Chapter 17. Question 10.

Determine which of the polynomials below is (are) irreducible over Q.

a). $x^5+9x^4+12x^2+6$

The polynomial $x^5+9x^4+12x^2+6$ is irreducible by Eisenstein's criterion with $p=3$.

2/2

$p \nmid 1$, $p|9$, $p|12$, $p|6$ and $p^2=9 \nmid 6$ then $x^5+9x^4+12x^2+6$ is irreducible over Q.

b). x^4+x+1

If x^4+x+1 factors over Q, then it factors over Z. Substitution of $x=0$, $x=1$, and $x=-1$ show that it has no linear factor, so that only remaining possibility is that $x^4+x+1=(x^2+ax+b)(x^2+cx+d)$ $= x^4+(c+a)x^3+(d+ca+b)x^2+(da+cb)x+db$.

This gives the system of equations

$$\begin{aligned} c+a &= 0 \\ d+b+ac &= 0 \\ ad+bc &= 1 \\ bd &= 1 \end{aligned}$$

The first equation tell us that $c=-a$, while the last one tells us that $b=d=\pm 1$. If $b=d=1$, then the second equation becomes $2-a^2=0$, which has no Integer solutions; If $b=d=-1$, Then the second equation becomes $-2-a^2=0$, which again has no Integer solutions!. Therefore, this polynomial is irreducible over Q

c) x^4+3x^2+3

The polynomial x^4+3x^2+3 is irreducible, via Eisenstein's criterion and the prime $p=3$.
$p \nmid 1$, $p \mid 3$, $p \mid 3$ and $p^2=9 \nmid 3$, then x^4+3x^2+3 is irreducible over $\mathbb{Q}$.

d) x^5+5x^2+1

The polynomial x^5+5x^2+1 has no linear factors over $\mathbb{Z}$ (and hence over $\mathbb{Q}$), as can be seen by substitution of $x=0$, $x=1$, and $x=-1$. The remaining possibility is that it factors as a quadratic times a cubic.

$$x^5+5x^2+1 = (x^2+ax+b)(x^3+cx^2+dx+e)$$

and expand to get.

$$x^5+5x^2+1 = x^5+(a+c)x^4+(b+ca+d)x^3+(cb+da+e)x^2+(db+ea)x+eb$$

which gives the following equations:

$$a+c=0$$
$$b+ca+d=0$$
$$cb+da+e=5$$
$$db+ea=0$$
$$be=1$$

Now we know from the first equation that $a=-c$ and the last tells us that $b=e=\pm 1$. In either event, $b=e\neq 0$, so the fourth equation becomes $d+a=0$, so $d=-a$. Now the second equation becomes $1-a^2-a=0$, which has no solutions in integers.

e) $(5/2)x^5 + (9/2)x^4 + 15x^3 + (3/7)x^2 + 6x + 3/14$.

then

$14f(x) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3$

apply the Eisenstein criterion with $p=3$ to conclude that $14f(x)$, and therefore $f(x)$, is irreducible

$p \nmid 35$ $p|63$, $p|210$, $p|6$, $p|84$, $p^2 = 9 \nmid 3$ over Q

Question 32

Prove that the ideal $\langle x^2+1 \rangle$ is prime in $Z[x]$ but not maximal in $Z[x]$.

Consider $Z[x]/\langle x^2+1 \rangle$. let $I = \langle x^2+1 \rangle$. Notice that $x^2+I = -1+I$. Thus any element $p(x)+I$ is equal to $ax+b+I$ for some $a,b \in Z$ since terms of degree ≥ 2 can be reduced. Thus $Z[x]/I = \{ax+b+I\}$ Notice that

$$(ax+b+I)(cx+d+I) = acx^2 + (ad+bc)x + bd + I = (ad+bc)x + bd - ac + I$$

This is exactly how complex numbers $ai+b$ multiply. Similarly for addition. Thus the map taking $a+bi$ to $a+bx+I$ gives an isomorphism between $Z[i]$ and $Z[x]/I$. Since $Z[i]$ is an integral domain but not a field. Thus I is prime but not maximal.

Chapter 20 Problem #2.

Show that $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}+\sqrt{3})$.

Obviously, $Q(\sqrt{2}+\sqrt{3}) \subseteq Q(\sqrt{2},\sqrt{3})$. To show equality, it suffices to show that $\sqrt{2}, \sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$.

Compute $(\sqrt{2}+\sqrt{3})^3 = 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$. Therefore,
$(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3}) = 2\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$, and so
$\sqrt{2} \in Q(\sqrt{2}+\sqrt{3})$.

Therefore, $(\sqrt{2}+\sqrt{3}) - \sqrt{2} = \sqrt{3} \in Q(\sqrt{2}+\sqrt{3})$

2/2

Problem #7.

Find a polynomial $p(x)$ in $Q[x]$ such that $Q(\sqrt{1+\sqrt{5}})$ is ring-isomorphic to $Q[x]/\langle p(x)\rangle$.

Find an irreducible polynomial $p(x)$ with root $\sqrt{1+\sqrt{5}}$. The easiest thing to do is proceed systematically:

$$x = \sqrt{1+\sqrt{5}}$$
$$x^2 = 1+\sqrt{5}$$
$$x^2-1 = \sqrt{5}$$
$$(x^2-1)^2 = 5$$
$$x^4-2x^2+1 = 5$$
$$x^4-2x^2-4 = 0$$

The desired polynomial is therefore x^4-2x^2-4. This has no linear factors by evaluating the polynomial at ± 1, ± 2, and ± 4, and seeing that we never get 0. The only way to check that it does not factor as a product of two quadratic polynomials is by trial and error, either by trying to factor as a product of polynomials with integer coefficients, or else by reducing modulo 3 and trying all possible factors.

2/2

Question #16

Suppose that B is a zero of $f(x)=x^4+x+1$ in some field extension E of Z_2. Write $f(x)$ as a product of linear factors in $Z[x]$.

From the question B is a root:

$\therefore B^4+B+1=0$

$1+B$ is also a root.

$$\therefore (1+B)^4+(1+B)+1 = (1+B)(1+B)(1+B)(1+B)+(1+B)+1$$
$$= (1+B+B+B^2)(1+B+B+B^2)+(1+B)+1$$
$$= (1+2B+B^2)(1+2B+B^2)+(1+B)+1$$
$$= (1+2B^2+B^4)+B+2$$
$$= B^4+B+1$$
$$= 0 \quad \text{is a root}$$

B^2 is a root

$$(B^2)^4+B^2+1$$
$$= B^8+B^2+1$$
$$= (B^4+B+1)(B^4+B+1) = 0\cdot 0 = 0$$

$(1+B^2)$ is also a root.

2/2

$$(1+B^2)^4+(1+B^2)+1$$
$$= (1+B^2)(1+B^2)(1+B^2)(1+B^2)+(1+B^2)+1$$
$$= (1+\cancel{B^2}+\cancel{B^2}+B^4)(1+B^4)+(1+B^2)+1$$
$$= (1+\cancel{B^4}+\cancel{B^4}+B^8)+(1+B^2)+1$$
$$= B^8+B^2+1$$
$$= (B^4+B+1)(B^4+B+1)$$
$$= 0\cdot 0 = 0$$

$\therefore f(x) = (x+B)(x+(1+B))(x+B^2)(x+(B^2+1))$