Math 1540: HW1

February 3, 2023

Book Problems:

49. This is equivalent to proving that a polynomial $p(x) \in F[x]$ of degree 2 or 3 must have at least one root in F iff $p(x)$ is reducible

    Suppose there exists a root, a, in F then a linear term $(x-a)$ can be divided out from $p(x)$ (Euclidean division); therefore $p(x)$ is reducible

    Suppose $p(x)$ is reducible, then $p(x)$ can be written as $p(x) = f(x)g(x)$ where $deg(f(x))$ and $deg(g(x))$ are not equal to 0. $deg(p(x)) = deg(f(x)) + deg(g(x))$ In the case of $deg(p(x)) = 2$, $deg(f(x))$ must be less than 2 and not equal to 0, so it's a linear term, and so $p(x)$ has a root in F. In the case of $deg(p(x)) = 3$, either $deg(f(x))$ or $deg(g(x))$ must be less than 2 and not equal to 0, so either $f(x)$ or $g(x)$ is a linear term, and so $p(x)$ has a root in F.

50. Since $p(x) \in F[x]$ is irreducible $p(x)$ is a maximal ideal therefore either $g(x) \in (p(x)) \Leftrightarrow p(x)|g(x)$ or $g(x) \notin (p(x)) \Leftrightarrow (p(x), g(x))$ contains the entire ring $\Leftrightarrow (p(x), g(x)) = 1$

63. Let the monic polynomial $f(x) = a_0 + a_1x \dots a_nx^n$ where $a_n = 1$ then $s|1 \Rightarrow s = 1$ and $r \in \mathbb{Z}$; therefore $r/s = r$ is an integer

69. Using the rational root thm and the fact that this polynomial (degree 3) has a root in $\mathbb{Z}$ (from Q49). $1, 36, 2, 18, 3, 12, 4, 9, 6$ all could be roots. By calculation, we can see that 3 is a root ($3^3 + 3^2 - 36 = 0$). Using Euclidean division we find that $x^3 + x^2 - 36$ splits into $(x-3)(x^2 + 4x - 12)$ Now we must check whether $(x^2 + 4x + 12)$ factors and using the discriminant from the Quadratic formula $b^2 - 4ac$ we find the discriminant is negative $16 - 4(1)(12)$, so $(x^2 + 4x + 12)$ cannot be factored further in $\mathbb{Q}[x]$

Given Problems:

1. Let $a = y^3$, then $y^6 + ry^3 - q^3/27$ becomes $a^2 + ra - q^3/27$. Now it is clear that this is in the form of a quadratic and we can solve it using the Quadratic formula. Therefore, $a = y^3 = (-r \pm \sqrt{r^2 + 4q^3/27})/2$

   Note: Like in the question I will be using the same notation (variables) as in the textbook. Some of the formulas/equations I use will be from the textbook (Rotman).

   From page 45 in the textbook we see that $y^3z^3 = -q^3/27$. From page 46 in the textbook we see that the roots are given as $y + z, wy + w^2z, w^2y + wz$

   Throughout the entire derivation of the cubic formula in the textbook both y and z are interchangeable (there is a symmetry between the two variables)

Let $y_1 = y^3 = \frac{1}{2}\left(-r + \sqrt{r^2 + 4q^3/27}\right)$ and $y_2 = y^3 = \frac{1}{2}\left(-r - \sqrt{r^2 + 4q^3/27}\right)$

Then

$$y_1 y_2 = \frac{1}{4}(r^2 - (r^2 + 4q^3/27)) = \frac{1}{4}(-4q^3/27) = -q^3/27$$

This mirrors an earlier result $y^3 z^3 = -q^3/27$, and suggests that if $y^3 = \frac{1}{2}\left(-r + \sqrt{r^2 + 4q^3/27}\right)$ then $z^3 = \frac{1}{2}\left(-r - \sqrt{r^2 + 4q^3/27}\right)$ and vice versa. And so, because of the symmetry of the variables y and z the choice between the $+$ and $-$ does not matter.

2. Let the characteristic, $q = mn \neq 0$, of a field, F, be composite, then $m1_F \cdot n1_F = q1_F = 0$ but $m1_F, n1_F \neq 0$; this is a contradiction since this implies that $m1_f$ and $n1_F$ are zero divisors, yet are in a field F

3. Case $n = 0$: Consider the map $f : \mathbb{Z} \to F$ such that $f(m) = m1_F$. This map is a homomorphism since:

$$f(m + p) = (m + p)1_F = m1_F + p1_F = f(m) + f(p)$$

$$f(mp) = (mp)1_F = m1_F \cdot n1_F = f(m) \cdot f(n)$$

Using this map we can construct a map to the $\mathbb{Q}$ similar to how we can create $\mathbb{Q}$ from $\mathbb{Z}$

Consider the map $g : \mathbb{Q} \to F$ such that $g(m/p) = f(m)/f(p)$ with $p \neq 0$ (to clarify $m, p \in \mathbb{Z}$ so $m/p \in \mathbb{Q}$) This map is a homomorphism since

$$g(\frac{m_1}{p_1} \cdot \frac{m_2}{p_2}) = g(\frac{m_1 m_2}{p_1 p_2}) = (\frac{f(m_1)f(m_2)}{f(p_1)f(p_2)}) = (\frac{f(m_1)}{f(p_1)} \cdot \frac{f(m_2)}{f(p_2)}) = g(\frac{m_1}{p_1}) \cdot g(\frac{m_2}{p_2})$$

$$g(\frac{m_1}{p_1} + \frac{m_2}{p_2}) = g(\frac{m_1 + m_2}{p_1 + p_2}) = (\frac{f(m_1) + f(m_2)}{f(p_1) + f(p_2)}) = (\frac{f(m_1)}{f(p_1)} \cdot \frac{f(m_2)}{f(p_2)}) = g(\frac{m_1}{p_1}) + g(\frac{m_2}{p_2})$$

Since any homomorphism between two fields is injective, this map is an injective map from $\mathbb{Q}$ to F. Therefore, F contains a subfield isomorphic to image of g, which in this case is $\mathbb{Q}$. Since the image is in terms of 1_F all fields must contain the image of g and the image of g is a subfield, so it must be P

Case $n = p$: When $n = p$ the image of g is $\{0, 1_F \ldots (p-1)1_F\}$ Therefore, $\mathbb{Z}_p$ is isomorphic to P

4. We showed in Q63 that if we have a monic polynomial, in this case $p(x)$, the rational root must be an integer; moreover, since the leading coefficient is 1 (s must be 1) we know that the rational root $r/s = r$, and by the rational root thm, $r|a_0 = 30$. The possible rational roots are $1, 30, 2, 15, 3, 10, 5, 6$. By calculation, can see that 2 is a root $2^3 - 19 + 30$. Using Euclidean division we find that $x^3 - 19x + 30$ splits into $(x-2)(x^2+2x-15)$. We know the sum of the other two roots must be -2, the negative of the linear coefficient of $(x^2 + 2x - 15)$ (Note: $(x - a)(x - b) = x^2 - (a + b)x + ab$ so

negative of the linear term is the sum of the roots); therefore, the sum of all the roots is $s_1 + s_2 + s_3 = 0$.

In the question, "expression," was somewhat vague so if it meant s_1: by factoring $(x^2 + 2x - 15) = (x + 5)(x - 3)$ (or using the Quadratic formula) we find that $-5, 3$ are the remaining roots. Since $-5, 2, 3$ divide 30, s_1 divides 30. $s_1 = 3$