \), then \( a + b\sqrt{3} = a \) and since \( \mathbb{Z}_7[\sqrt{3}] \) is a field we can always find \( x \) such that \( ax = 1 \).

On the other hand if \( a = 0 \), then \( a + b\sqrt{3} = b\sqrt{3} \) so:

\[(b\sqrt{3})(y\sqrt{3}) = 3by\]

\( b \neq 0 \implies 3b \neq 0 \) in \( \mathbb{Z}_7[\sqrt{3}] \).

So we can assume \( a \) and \( b \) are both non-zero.

We are trying to solve a system of equations:

\[
ax + 3by \equiv 1 \pmod{7} \\
ay + xb \equiv 0 \pmod{7}
\]

Since \( a \) and \( b \) are both non-zero, we can always find a \( \lambda \in \mathbb{Z}_7[\sqrt{3}] \) such that \( \lambda a = 3b \), and so:

\[
ax + 3by \equiv 1 \pmod{7} \\
\lambda ay + \lambda xb \equiv 0 \pmod{7}
\]

(1)

Subtracting the second equation from the first (and using \( \lambda a = 3b \)) we get:

\[ax - \lambda bx \equiv 1 \pmod{7} \implies x(a - \lambda b) \equiv 1 \pmod{7}\]
Again since $\mathbb{Z}_7[\sqrt{3}]$ is a field the $x(a - \lambda b) \equiv 1 \pmod{7}$ has a solution unless $a - \lambda b \equiv 0$

But in this case ($a = \lambda b$) the equations (1) become:

$$
\begin{align*}
\lambda bx + 3by & \equiv 1 \pmod{7} \\
\lambda by + xb & \equiv 0 \pmod{7}
\end{align*}
$$

Since $b \neq 0$ we can cancel in the second equation to get:

$$
\begin{align*}
\lambda bx + 3by & \equiv 1 \pmod{7} \\
\lambda y + x & \equiv 0 \pmod{7}
\end{align*}
$$

Substitute the second equation:

$$
\begin{align*}
-\lambda^2 by + 3by & \equiv 1 \pmod{7} \implies by(3 - \lambda^2) \equiv 1 \pmod{7}
\end{align*}
$$

Again this has a solution for $y$ unless $3 = \lambda^2$.

But $\lambda$ lives inside $\mathbb{Z}_7[\sqrt{3}]$ and $3$ is not a square in $\mathbb{Z}_7[\sqrt{3}]$. (The only squares are $\{0, 1, 2, 4\}$).

So the above system of equations (1) always has a solution, and consequently $\mathbb{Z}_7[\sqrt{3}]$ is a field.

Now try and generalize this to $\mathbb{Z}_p[\sqrt{k}]$.

**Hint:** Notice that the punchline of the proof was the fact that $3$ was not a square in $\mathbb{Z}_7$. 

\square