MAT220 manditory 3

Fromsa Hera

March 15, 2018

1. (a) Let $a = x^4 - x^3 - x^2 + 1 = (x-1)(x^3 - x - 1)$ and $b = x^3 - 1 = (x-1)(x^2+x+1)$
$\boldsymbol{x^4 - x^3 - x^2 + 1 = (x^3 - 1)(x - 1)} + (\boldsymbol{-x^2 + x})$ and $(-x^2+x) \nmid a$ and $(-x^2+x) \nmid b$
$\therefore gcd(a,b) = (x-1)$ in $\mathbb{Q}[x]$

DOWN

$$a = b(x-1) + (-x^2+x)$$
$$x^3 - 1 = (-x^2+x)(-x-1)$$
$$(-x^2+x) = (x-1)(-x) + 0$$

UP

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

(b) Let $s(x) = x^4 + x^3 + 1$ and $t(x) = x^2 + x + 1$

- $t(0) = 0^2 + 0 + 1 = 1$
- $t(1) = 1^2 + 1 + 1 = 1$

By theorem 4.16, The Factor theorem, none of $0, 1 \in \mathbb{Z}_2$ are roots of $t(x)$, thus by corollary 4.19 $t(x)$ is irreducible in $\mathbb{Z}_2[x]$
$t(x) \nmid s(x)$ and
by the definition of *gcd*, two polynomials, not both zero, in a field F have at least one *gcd* (namley 1_F)
$\therefore gcd(s(x), t(x)) = 1_{\mathbb{Z}_2}$
For part 2, look to task 8.

2. **(R with identity 1_R)$\rightarrow$($R[x]$ with identity $1_{R[x]}$)?**
Theorem 4.1 says that $R[x]$ is a ring whenever R is a ring. So we just need to prove for multiplicative identity, to show that $R[x]$ is a ring with identity.
Since R is a ring, notice that $a1_R = a = 1_R a$ for all $a \in R$.
Assume $R[x]$ is a ring, then given any polynomial $n(x) \in R[x]$ there exists $i(x) \in R[x]$ such that $n(x)i(x) = n(x) = i(x)n(x)$

- $n(x)i(x) = n(x) \iff$
$\iff (n_0, n_1, n_2, \dots) \odot (i_0, i_1, i_2, \dots) = (c_0, c_1, c_2, \dots)$
$\iff c_k = n_k$ for any $k \in \mathbb{Z}$
$\iff n_j = \sum_{k=0}^{j} i_k n_{j-k}$ Since $c_j = \sum_{k=0}^{j} i_k n_{j-k}$
$\iff i_0 = 1_R, i_k = 0_R$ for all $k > 1$
Thus $i(x) = (1_R, 0_R, 0_R, \dots)$
- $i(x)n(x) = n(x) \iff$
$\iff (i_0, i_1, i_2, \dots) \odot (n_0, n_1, n_2, \dots) = (c_0, c_1, c_2, \dots)$
$\iff c_k = n_k$for any $k \in \mathbb{Z}$
$\iff n_j = \sum_{k=0}^{j} i_k n_{j-k}$ Since $c_j = \sum_{k=0}^{j} i_k n_{j-k}$
$\iff i_0 = 1_R, i_k = 0_R$ for all $k > 1$
Thus $i(x) = (1_R, 0_R, 0_R, \dots)$

$\therefore R[x]$ is a ring with identity $1(x)_R = i(x) = (1_R, 0_R, 0_R, \dots)$ $\square$

3. $\mathbb{Z}_p$ has exactly p congruence classes of modulo p including the $[0]$. Meaning that there are $p-1$ nonzero constants in $\mathbb{Z}_p$
$\therefore$ For any given $g(x) \in \mathbb{Z}_p[x]$ there are exactly $p-1$ associates $f(x)$ of $g(x)$, such that for a non zero $c \in \mathbb{Z}_p$, $f(x) = cg(x)$.

