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

Because $Q(\sqrt{2} + \sqrt{3})$ is the intersection of all fields containing $Q$ and $\sqrt{2} + \sqrt{3}$, in order to demonstrate that $Q(\sqrt{2} + \sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3})$ it is enough to show that $Q \subseteq Q(\sqrt{2}, \sqrt{3})$ and $\sqrt{2} + \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$. Of course $Q \subseteq Q(\sqrt{2}, \sqrt{3})$ is obvious, and $\sqrt{2} + \sqrt{3} \in Q(\sqrt{2}, \sqrt{3})$ is clear by closure. To show that $Q(\sqrt{2}, \sqrt{3}) \subseteq Q(\sqrt{2} + \sqrt{3})$, it is similarly enough to demonstrate that $Q$ is a subset of and $\sqrt{2}$ and $\sqrt{3}$ are elements of $Q(\sqrt{2} + \sqrt{3})$ (because $Q(\sqrt{2}, \sqrt{3})$ is the intersection of all ideals containing $Q$, $\sqrt{2}$, and $\sqrt{3}$). Note that $(\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}$ is in $Q(\sqrt{2} + \sqrt{3})$ by closure, and hence so is $\frac{1}{3}((\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})) = \frac{1}{3}(11\sqrt{2} + 9\sqrt{3} - 9\sqrt{2} - 9\sqrt{3}) = \sqrt{2}$. Once $\sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$ we easily show that $\sqrt{3} = \sqrt{2} + \sqrt{3} - \sqrt{2} \in Q(\sqrt{2} + \sqrt{3})$ as well. We conclude that $Q(\sqrt{2} + \sqrt{3}) \supseteq Q(\sqrt{2}, \sqrt{3})$ as required.

20.20 Let $F$ be a field, and let $a$ and $b$ belong to $F$ with $a \neq 0$. If $c$ belongs to some extension of $F$, prove that $F(c) = F(ac + b)$.

This problem is very similar to the previous one. The inclusion $F(ac + b) \subseteq F(c)$ is obvious, so it is enough to show that $F(c) \subseteq F(ac + b)$ which follows if $c \in F(ac + b)$. But $a \neq 0$ so $a^{-1}(ac + b) - a^{-1}b = c$ is an element of $F(ac + b)$ by closure. We conclude that the two fields are equal as required.

20.22 Recall that two polynomials $f(x)$ and $g(x)$ from $F[x]$ are said to be relatively prime if there is no polynomial of positive degree in $F[g(x)]$ that divides both $f(x)$ and $g(x)$. Show that if $f(x)$ and $g(x)$ are relatively prime if $F[x]$, they are relatively prime in $K[x]$, where $K$ is any extension of $F$.

The theorem is obvious if the degree of either $f(x)$ or $g(x)$ is less than or equal to zero, so we suppose that this is not the case.

We prove first that for any polynomials $f(x), g(x) \in F[x]$ where $F$ is any field, the elements $f(x)$ and $g(x)$ are relatively prime if and only if there are $s(x), t(x) \in F(x)$ such that $f(x)s(x) + g(x)t(x) = 1$. Actually, necessity is easy to show because if there are $s(x), t(x) \in F[x]$ such that $f(x)s(x) + g(x)t(x) = 1$, then any divisor of $f(x)$ and $g(x)$ must also divide 1, and hence cannot have positive degree (so $f(x)$ and $g(x)$ must be relatively prime in that case). Suppose then that $f(x)$ and $g(x)$ are relatively prime, let $S$ be the set

$$S = \{\deg(h(x)) \mid h(x) \in S\}.$$  

and let $S' = \{\deg(h(x)) \mid h(x) \in S\}$. Since $f(x) \in S$, it is clear that $S$ is non-empty. Therefore $S'$ is non-empty and by the Well Ordering Axiom there is a smallest element $a \in S'$. Let $s(x), t(x) \in F[x]$ such that $h(x) = f(x)s(x) + g(x)t(x)$ has degree $a$. Now we can divide both $f(x)$ and $g(x)$ by $h(x)$. So there are $q_1(x), r_1(x), q_2(x), r_2(x) \in F[x]$ such that $f(x) = h(x)q_1(x) + r_1(x)$, $g(x) = q_2(x)h(x) + r_2(x)$ and $\deg(r_1(x)) < \deg(h(x)) = a$. Because the degrees of the $r_i(x)$ are strictly smaller than $a$, it must be that $\deg(r_i(x)) \notin S'$ and hence $r_i(x) \notin S$ (for $i = 1, 2$). But $r_i(x) = f(x) - h(x)q_i(x) = f(x) - f(x)s(x)q_i(x) - g(x)t(x)q_i(x) = f(x)(1 - s(x)q_i(x)) + g(x)(-t(x)q_i(x))$, so $r_i(x) \in S$ unless $\deg(r_i(x)) \leq 0$ (again for $i = 1, 2$). Suppose that $\deg(r_i(x)) = 0$ for either $i = 1$ or $i = 2$ (without loss of generality we may assume that $\deg(f_1(x)) = 0$, then $r_1(x)$ is a non-zero constant and thus $f(x)((1 - s(x)q_1(x))r_1(x)^{-1}) + g(x)(t(x)q_1(x)r_1(x)^{-1}) = 1$ proving the assertion. If $\deg(r_1(x)) = -1$ for both $i$, that is, if $r_1(x) = 0$ for $i = 1$ and $i = 2$, then $f(x) = q_1(x)(f(x)s(x) + g(x)t(x))$ and $g(x) = q_2(x)(f(x)s(x) + g(x)t(x))$. Note that according to these equations $\deg(f(x)) = \deg(q_1(x)) + a$ and $\deg(g(x)) = \deg(q_2(x)) + a$. Because $a$ is smallest in $S'$, it must therefore be that $q_1(x)$ and $q_2(x)$ have degree zero. This implies, however, that $f(x)$ and $g(x)$ are associates, and can not be relatively prime, a contradiction.

