Homework 4 Solutions

22.15: $f(x)\,g(x)$ where $f(x) = x^3+2x^2+5$ and $g(x) = 3x^2+2x$ in $\mathbb{Z}_7$.

Solution: $f(2) = 0$ so $x-2 \mid x^3+2x^2+5$

factoring out gives us $f(x) = (x-2)(x^2+4x+1)$.
By trying out all candidates we see x^2+4x+1 has no zeros in $\mathbb{Z}_7$.

$g(0) = 0$ so we factor $g(x) = x(3x+2)$ and then we see that 4 is a zero of $3x+2$.

So then the zeros of $f(x)g(x)$ are precisely $0, 2, 4$.

22.16: Let $\phi_a : \mathbb{Z}_5[x] \to \mathbb{Z}_5$. Use Fermat's theorem to evaluate

$$\phi_3(x^{231}+3x^{117}-2x^{53}+1).$$

Solution:

Fermat's theorem says $a^4 \equiv 1 \pmod 5$ for $a \equiv 0 \pmod 5$.

$$\phi_3(x^{231}+3x^{117}-2x^{53}+1)$$
$$= 3^{231}+3\cdot 3^{117}-2\cdot 3^{53}+1$$
$$= 3^{4\cdot 57+3}+3^{4\cdot 29+2}-2\cdot 3^{4\cdot 13+1}+1$$
$$\equiv 3^3+3^2-2\cdot 3^1+1 \pmod 5$$
$$\equiv 2+4-6+1 \pmod 5$$
$$\equiv \boxed{1} \pmod 5$$

22.17: Use Fermat's theorem to find all zeros in $\mathbb{Z}_5$ of $2x^{219}+3x^{74}+2x^{57}+3x^{44}$.

Solution: $\phi_a(2x^{219}+3x^{74}+2x^{57}+3x^{44})$

$$= 2a^{219}+3a^{74}+2a^{57}+3a^{44}$$

by Fermats theorem when $a \neq 0$

$$\equiv 2a^3+3a^2+2a+3 \pmod 5$$
$$= (a^2+1)(2a+3)$$

which has zeros at

$\boxed{\text{$a=1$, $a=2$, $a=3$, and we see from the original polynomial that $a=0$ is a root.}}$

23.1:

$$x^4 + x^3 + x^2 + x + 5$$

$$x^2 + 2x - 3 \,\big)\, x^6 + 3x^5 + 0x^4 + 0x^3 + 4x^2 - 3x + 2$$

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

$$0 \quad x^5 + 3x^4 + 0x^3$$

$$-(x^5 + 2x^4 - 3x^3)$$

$$0 \quad x^4 + 3x^3 + 4x^2$$

$$-(x^4 + 2x^3 - 3x^2)$$

$$0 \quad x^3 + 7x^2 - 3x$$

$$-(x^3 + 2x^2 - 3x)$$

$$0 + 5x^2 + 0x + 2$$

$$5x^2 + 0x + 2$$

$$-(5x^2 + 10x - 15)$$

$$0 \; -10x + 17$$

so
$$\boxed{\begin{aligned} q(x) &= x^4 + x^3 + x^2 + x + 5 \\ r(x) &= -3x + 3 \end{aligned}}$$

__23.2:__

$$
\begin{array}{r}
5x^4 + 0x^3 + 5x^2 - x \\
3x^2 + 2x - 3 \overline{\big)\, x^6 + 3x^5 + 0x^4 + 0x^3 + 4x^2 - 3x + 2} \\
-(x^6 + 3x^5 - x^4) \qquad\qquad\qquad\qquad\qquad \\
\hline
0 \quad 0 \quad + x^4 + 0x^3 + 4x^2 \qquad\qquad \\
-(x^4 + 3x^3 - x^2) \qquad\qquad \\
\hline
0 \; - 3x^3 + 5x^2 - 3x \qquad \\
-(-3x^3 - 2x^2 + 3x) \quad \\
\hline
0 \quad 0 \quad x + 2
\end{array}
$$

$$
\boxed{\begin{array}{l} q(x) = 5x^4 + 5x^2 - x \\ r(x) = x + 2 \end{array}}
$$

__23.7:__ $\mathbb{Z}_{17}^{\times} = \{1, 2, \dots, 16\}$

$2^1 = 2$
$2^2 = 4$
$2^4 = 16$
$2^8 = 1$

so order of 2 in the group of units is 8, need element of order 16 to be a generator of the cyclic group.

