Homework 14 - MATH 791

Will Thomas

Problem 1:
Let F be a field. Follow (and prove each of) the steps given in the Lecture of February 24 to prove the Fundamental Theorem of Arithmetic to show that every monic polynomial with coefficients in F can be factored uniquely as a product of monic, irreducible, polynomials with coefficients in F.
Solution:
Lemma:
Given f, g_1, g_2 all monic irreducible polynomials.

$$f = g_1 \cdot g_2 \implies f \mid g_1 \vee f \mid g_2$$

Proof:
Since f is irreducible $\implies f = g_1 \cdot g_2 \implies g_1$ is a unit or g_2 is a unit.
Since g_1 and g_2 are monic, the only units they could be are 1 themselves
WLOG this implies that $f = g_1 * 1 \implies f = g_1$ and thus $f \mid g_1$ and $f \mid g_1 \vee f \mid g_2$
End Proof
First, we will prove that any $x \in F[X]$ can be factored as a product of monic, irreducibles (not uniquely)
Let us define

$$X := \{\text{monic polynomials that cannot be factored by monic,irreducibles}\}$$

Since polynomials are well-ordered when you look at the degree, we can pick a least element $n \in X$.
Since n was the least element, if n is irreducible, then it can be factored as itself trivially. If n is not irreducible, then there exists a factorization such that $n = a * b$ where a, b are not monic, irreducibles. However, since $a, b \notin X$, they themselves can be factored into monic, irreducibles $\implies a = \alpha_1 \cdots \alpha_n,\ b = \beta_1 \cdots \beta_m$. This can be combined to create a monic, irreducible factorization of $n = \alpha_1 \cdots \alpha_n \cdot \beta_1 \cdots \beta_m$

$$\therefore X = \emptyset \text{ and any monic polynomial can be factored}$$

Now to prove the uniqueness:
Given $x \in F[X]$, where $x = f_1(x) \cdots f_r(x)$ and $x = g_1(x) \cdots g_s(x)$ where f_i, g_i are all monic, irreducible polynomials.
We want to show that after re-indexing, $f_i = g_i$ and $r = s$ (uniqueness up to ordering).
Let us assume WLOG $r < s$ and set $e_i := deg(f_i)$ and $h_i := deg(g_i)$
Induct on $n = e_1 + \cdots + e_r$:

If $n = 1$ then $f_1(x) = g_1(x) \cdots g_s(x)$, we know by our Lemma that since f_1 is monic, irreducible that $f_1 \mid g_1 \vee f_1 \mid g_2 \cdots g_s$. Let us assume that the first case holds and $f_1 \mid g_1$ or we re-index to force this case to hold.
Since g_1 is also monic, irreducible $\implies f_1 = g_1$ and $e_1 = h_1$. Additionally, this will force the rest of the $g_i = 1$ and they can then not be counted as part of the factorization, so $r = s = 1$.
If $n > 1$ then $\implies f_1 \mid f_1 \cdots f_r \implies f_1 \mid g_1 \cdots g_s \implies f_1 \mid g_i$ for some i (by a similar argument as the case when $n = 1$)
Since g_i is prime $\implies f_1 = g_i \implies$ after re-indexing $f_1 = g_1$ and

$$f_1 \cdot f_2 \cdots f_r = f_1 \cdot g_2 \cdots g_s$$

We can divide both sides by f_1 to get $f_2 \cdots f_r = g_2 \cdots g_s$, and then apply our induction hypothesis to solve the rest of the problem.

$\therefore$ We can factor every monic polynomial in $F[X]$ uniquely as a product of irreducibles

Problem 2:
Prove that repeated applications of the division algorithm can be used to find the GCD to $a, b \in \mathbb{Z}$, and that backwards substitution with the system of equations generated by this process gives $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = ma + nb$
Solution:
We will make the assumption that a, b are positive, if not, re-index them to have a lower bounded finite subset of $\mathbb{Z}$ for well-foundedness.
First, let us prove that the division algorithm will halt.
Given $a, b \in \mathbb{Z}$ we have two cases WLOG $a < b$ or $a = b$. If $a = b$ this stops trivially
If $a < b$, then we will get $\exists q, r \in \mathbb{Z},\ b = q_0 * a + r$ for $0 \leq r < a$. This can be repeated by taking $a = q_1 * r + r_1$ for $0 \leq r_1 < r$. Since $\mathbb{Z}$ is well-founded, we know that this relation will eventually reach 0 and halt.
Next, we will prove that this method preserves the GCD.
Let us assume that $r > 0$, and we know by induction that for $a = q_1 * r + r_1$ that the $\gcd(a, r) = x_1 = m_1 * a + n_1 * r$. We want to show that since $x_1 \mid a \wedge x_1 \mid r \implies x_1 \mid b$ and is the maximal such element that allows $x_1 \mid a \wedge x_1 \mid b$.
Since $x_1 \mid a \implies a = x_1 * a'$ and $x_1 \mid r \implies r = x_1 * r'$. We can back-substitute this to get $b = q_0 * (x_1 * a') + x_1 * r'$ which can be factored to $b = x_1 * (q_0 * a' + r')$.

$$\therefore x_1 \mid b$$

To show that it is maximal, we need to show that no greater gcd could exist. Let us assume a greater gcd $x_1 < x'$ existed. Then $b = x' * b'$ and we also know that $a = x' * a'$. This can be combined into $x' * b' = q_0 * x' * a' + r \implies x' * (b' - q_0 * a') = r$. This leads to a contradiction as this implies that $x' \mid r$, but we assumed $x' > x_1$ and x_1 was the GCD for r

$$\therefore x_1 \text{ is the maximal element, thus it is the GCD}$$

To show that we can use backwards substitution to reach the GCD value, we can use the same induction setup as before.
We know that $\gcd(b, a) = \gcd(a, r) = m_1 * a + n_1 * r$ we also know that
$b = q_0 * a + r \implies r = b - q_0 * a$

$$\gcd(a, b) = m_1 * a + n_1 * (b - q_0 * a)$$

$$= m_1 * a + n_1 * b - n_1 * q_0 * a = (m_1 - n_1 * q_0) * a + n_1 * b$$

Thus, using backwards substitution we can solve for the Bezout coefficients

Problem 3:
Use the Euclidean algorithm to find $\gcd(120, 54)$ and write the GCD as an integer combination of 120 and 54 as in Bezout's Principle.
Solution:

$$\begin{aligned} 120 &= 54 * 2 + 12 \\ 54 &= 12 * 4 + 6 \\ 12 &= 6 * 2 + 0 \end{aligned}$$

So the $\gcd(120, 54) = 6$, we can back-substitute to get

$$6 = 1 * 54 - 4 * 12 = 1 * 54 - 4 * (1 * 120 - 2 * 54) = 9 * 54 - 4 * 120$$

$$6 = (9)(54) + (-4)(120)$$

The Bezout coefficients are 9 and -4