MATH 501, Section 23 Solutions

6. Doing the long division, we get

$$
\begin{array}{rcccccccccccccccccc}
 & & & & & & & & & & 5x^4 & & & + & 5x^2 & + & 6x & & \\
 & & & & & & & & & & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} \\
3x^2 & + & 2x & - & 3 &) & x^6 & + & 3x^5 & + & 0x^4 & + & 0x^3 & + & 4x^2 & - & 3x & + & 2 \\
 & & & & & & x^6 & + & 3x^5 & + & 6x^4 & & & & & & & & \\
 & & & & & & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & & & & \\
 & & & & & & & & & & x^4 & + & 0x^3 & + & 4x^2 & & & & \\
 & & & & & & & & & & x^4 & + & 3x^3 & + & 6x^2 & & & & \\
 & & & & & & & & & & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & & \\
 & & & & & & & & & & & & 4x^3 & + & 5x^2 & - & 3x & & \\
 & & & & & & & & & & & & 4x^3 & + & 5x^2 & + & 3x & & \\
 & & & & & & & & & & & & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} & \text{—} \\
 & & & & & & & & & & & & & & & & x & + & 2
\end{array}
$$

Thus $x^4 + 3x^5 + 4x^2 - 3x + 2 = (3x^2 + 2x - 3)(5x^4 + 5x^2 + 6x) + (x + 2)$.

6. The units in $\mathbb{Z}_7$ are $G = \{1, 2, 3, 4, 5, 6\}$.
The product of two units is also a unit, so G is closed under multiplication.
Because $\mathbb{Z}_7$ is a field, we know these six elements form a group under multiplication:
($\mathscr{G}_1$) multiplication is associative in the ring $\mathbb{Z}_7$, hence also in G
($\mathscr{G}_2$) $1 \in G$
($\mathscr{G}_3$) Any unit in a field has a multiplicative inverse that is a unit in the field, so the inverse of any element of G is also in G.

Thus G is a multiplicative abelian group of order 6, so it must be isomorphic to $\mathbb{Z}_6$. (Since the operation is multiplication, maybe U_6 would be a better choice than $\mathbb{Z}_6$.) Anyway, lets find the generators of this multiplicative group by looking at cyclic subgroups generated by its elements.

$\langle 1 \rangle = \{1^n \ | n \in \mathbb{Z}\} = \{1\}$
$\langle 2 \rangle = \{2^n \ | n \in \mathbb{Z}\} = \{1, 2, 4\}$
$\langle 3 \rangle = \{3^n \ | n \in \mathbb{Z}\} = \{1, 3, 2, 6, 4, 5\}$
$\langle 4 \rangle = \{4^n \ | n \in \mathbb{Z}\} = \{1, 4\}$
$\langle 5 \rangle = \{5^n \ | n \in \mathbb{Z}\} = \{1, 5, 4, 6, 2, 3\}$
$\langle 6 \rangle = \{6^n \ | n \in \mathbb{Z}\} = \{1, 6\}$

Thus $\boxed{\text{the generators are 3 and 5.}}$

12. Is $f(x) = x^3 + 2x + 3$ irreducible over $\mathbb{Z}_5$?

Notice that $f(2) = 2^3 + 2 \cdot 2 + 3 = 0$, so f factors with a linear term of $(x - 2) = (x + 3)$.
Doing the long division, $x^3 + 2x + 3 = (x + 3)(x^2 + 2x + 1)$
Factoring further, $\boxed{x^3 + 2x + 3 = (x + 3)(x + 1)(x + 1), \text{ so } f \text{ is not irreducible.}}$

14. Show that $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$.

By Corollary 32.12, if f has a zero in $\mathbb{Q}$, then it must have a zero in $\mathbb{Z}$, and that zero must divide 2. The possibilities are $1, -1, 2, -2$. Checking:
$f(1) = 7 \neq 0$
$f(-1) = -9 \neq 0$
$f(2) = 18 \neq 0$
$f(-1) = -14 \neq 0$
Since none of these are actually zeroes, we conclude $\boxed{f \text{ is irreducible over } \mathbb{Q}.}$

Is $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{R}$?
The quadratic formula says the solutions of $x^2 + 8x - 2 = 0$ are $\frac{-8 \pm \sqrt{8^2 - 4(1)(-2)}}{2(1)} = -4 \pm 3\sqrt{2}$.
Thus f factors over $\mathbb{R}$ as $(x - (-4 + 3\sqrt{2}))(x - (-4 - 3\sqrt{2}))$
so $\boxed{f \text{ is not irreducible over } \mathbb{R}, \text{ hence neither is it irreducible over } \mathbb{C}.}$

21. Is $2x^{10} - 25x^3 + 10x^2 - 30$ irreducible over $\mathbb{Q}$?

Take the prime number $p = 5$. Notice that:
$2 \not\equiv 0 \pmod 5$
$-25 \equiv 0 \pmod 5$
$10 \equiv 0 \pmod 5$
$-30 \not\equiv 0 \pmod{25}$
Thus, by the Eisenstein Criterion, the give polynomial is irreducible over $\mathbb{Q}$.

34. If p is prime, then $x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p[x]$.

Proof. Let $a \in \mathbb{Z}_p[x]$ and $f(x) = x^p + a$. Our strategy will be to show $f(-a) = 0$, for then the factor theorem implies $f(x) = x^p + a = (x + a)q(x)$.

If $a = 0$ then $f(x) = x^p + a = x^p = xx^{p-1}$ is reducible.

Now suppose $a \neq 0$. The group of units in $\mathbb{Z}_p$ has $p - 1$ elements (every element except 0 is a unit). We know the order of an element of a group must divide the order of the group.
Let n be the order of the element $-a$, so $p - 1 = nk$ for some integer k.
Then $(-a)^{p-1} = (-a)^{nk} = ((-a)^n)^k = 1^k = 1$.

Using this fact, $f(-a) = (-a)^p + a = (-a)^{p-1}(-a) + a = (1)(-a) + a = 0$.
Thus $f(x)$ factors as $x^p + a = (x + a)q(x)$.