Field Theory Problems.

Problem 1. Show $f(x) = x^4 - 2x^2 + 2 \in \mathbb{Q}[x]$ is irreducible and find its splitting field. $\square$

Problem 2. As a generalization of the previous problem, let b and c be integers such that neither c or $b^2 - 4c$ are squares of integers. Show that $x^4 + bx^2 + c$ is irreducible over the rationals and find its splitting field. *Hint:* Solving for x^2 gives

$$x^2 = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

and $\sqrt{b^2 - 4c}$ is irrational. Thus $f(x) = 0$ has no rational roots and therefore any irreducible factors must be quadratic. Thus if $f(x)$ factors it is of the form

$$f(x) = (x^2+Ax+B)(x^2+Cx+D) = x^4+(A+C)x^3+(B+D+AC)x^2+(AD+CB).$$

This gives the equations

$$\begin{aligned} A + C &= 0 \\ B + D + AC &= b \\ AD + BC &= 0 \\ BD &= c \end{aligned}$$

The first of these implies $C = -A$. Using this the remaining equations become

$$\begin{aligned} B + D - A^2 &= b \\ A(D - B) &= 0 \\ BD &= c \end{aligned}$$

If $A = 0$ show that $b^2 - 4c = (B - D)^2$, contradicting that $b^2 - 4c$ is not the square of an integer. If $A \neq 0$, show that $B = D$ and thus $c = B^2$ is the square of an integer, again a contradiction. $\square$

Problem 3. Let m and n be integers such that none of n, m, or mn are squares of integers. Show $\mathbb{Q}(\sqrt{m} + \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ and that the polynomial $f(x) = x^4 - 2(m+n)x + (m-n)^2$ is irreducible. *Hint:* A natural way to start is to let $x = \sqrt{m} + \sqrt{n}$. Then

$$x^2 = m + n + 2\sqrt{mn}$$

so

$$(x - (m+n))^2 = 4mn$$

which can be rearranged to give

$$x^4 - 2(m+n)x^2 + (m-n)^2 = 0.$$

We can now try to show this is irreducible. A very annoying fact is that the method used Problem 2 does not apply as the constant term is a perfect square.

So we try anther method. The roots of $f(x)$ are $\pm\sqrt{m} \pm \sqrt{n}$. We first note that none of these are rational. For if $r = \pm\sqrt{m} \pm \sqrt{n}$ is rational, then so is $r^2 = m + n \pm 2\sqrt{mn}$, implying that $\sqrt{mn}$ is rational, which is not the case (as mn is not a perfect square). Thus $f(x)$ has no rational roots. So if it factors over the rationals the factors are both quadratic. The linear factors of $f(x)$ over its splitting field are

$$(x + \sqrt{m} + \sqrt{n}), \quad (x + \sqrt{m} - \sqrt{n}), \quad (x - \sqrt{m} + \sqrt{n}), \quad (x - \sqrt{m} - \sqrt{n}).$$

If $f(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are quadratic, then one of them, say $p(x)$, will contain the factor $(x + \sqrt{m} + \sqrt{n})$. Thus $p(x)$ will be one of

$$\begin{aligned}
(x + \sqrt{m} + \sqrt{n})(x + \sqrt{m} - \sqrt{n}) &= x^2 + 2\sqrt{m}x + m - n \\
(x + \sqrt{m} + \sqrt{n})(x - \sqrt{m} + \sqrt{n}) &= x^2 + 2\sqrt{n}x + n - m \\
(x + \sqrt{m} + \sqrt{n})(x - \sqrt{m} - \sqrt{n}) &= x^2 - m - n - 2\sqrt{mn}.
\end{aligned}$$

None of these have all coefficients rational. Therefore no factorization of $f(x)$ over the rational numbers is possible.

As $\sqrt{m} + \sqrt{n}$ is a root of the irreducible polynomial $f(x)$, the degree of $\mathbb{Q}(\sqrt{m} + \sqrt{n})$ over $\mathbb{Q}$ is $\deg(f(x)) = 4$. Clearly $\mathbb{Q}(\sqrt{m} + \sqrt{n}) \subseteq \mathbb{Q}(\sqrt{m}, \sqrt{n})$ and $[\mathbb{Q}(\sqrt{m}, \sqrt{n}), \mathbb{Q}] \leq 4$. Thus we must have $\mathbb{Q}[\sqrt{m} + \sqrt{n}] = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ as required. $\square$

Problem 4. Let $\mathbb{F}_q$ be the finite field with q elements. (This q is a power of prime.) Find all the irreducible monic polynomials of degree 2 and 3 in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$. $\square$

Problem 5. Using that $f(x) = x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ explicitly construct a field with 4 elements. Likewise use that $x^3 + x + 1$ is irreducible to explicitly construct a field with 8 elements. $\square$

Problem 6. Let $\mathbb{F}$ be a finite field. Show that there is at least one irreducible monic polynomial in $\mathbb{F}[x]$ and therefore $\mathbb{F}$ has an extension of degree 2. $\square$

Problem 7. Show $\left[\mathbb{Q}(\sqrt[5]{3} + \sqrt{5}) : \mathbb{Q}\right] = 10$. $\square$

Problem 8. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of odd degree and let α be a root of $f(x)$. Show $\mathbb{Q}[\alpha] = \mathbb{Q}[\alpha^2]$. $\square$

Problem 9 (January 2011, Problem 7). Let F be a field and $f(x) = x^2 + ax + b \in F[x]$ irreducible over F. Show $F[x]/\langle f(x)\rangle$ is a splitting field for $f(x)$ over F. $\square$

Problem 10 (January 1012, Problem 9). Prove every algebraically closed field has infinitely many subfields. $\square$