(January 14, 2009)

[04.1] (Lagrange interpolation) Let \( \alpha_1, \ldots, \alpha_n \) be distinct elements in a field \( k \), and let \( \beta_1, \ldots, \beta_n \) be any elements of \( k \). Prove that there is a unique polynomial \( P(x) \) of degree \(<n\) in \( k[x] \) such that, for all indices \( i \),

\[
P(\alpha_i) = \beta_i
\]

Indeed, letting

\[
Q(x) = \prod_{i=1}^{n} (x - \alpha_i)
\]

show that

\[
P(x) = \sum_{i=1}^{n} \frac{Q(x)}{(x - \alpha_i) \cdot Q'(\alpha_i)} \cdot \beta_i
\]

Since the \( \alpha_i \) are distinct,

\[
Q'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \neq 0
\]

(One could say more about purely algebraic notions of derivative, but maybe not just now.) Evaluating \( P(x) \) at \( x \to \alpha_i \),

\[
\frac{Q(x)}{(x - \alpha_j) \cdot Q'(\alpha_i)} \text{ evaluated at } x \to \alpha_i = \begin{cases} 1 & \text{for } j = i \\ 0 & \text{for } j \neq i \end{cases}
\]

Thus, all terms but the \( i^{th} \) vanish in the sum, and the \( i^{th} \) one, by design, gives \( \beta_i \). For uniqueness, suppose \( R(x) \) were another polynomial of degree \(<n\) taking the same values at \( n \) distinct points \( \alpha_i \) as does \( Q(x) \). Then \( Q - R \) is of degree \(<n\) and vanishes at \( n \) points. A non-zero degree \( \ell \) polynomial has at most \( \ell \) zeros, so it must be that \( Q - R \) is the 0 polynomial.

[04.2] (Simple case of partial fractions) Let \( \alpha_1, \ldots, \alpha_n \) be distinct elements in a field \( k \). Let \( R(x) \) be any polynomial in \( k[x] \) of degree \(<n\). Show that there exist unique constants \( c_i \in k \) such that in the field of rational functions \( k(x) \)

\[
\frac{R(x)}{(x - \alpha_1) \ldots (x - \alpha_n)} = \frac{c_1}{x - \alpha_1} + \ldots + \frac{c_n}{x - \alpha_n}
\]

In particular, let

\[
Q(x) = \prod_{i=1}^{n} (x - \alpha_i)
\]

and show that

\[
c_i = \frac{R(\alpha_i)}{Q'(\alpha_i)}
\]

We might emphasize that the field of rational functions \( k(x) \) is most precisely the field of fractions of the polynomial ring \( k[x] \). Thus, in particular, equality \( r/s = r'/s' \) is exactly equivalent to the equality \( rs' = r's \) (as in elementary school). Thus, to test whether or not the indicated expression performs as claimed, we test whether or not

\[
R(x) = \sum_{i} \left( \frac{R(\alpha_i)}{Q'(\alpha_i)} \cdot \frac{Q(x)}{x - \alpha_i} \right)
\]

One might notice that this is the previous problem, in case \( \beta_i = R(\alpha_i) \), so its correctness is just a special case of that, as is the uniqueness (since \( \deg R < n \)).

[04.3] Show that the ideal \( I \) generated in \( \mathbb{Z}[x] \) by \( x^2 + 1 \) and 5 is not maximal.

We will show that the quotient is not a field, which implies (by the standard result proven above) that the ideal is not maximal (proper).
First, let us make absolutely clear that the quotient of a ring $R$ by an ideal $I = Rx + Ry$ generated by two elements can be expressed as a two-step quotient, namely

$$\left(\frac{R}{\langle x \rangle}\right)/\langle \bar{y} \rangle \approx \frac{R}{Rx + Ry}$$

where the $\langle \bar{y} \rangle$ is the principal ideal generated by the image $\bar{y}$ of $y$ in the quotient $R/\langle x \rangle$. The principal ideal generated by $y$ in the quotient $R/\langle x \rangle$ is the set of cosets

$$\langle \bar{y} \rangle = \{(r + Rx) \cdot (y + Rx) : r \in R\} = \{ry + Rx : r \in R\}$$

noting that the multiplication of cosets in the quotient ring is not just the element-wise multiplication of the cosets. With this explication, the natural map is

$$r + \langle x \rangle = r + \langle x \rangle \rightarrow r + \langle x \rangle + \langle y \rangle' = r + (Rx + Rx)$$

which is visibly the same as taking the quotient in a single step.

Thus, first

$$\mathbb{Z}[x]/\langle 5 \rangle \approx (\mathbb{Z}/5)[x]$$

by the map which reduces the coefficients of a polynomial modulo 5. In $(\mathbb{Z}/5)[x]$, the polynomial $x^2 + 1$ does factor, as

$$x^2 + 1 = (x - 2)(x + 2)$$

(where these 2s are in $\mathbb{Z}/5$, not in $\mathbb{Z}$). Thus, the quotient $(\mathbb{Z}/5)[x]/(x^2 + 1)$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} + 2$, where $\bar{x}$ is the image of $x$ in the quotient. Thus, it’s not even an integral domain, much less a field.

[04.4] Show that the ideal $I$ generated in $\mathbb{Z}[x]$ by $x^2 + x + 1$ and 7 is not maximal.

As in the previous problem, we compute the quotient in two steps. First,

$$\mathbb{Z}[x]/\langle 7 \rangle \approx (\mathbb{Z}/7)[x]$$

by the map which reduces the coefficients of a polynomial modulo 7. In $(\mathbb{Z}/7)[x]$, the polynomial $x^2 + x + 1$ does factor, as

$$x^2 + x + 1 = (x - 2)(x - 4)$$

(where 2 and 4 are in $\mathbb{Z}/7$). Thus, the quotient $(\mathbb{Z}/7)[x]/(x^2 + x + 1)$ has proper zero divisors $\bar{x} - 2$ and $\bar{x} - 4$, where $\bar{x}$ is the image of $x$ in the quotient. Thus, it’s not even an integral domain, so certainly not a field.