13. In the proof of Theorem 9.9 the polynomial $q(x) \in K[x]$ was defined so that $ker(f_c) = \langle q(x) \rangle$. Prove that $q(x)$ is irreducible over K.

If $q(x)$ is reducible over K, then $q(x) = u(x)w(x)$ for some nonconstant $u(x), w(x) \in K[x]$. By Theorem 7.20 we know that $deg(u(x)) < deg(q(x))$ and $deg(w(x)) < deg(q(x))$. Since in E we have $0_E = q(c) = u(c)w(c)$, then either $u(c) = 0_E$ or $w(c) = 0_E$. If $u(c) = 0_E$ then $u(x) \in ker(f_c) = \langle q(x) \rangle$ and so $u(x) = q(x)s(x)$. But this means $deg(u(x)) \geq deg(q(x))$ which is a contradiction. Similarly if $w(c) = 0_E$ then $w(x) \in ker(f_c) = \langle q(x) \rangle$ and so $w(x) = q(x)s(x)$. Again we have $deg(w(x)) \geq deg(q(x))$, a contradiction. Thus $q(x)$ is irreducible over K.

14. Find the minimum polynomial for $u = \sqrt[3]{10}$ over $\mathbb{Q}$. Be sure to prove your polynomial is irreducible.

Let $p(x) = -10 + x^3$. Then $p(x) \in \mathbb{Q}[x]$ and $p\left(\sqrt[3]{10}\right) = -10 + \left(\sqrt[3]{10}\right)^3 = -10 + 10 = 0$. Hence u is a root of $p(x)$. Also by Eisenstein's criterion ($p = 2$) we know $p(x)$ is irreducible over $\mathbb{Q}$. Hence $p(x) = -10 + x^3$ is the minimum polynomial for $u = \sqrt[3]{10}$ over $\mathbb{Q}$.

#18 find min poly of sqrt2 + sqrt7

Let $p(x) = 25 - 18x^2 + x^4$ which is in $\mathbb{Q}[x]$.

$$\begin{aligned} p(\sqrt{2}+\sqrt{7}) &= 25 - 18(\sqrt{2}+\sqrt{7})^2 + (\sqrt{2}+\sqrt{7})^4 \\ &= 25 - 18(9 + 2\sqrt{14}) + (2 + 2\sqrt{14} + 7)^2 \\ &= 25 - 162 - 36\sqrt{14} + 137 + 36 \\ sqrt14 & \\ &= (25 - 162 + 137) + (-36 + 36)\sqrt{14} = 0 \end{aligned}$$

Hence $\sqrt{2}+\sqrt{7}$ is a root of $p(x)$. There are no possible rational roots for $p(x)$ since the only possibilities are 1, -1, 5, -5, 25, -25 but $p(1) = 8, p(-1) = 8, p(5) = 200, p(-5) = 200, p(25) = 379400, p(-25) = 379400$. Thus unless $p(x)$ factors into two quadratics we know it is irreducible over $\mathbb{Q}$. From Theorem 8.33 we can assume the factors are in $\mathbb{Z}[x]$.

Suppose we have $25 - 18x^2 + x^4 = (a + bx + x^2)(c + dx + x^2)$ then $25 - 18x^2 + x^4 = (ac) + (ad + bc)x + (a + c + bd)x^2 + (b + d)x^3 + x^4$. So $25 = ac$, $ad + bc = 0$, $a + c + bd = -18$, and $b+d = 0$. Now as $ac = 25$ we have choices of $a = 1, c = 25$ or $a = 5, c = 5$ or $a = 25, c = 1$, or the same options with both a and c negative.

- If $a = 1, c = 25$ then $d + 25b = 0$ and $b + d = 0$. Now $b = -d$ so we have $-24d = 0$ which only happens if $d = 0 = b$. But now $-18 \neq a + c + bd$.
- If $a = -1, c = -25$ then similarly we have $-d - 25b = 0$ and $b + d = 0$. Now $b = -d$ so we have $-26d = 0$ which only happens if $d = 0 = b$. But now $-18 \neq a + c + bd$.
- If $a = 5, c = 5$ then $10 + bd = -18$ and $b + d = 0$. Thus $b = -d$ and $(-d)d = -28$. But there is no integer that satisfies $d^2 = 28$.
- If $a = -5, c = -5$ then $-10 + bd = -18$ and $b + d = 0$. Thus $b = -d$ and $(-d)d = -8$. But there is no integer that satisfies $d^2 = 8$.
- If $a = 25, c = 1$ the argument is virtually identical to the one with $a = 1, c = 25$.
- If $a = -25, c = -1$ the argument is virtually identical to the one with $a = 25, c = 1$.