Having established this fact, the proof becomes very easy. If $f(x)$ and $g(x)$ are relatively prime over $F$, then there are $s(x), t(x) \in F[x]$ such that $f(x)s(x) + g(x)t(x) = 1$. Since this equation also holds over $K[x]$, that is, $f(x), g(x), s(x),$ and $t(x)$ are also polynomials in $K[x]$ such that $f(x)s(x) + g(x)t(x) = 1$, we conclude that $f(x)$ and $g(x)$ are relatively prime over $K$ as required.
20.28 For any prime \( p \) find a field of characteristic \( p \) that is not perfect.

Consider the field \( F = \mathbb{Q}(\mathbb{Z}_p[x]) \), the field of quotients of \( \mathbb{Z}_p[x] \). Here \( F \) is certainly characteristic \( p \) because if \( f(x)/g(x) \in F \), then \( pf(x)/g(x) = (pf(x))/g(x) = 0/g(x) = 0 \). But \( F \) is not perfect because \( x \) is not a \( p \)th power. To wit, if \( x = \left( \frac{f(x)}{g(x)} \right)^p \), then \( xg(x)^p = f(x)^p \). This implies that \( p \deg(f(x)) = 1 + p \deg(g(x)) \) (note that \( \mathbb{Z}_p \) is a field) and hence \( p|1 \), a contradiction.

20.34 Find the splitting field for \( f(x) = (x^2 + x + 2)(x^2 + 2x + 2) \) over \( \mathbb{Z}_3[x] \). Write \( f(x) \) as a product of linear factors.

Using the quadratic formula, we see that the roots of \( x^2 + x + 2 \) and \( x^2 + 2x + 2 \) are \(-\frac{1}{2} \pm \sqrt{-\frac{7}{2}}\) and \(-2 + \sqrt{2}\) over \( \mathbb{Q} \). To translate these into roots over \( \mathbb{Z}_3 \), we note that \( \frac{1}{2} = 2 \), \(-2 = 1 \), and \(-1 = -7 = -4 = 2 \). So over \( \mathbb{Z}_3 \) we have roots \( 2(2 + \sqrt{2}) = 1 + 2\sqrt{2}, 2(2 + 2\sqrt{2}) = 1 + \sqrt{2}, 2(1 + \sqrt{2}) = 2 + 2\sqrt{2}, \) and \( 2(1 + 2\sqrt{2}) = 2 + \sqrt{2} \). We can show that \( \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + 2\sqrt{2}, 1 + \sqrt{2}, 2 + 2\sqrt{2}, 2 + \sqrt{2}) \) (as in the first two assigned problems: one inclusion is obvious and the other follows because \( \sqrt{2} = (1 + 2\sqrt{2}) + (2 + 2\sqrt{2}) \) is an element of \( \mathbb{Q}(1 + 2\sqrt{2}, 1 + \sqrt{2}, 2 + 2\sqrt{2}, 2 + \sqrt{2}) \) by closure) and hence \( \mathbb{Q}(\sqrt{2}) \) is the splitting field for \( f(x) \) over \( \mathbb{Q} \) (I am using that if \( a_1, \ldots, a_n \in E \) are the roots of a polynomial \( f(x) \in F[x] \) for \( E \) some extension field of \( F \), then \( F(a_1, \ldots, a_n) \) is the splitting field of \( f(x) \) over \( F \)). We can factor \( f(x) \) as \( f(x) = (x - (1 + 2\sqrt{2}))(x - (1 + \sqrt{2}))(x - (2 + 2\sqrt{2}))(x - (2 + \sqrt{2})) \) in \( \mathbb{Q}(\sqrt{2}) \). (To be technically correct, we should point out that by \( \sqrt{2} \) we mean the element in an extension field of \( \mathbb{Z}_3 \) whose square is 2).