Then since $6^2 = 2$ it follows that the order of 6 is 16. Then 6 is a generator and all the other generators are powers 6^a where a is coprime to 16, meaning a is odd.

So the generators are:

$$\boxed{6, 12, 7, 14, 11, 5, 10, 3}$$

<u>23.9</u>: The polynomial x^4+4 can be factored into linear factors in $\mathbb{Z}_5[x]$. Find this factorization.

<u>Solution</u>:

$$x^4+4 = x^4 - 1 = (x^2-1)(x^2+1)$$

$$= (x-1)(x+1)(x^2-4)$$

$$= (x-1)(x+1)(x-2)(x+2)$$

23.16: Demonstrate that x^3+3x^2-8 is irreducible over $\mathbb{Q}$.

Solution:

The only possible roots in $\mathbb{Q}$ are $\pm 1, 2, 4, 8$ by the rational roots theorem.

We can check that none of these 8 are roots of x^3+3x^2-8.

Since x^3+3x^2-8 is degree 3, it is irreducible over $\mathbb{Q}[x]$ because it has no roots.

23.18: x^2-12 is Eisenstein for $p=3$.

23.19: $8x^3+6x^2-9x+24$ is Eisenstein for $p=3$.

23.35: If F is a field and $a \neq 0$ is a zero of $f(x)=a_0+a_1x+\ldots+a_nx^n$ in $F[x]$, show that $1/a$ is a zero of $a_n+a_{n-1}x+\ldots+a_0x^n$.

Solution:

$$a_n + a_{n-1} \cdot \frac{1}{a} + \dots + a_1 \cdot \frac{1}{a^{n-1}} + a_0 \frac{1}{a^n}$$

$$= \frac{1}{a^n}\left[a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a + a_0 \right]$$

$$= \frac{1}{a^n} f(a)$$

$$= 0$$

23.37:

Proof:

a) $\overline{\sigma_m}\left(\sum_{i=0}^{n} (a_i + b_i) x^i \right)$

$$= \sum_{i=0}^{n} \sigma_m(a_i + b_i) x^i = \sum_{i=0}^{n} \sigma_m(a_i) x^i + \sum_{i=0}^{n} \sigma_m(b_i) x^i$$

$$= \overline{\sigma_m}\left(\sum_{i=0}^{n} a_i x^i \right) + \overline{\sigma_m}\left(\sum_{i=0}^{n} b_i x^i \right)$$

$$\overline{\sigma_m}\left(\sum_{i=0}^{m+n} \sum_{j+k=i} a_j b_k x^i \right) =$$

$$\sum_{i=0}^{m+n} \sigma_m\left(\sum_{j+k=i} a_j b_k \right) x^i$$

$$= \sum_{i=0}^{m+n} \sum_{j+k=i} \sigma_m(a_j)\,\sigma_m(b_k)\,x^i$$

$$= \left[\sum_{i=0}^{m} \sigma_m(a_i)\,x^i\right]\left[\sum_{j=0}^{n} \sigma_m(b_j)\,x^j\right]$$

$$= \overline{\sigma}_m\left(\sum_{i=0}^{m} a_i x^i\right)\,\overline{\sigma}_m\left(\sum_{j=0}^{n} b_j x^j\right).$$

b) We prove the contrapositive, if $f(x) = g(x)\,h(x)$ is reducible over $\mathbb{Q}[x]$

Then $\overline{\sigma}_m(f(x)) = \overline{\sigma}_m(g(x))\,\overline{\sigma}_m(h(x))$ means that either $\overline{\sigma}_m(f(x))$ is reducible or one of $\overline{\sigma}_m(g(x))$ or $\overline{\sigma}_m(h(x))$ are constant, meaning $\overline{\sigma}_m(f(x))$ must have degree less than n.

c) $\overline{\sigma}_5(x^3+17x+36) = x^3+2x+1$

x^3+2x+1 has no roots in $\mathbb{Z}_5$ by direct evaluation so since it is degree 3 this means it does not factor in $\mathbb{Z}_5[x]$. Then by (b) we have that $x^3+17x+36$ is irreducible in $\mathbb{Q}[x]$.