Hence $p(x)$ is irreducible over $\mathbb{Q}$ and is the minimum polynomial for $\sqrt{2}+\sqrt{7}$ over $\mathbb{Q}$.

19. Find the minimum polynomial for $\sqrt[4]{2}i$ over $\mathbb{Q}$. Be sure to prove your polynomial is irreducible.

Let $p(x) = -2 + x^4$ which is in $\mathbb{Q}[x]$. Also $p(\sqrt[4]{2}i) = -2 + (\sqrt[4]{2}i)^4 = -2 + (\sqrt[4]{2})^4(i)^4 = -2 + (2)(1) = 0$. So $\sqrt[4]{2}i$ is a root of $p(x)$. By Eisenstein's Criterion we know $p(x)$ is irreducible over $\mathbb{Q}$, so $p(x)$ is the minimum polynomial for $\sqrt[4]{2}i$ over $\mathbb{Q}$.

21. Prove (i) of Theorem 9.12.

Suppose K is a field, E is an extension of K, and $c \in E$ is algebraic over K with minimum polynomial $p(x)$. We need to show that $ker(f_c) = \langle p(x) \rangle$. Let $T = ker(f_c)$ and $S = \langle p(x) \rangle$. We know T is a principal ideal by Theorem 7.26, so $T = \langle t(x) \rangle$ for some $t(x) \in K[x]$. Exercise 13 tells us that $t(x)$ is irreducible over K and c is a root of $t(x)$. Since $p(x) \in T$ then $p(x) = t(x)w(x)$ for some $w(x) \in K[x]$. However $p(x)$ is irreducible so one of $t(x)$ or $w(x)$ is constant. Since a nonzero constant polynomial cannot have c as a root, then $t(x)$ is not constant and $w(x)$ is a constant polynomial. Thus $t(x)$ and $p(x)$ are associates and so $\langle p(x) \rangle = \langle t(x) \rangle$ (Exercise 20).

22. Explain how (ii) follows from (i) in Theorem 9.12.

Suppose K is a field, E is an extension of K, and $c \in E$ is algebraic over K with minimum polynomial $p(x)$. Let $b(x) \in K[x]$ be a nonzero polynomial with $b(c) = 0_E$. Thus $b(x) \in ker(f_c)$ so $b(x) \in \langle p(x) \rangle$ from part (i). Hence we know $b(x) = p(x)q(x)$ for some $q(x) \in K[x]$.

23. Show that it was necessary to have the minimum polynomial for c, $p(x)$, in the statement

31. Consider the polynomial $a(x) = 5+3x+4x^2+6x^3+x^4$ in $\mathbb{Q}[x]$. Prove $a(x)$ is irreducible over $\mathbb{Q}$ (try Theorem 8.37 to help), then if u is a root of $a(x)$ in an extension field of $\mathbb{Q}$, describe carefully the elements of $\mathbb{Q}(u)$.

Let $a(x) = 5 + 3x + 4x^2 + 6x^3 + x^4$ in $\mathbb{Q}[x]$. Using $n = 3$ and Theorem 8.37 we have $b(x) = h(a(x)) = 2 + x^2 + x^4$ in $\mathbb{Z}_3[x]$.Note that $b(0) = 2, b(1) = 1, b(2) = 1$ so $b(x)$ has no roots in $\mathbb{Z}_3$. If it factors it must be $(a + bx + x^2)(c + dx + x^2)$ where $ac = 2, ad + bc = 0, a + c + bd = 1, b + d = 0$. The only way to have $ac = 2$ in $\mathbb{Z}_3$ is for one of $a = 1, c = 2$ or $a = 2, c = 1$.

Suppose $a = 1, c = 2$ then $d + 2b = 0$, $bd = 1$, $b + d = 0$. Now $b = -d$ so that $-d^2 = 1$ or $d^2 = 2$. This is impossible in $\mathbb{Z}_3$ since $0^2 = 0$, $1^2 = 1$, and $2^2 = 1$.

