Now suppose the characteristic is not 3. In effect applying the Euclidean algorithm to
if the characteristic of the field is 3, then the derivative is the constant

\[ \alpha \]

\[ \beta \]

\[ 0 \]

(One might try to do this as a symmetric function computation, but it's a bit tedious.)

If \( P(x) = x^3 + ax + b \) has a repeated factor, then it has a common factor with its derivative \( P'(x) = 3x^2 + a \).

If the characteristic of the field is 3, then the derivative is the constant \( a \). Thus, if \( a \neq 0 \), \( \gcd(P, P') = a \in k^* \) is never 0. If \( a = 0 \), then the derivative is 0, and all the \( \alpha_i \) are the same.

Now suppose the characteristic is not 3. In effect applying the Euclidean algorithm to \( P \) and \( P' \),

\[ (x^3 + ax + b) - \frac{x}{3} \cdot (3x^2 + a) = ax + b - \frac{x}{3} \cdot a = \frac{2}{3} ax + b \]

If \( a = 0 \) then the Euclidean algorithm has already terminated, and the condition for distinct roots or factors
is \( b \neq 0 \). Also, possibly surprisingly, at this point we need to consider the possibility that the characteristic
is 2. If so, then the remainder is \( b \), so if \( b \neq 0 \) the roots are always distinct, and if \( b = 0 \)

Now suppose that \( a \neq 0 \), and that the characteristic is not 2. Then we can divide by \( 2a \). Continue the algorithm

\[ (3x^2 + a) - \frac{9x}{2a} \cdot \left( \frac{2}{3} ax + b \right) = a + \frac{27b^2}{4a^2} \]

Since \( 4a^2 \neq 0 \), the condition that \( P \) have no repeated factor is

\[ 4a^3 + 27b^2 \neq 0 \]

[09.3] The first three \textbf{elementary symmetric functions} in indeterminates \( x_1, \ldots, x_n \) are

\[ \sigma_1 = \sigma_1(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_n = \sum_i x_i \]

\[ \sigma_2 = \sigma_2(x_1, \ldots, x_n) = \sum_{i<j} x_i x_j \]

\[ \sigma_3 = \sigma_3(x_1, \ldots, x_n) = \sum_{i<j<\ell} x_i x_j x_\ell \]

Express \( x_1^3 + x_2^3 + \ldots + x_n^3 \) in terms of \( \sigma_1, \sigma_2, \sigma_3 \).

Execute the algorithm given in the proof of the theorem. Thus, since the degree is 3, if we can derive the
right formula for just 3 indeterminates, the same expression in terms of elementary symmetric polynomials
will hold generally. Thus, consider \( x^3 + y^3 + z^3 \). To approach this we first take \( y = 0 \) and \( z = 0 \), and consider
\( x^3 \). This is \( s_1(x)^3 = x^3 \). Thus, we next consider

\[ (x^3 + y^3) - s_1(x,y)^3 = 3x^2y + 3xy^2 \]

As the algorithm assures, this is divisible by \( s_2(x,y) = xy \). Indeed,

\[ (x^3 + y^3) - s_1(x,y)^3 = (3x + 3y)s_2(x,y) = 3s_1(x,y)s_2(x,y) \]
Then consider
\[(x^3 + y^3 + z^3) - (s_1(x, y, z)^3 - 3 s_2(x, y, z) s_1(x, y, z)) = 3xyz = 3s_3(x, y, z)\]

Thus, again, since the degree is 3, this formula for 3 variables gives the general one:
\[x_1^3 + \ldots + x_n^3 = s_1^3 - 3s_1s_2 + 3s_3\]

where \(s_i = s_i(x_1, \ldots, x_n)\).

[09.4] Express \(\sum_{i \neq j} x_i^2 x_j\) as a polynomial in the elementary symmetric functions of \(x_1, \ldots, x_n\).

We could (as in the previous problem) execute the algorithm that proves the theorem asserting that every symmetric (that is, \(S_n\)-invariant) polynomial in \(x_1, \ldots, x_n\) is a polynomial in the elementary symmetric functions.

But, also, sometimes *ad hoc* manipulations can yield short-cuts, depending on the context. Here,

\[\sum_{i \neq j} x_i^2 x_j = \sum_{i,j} x_i^2 x_j - \sum_{i=j} x_i^2 x_j = \left(\sum_i x_i^2\right)\left(\sum_j x_j\right) - \sum_i x_i^3\]

An easier version of the previous exercise gives
\[\sum_i x_i^2 = s_1^2 - 2s_2\]

and the previous exercise itself gave
\[\sum_i x_i^3 = s_1^3 - 3s_1s_2 + 3s_3\]

Thus,
\[\sum_{i \neq j} x_i^2 x_j = (s_1^2 - 2s_2)s_1 - (s_1^3 - 3s_1s_2 + 3s_3) = s_1^3 - 2s_1s_2 - s_1^3 + 3s_1s_2 - 3s_3 = s_1s_2 - 3s_3\]

[09.5] Suppose the characteristic of the field \(k\) does not divide \(n\). Let \(\ell > 2\). Show that
\[P(x_1, \ldots, x_n) = x_1^n + \ldots + x_\ell^n\]
is irreducible in \(k[x_1, \ldots, x_\ell]\).

First, treating the case \(\ell = 2\), we claim that \(x^n + y^n\) is not a unit and has no repeated factors in \(k(y)[x]\). (We take the field of rational functions in \(y\) so that the resulting polynomial ring in a single variable is Euclidean, and, thus, so that we understand the behavior of its irreducibles.) Indeed, if we start executing the Euclidean algorithm on \(x^n + y^n\) and its derivative \(nx^{n-1}\) in \(x\), we have
\[(x^n + y^n) - \frac{x}{n}(nx^{n-1}) = y^n\]

Note that \(n\) is invertible in \(k\) by the characteristic hypothesis. Since \(y\) is invertible (being non-zero) in \(k(y)\), this says that the \(\gcd\) of the polynomial in \(x\) and its derivative is 1, so there is no repeated factor. And the degree in \(x\) is positive, so \(x^n + y^n\) has some irreducible factor (due to the unique factorization in \(k(y)[x]\), or, really, due indirectly to its Noetherian-ness).
Thus, our induction (on $n$) hypothesis is that $x_2^p + x_3^p + \ldots + x_n^p$ is a non-unit in $k[x_2, x_3, \ldots, x_n]$ and has no repeated factors. That is, it is divisible by some irreducible $p$ in $k[x_2, x_3, \ldots, x_n]$. Then in

$$k[x_2, x_3, \ldots, x_n][x_1] \approx k[x_1, x_2, x_3, \ldots, x_n]$$

Eisenstein’s criterion applied to $x_1^n + \ldots$ as a polynomial in $x_1$ with coefficients in $k[x_2, x_3, \ldots, x_n]$ and using the irreducible $p$ yields the irreducibility.

[09.6] Find the determinant of the circulant matrix

$$
\begin{pmatrix}
  x_1 & x_2 & \cdots & x_{n-2} & x_{n-1} & x_n \\
  x_n & x_1 & x_2 & \cdots & x_{n-2} & x_{n-1} \\
  x_{n-1} & x_n & x_1 & x_2 & \cdots & x_{n-2} \\
  \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
  x_3 & x_4 & \cdots & x_1 & x_2 & x_3 \\
  x_2 & x_3 & \cdots & x_n & x_1 & x_2
\end{pmatrix}
$$

(Hint: Let $\zeta$ be an $n^{th}$ root of 1. If $x_{i+1} = \zeta \cdot x_i$ for all indices $i < n$, then the $(j+1)^{th}$ row is $\zeta$ times the $j^{th}$, and the determinant is 0.)

Let $C_{ij}$ be the $ij^{th}$ entry of the circulant matrix $C$. The expression for the determinant

$$\det C = \sum_{p \in S_n} \sigma(p) C_{1,p(1)} \ldots C_{n,p(n)}$$

where $\sigma(p)$ is the sign of $p$ shows that the determinant is a polynomial in the entries $C_{ij}$ with integer coefficients. This is the most universal viewpoint that could be taken. However, with some hindsight, some intermediate manipulations suggest or require enlarging the ‘constants’ to include $n^{th}$ roots of unity $\omega$. Since we do not know that $\mathbb{Z}[\omega]$ is a UFD (and, indeed, it is not, in general), we must adapt. A reasonable adaptation is to work over $\mathbb{Q}(\omega)$. Thus, we will prove an identity in $\mathbb{Q}(\omega)[x_1, \ldots, x_n]$.

Add $\omega^{i-1}$ times the $i^{th}$ row to the first row, for $i \geq 2$. The new first row has entries, from left to right,

$$x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n$$

$$x_2 + \omega x_3 + \omega^2 x_4 + \ldots + \omega^{n-1} x_{n-1}$$

$$x_3 + \omega x_4 + \omega^2 x_5 + \ldots + \omega^{n-1} x_{n-2}$$

$$x_4 + \omega x_5 + \omega^2 x_6 + \ldots + \omega^{n-1} x_{n-3}$$

$$\ldots$$

$$x_2 + \omega x_3 + \omega^2 x_4 + \ldots + \omega^{n-1} x_1$$

The $t^{th}$ of these is

$$\omega^{-t} \cdot (x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n)$$

since $\omega^n = 1$. Thus, in the ring $\mathbb{Q}(\omega)[x_1, \ldots, x_n]$,

$$x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n$$

divides this new top row. Therefore, from the explicit formula, for example, this quantity divides the determinant.

Since the characteristic is 0, the $n$ roots of $x^n - 1 = 0$ are distinct (for example, by the usual computation of $gcd$ of $x^n - 1$ with its derivative). Thus, there are $n$ superficially-different linear expressions which divide $\det C$. Since the expressions are linear, they are irreducible elements. If we prove that they are non-associate elements.
Paul Garrett:  (January 14, 2009)

(Do not differ merely by units), then their product must divide \( \det C \). Indeed, viewing these linear expressions in the larger ring

\[
\mathbb{Q}(\omega)(x_2, \ldots, x_n)[x_1]
\]

we see that they are distinct linear monic polynomials in \( x_1 \), so are non-associate.

Thus, for some \( c \in \mathbb{Q}(\omega) \),

\[
\det C = c \cdot \prod_{1 \leq \ell \leq n} \left( x_1 + \omega^\ell x_2 + \omega^{2\ell} x_3 + \omega^{3\ell} x_4 + \ldots + \omega^{(n-1)\ell} x_n \right)
\]

Looking at the coefficient of \( x_1^n \) on both sides, we see that \( c = 1 \).

(One might also observe that the product, when expanded, will have coefficients in \( \mathbb{Z} \).)