Now suppose $a = 2, c = 1$. Then again $bd = 1$ and $b + d = 0$ which is still impossible. Thus

$b(x)$ is irreducible over $\mathbb{Z}_3$ so by Theorem 8.37 $a(x)$ is irreducible over $\mathbb{Q}$. If u is a root of $p(x)$ in an extension field of $\mathbb{Q}$ we know $\mathbb{Q}(u) = \{r_0 + r_1 u + r_2 u^2 + r_3 u^3 : r_i \in \mathbb{Q}\}$.

46. Find the complete addition and multiplication tables for the field $\mathbb{Z}_2(c)$ where c is a root of the polynomial $p(x) = 1 + x + x^2$ which is irreducible over $\mathbb{Z}_2$.

The elements of $\mathbb{Z}_2(c)$ are $0, 1, c, 1+c$. Recall that $1+c+c^2$, so $c^2 = 1+c$. The Cayley tables are shown below.

$+$	0	1	c	$1+c$
0	0	1	c	$1+c$
1	1	0	$1+c$	c
c	c	$1+c$	0	1
$1+c$	$1+c$	c	1	0

$\cdot$	0	1	c	$1+c$
0	0	0	0	0
1	0	1	c	$1+c$
c	0	c	$1+c$	1
$1+c$	0	$1+c$	1	c

52. Find the complete addition and multiplication tables for the field $\mathbb{Z}_3(c)$ where c is a root of the polynomial $p(x) = 2 + x + x^2$ which is irreducible over $\mathbb{Z}_3$.

The elements of $\mathbb{Z}_3(c)$ are $0, 1, 2, c, 1+c, 2+c, 2c, 1+2c, 2+2c$. Since $2 + c + c^2 = 0$ then $c^2 = 1 + 2c$. The Cayley tables are shown below.

$+$	0	1	2	c	$1+c$	$2+c$	$2c$	$1+2c$	$2+2c$
0	0	1	2	c	$1+c$	$2+c$	$2c$	$1+2c$	$2+2c$
1	1	2	0	$1+c$	$2+c$	c	$1+2c$	$2+2c$	$2c$
2	2	0	1	$2+c$	c	$1+c$	$2+2c$	$2c$	$1+2c$
c	c	$1+c$	$2+c$	$2c$	$1+2c$	$2+2c$	0	1	2
$1+c$	$1+c$	$2+c$	c	$1+2c$	$2+2c$	$2c$	1	2	0
$2+c$	$2+c$	c	$1+c$	$2+2c$	$2c$	$1+2c$	2	0	1
$2c$	$2c$	$1+2c$	$2+2c$	0	1	2	c	$1+c$	$2+c$
$1+2c$	$1+2c$	$2+2c$	$2c$	1	2	0	$1+c$	$2+c$	c
$2+2c$	$2+2c$	$2c$	$1+2c$	2	0	1	$2+c$	c	$1+c$

$\cdot$	0	1	2	c	$1+c$	$2+c$	$2c$	$1+2c$	$2+2c$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	c	$1+c$	$2+c$	$2c$	$1+2c$	$2+2c$
2	0	2	1	$2c$	$2+2c$	$1+2c$	c	$2+c$	$1+c$
c	0	c	$2c$	$1+2c$	1	$1+c$	$2+c$	$2+2c$	2
$1+c$	0	$1+c$	$2+2c$	1	$2+c$	$2c$	2	c	$1+2c$
$2+c$	0	$2+c$	$1+2c$	$1+c$	$2c$	2	$2+2c$	1	c
$2c$	0	$2c$	c	$2+c$	2	$2+2c$	$1+2c$	$1+c$	1
$1+2c$	0	$1+2c$	$2+c$	$2+2c$	c	1	$1+c$	2	$2c$
$2+2c$	0	$2+2c$	$1+c$	2	$1+2c$	c	1	$2c$	$2+c$

55. Suppose K is a field and c is algebraic over K. Prove $[K(c) : K] = 1$ if and only if $c \in K$.

Suppose K is a field and c is algebraic over K. First assume that $[K(c) : K] = 1$. By Theorem 9.20 this tells us that the minimum polynomial $p(x)$ for c over K has $deg(p(x)) = 1$. Now by Theorem 9.4 since $p(c) = 0_{K(c)}$ we know $c \in K$. Similarly if we assume that $c \in K$, then we have $b(x) = -c + x \in K[x]$. Since $deg(b(x)) = 1$ then $b(x)$ is irreducible by Theorem 8.9. Thus $b(x)$ is the minimum polynomial for c over K and $[K(c) : K] = 1$. Hence $[K(c) : K] = 1$ if and only if $c \in K$.