4. Given $g(x)$, an associate of $p(x)$ such that $g(x) = cp(x)$ where $c \in F$ and $deg\,[g(x)] = deg\,[p(x)]$.

   - **Assume $g(x)$ is irreducible and $p(x)$ is reducible.**
     Then there exists $m(x), n(x)$ where $deg\,[m(x)], deg\,[n(x)] < deg\,[p(x)]$ such that

     $$p(x) = m(x)n(x) \implies cp(x) = cm(x)n(x) \implies g(x) = cm(x)n(x).$$

     This is a contradiction, which means that $g(x)$ is irreducible $\implies p(x)$ is irreducible. ✓
   - **Assume $p(x)$ is irreducible and $g(x)$ is reducible.**
     Then there exists $a(x), b(x)$ where $deg\,[a(x)], deg\,[b(x)] < deg\,[g(x)]$ such that

     $$g(x) = m(x)n(x) \implies cp(x) = m(x)n(x) \implies p(x) = m(x)n(x)c^{-1}.$$

     This is a contraction, which means that $p(x)$ is irreducible $\implies g(x)$ is irreducible. ✓

   $\therefore p(x)$ is irreducible $\iff$ its associates are irreducible □

5. All monic polynomials of degree 2 in $\mathbb{Z}_3[x]$ have the form $x^2 + ax + b$ where $a, b \in \mathbb{Z}_3$ Out of all possible polynomials, the ones that are irreducible are given here:

   1) $x^2 + 1$
   2) $x^2 + 2$
   3) $x^2 + x + 1$
   4) $x^2 + x + 2$
   5) $x^2 + 2x + 2$

6. $\mathbb{Q}[x] \cong \mathbb{Q}[\pi]$?

   - **Homomorphic?**

     - $\varphi(\sum a_i X^i + \sum b_i X^i)$
       $= \varphi(\sum (a_i + b_i) X^i)$
       $= \sum (a_i + b_i)\pi^i$
       $= \sum a_i \pi^i + b_i \pi^i$
       $= (\sum a_i \pi^i) + (\sum b_i \pi^i)$
       $= \varphi(\sum a_i X^i) \oplus \varphi(\sum b_i X^i)$ ✓
     - $\varphi(\sum a_i X^i \times \sum b_i X^i)$
       $= \varphi(\sum_{i=0}^{\infty} \sum_{j=0}^{i} a_j X^j b_{i-j} X^{i-j})$
       $= \varphi(\sum_{i=0}^{\infty} (\sum_{j=0}^{i} a_j b_{i-j}) X^i)$
       $= \sum (\sum_{j=0}^{i} a_j b_{i-j}) \pi^i$
       By the rule of polynomial multiplicaiton
       $= \sum a_i \pi^i * \sum b_i \pi^i$
       $= \varphi(\sum a_i X^i) \odot \varphi(\sum b_i X^i)$ ✓

     $\therefore \varphi$ is homomorphic. □
   - **Injective?**
     Given $p(x), q(x) \in \mathbb{Q}[x]$, $\quad p(x) = \sum m_i X^i$ and $q(x) = \sum n_i X^i$
     Assume $\varphi(p(x)) = \varphi(q(x)) \iff \varphi(\sum m_i X^i) = \varphi(\sum n_i X^i)$,that is $\sum m_i \pi^i = \sum n_i \pi^i$ then since π is transcendent over $\mathbb{Q}$, $\sum m_i \pi^i = \sum n_i \pi^i$ if and only iff for all $i \in \mathbb{Z}, m_i \pi^i = n_i \pi^i$.
     $\therefore \varphi$ is injective. □
   - **Surjetive?**
     For any given $\sum v_i \pi^i \in \mathbb{Q}[\pi]$, let $h(x) = \sum v_i X^i$ then $\varphi(h(x)) = \sum v_i \pi^i$
     $\therefore \varphi$ is surjective □

$\therefore \mathbb{Q}[x] \cong \mathbb{Q}[\pi]$. $\square$

7. (a) Let $y(x) := x^4 - 2x^2 + 8x + 1$. Assume $y(x)$ is reducible in $\mathbb{Q}[x]$, then there are 2 options;
   1) That $y(x)$ has a root in $\mathbb{Q}$
      The only possible roots of $y(x)$ are of the form r/s where
      $r = \pm 1$(divisor of the constant term 1)
      and $s = \pm 1$ (divisor of the leading term 1)
      $\implies r/s = 1 \vee -1 \implies \quad y(1) = 8$ and $y(-1) = -10$
      $\therefore$ By the rational root test, $y(x)$ has no root in $\mathbb{Q}$
   2) Or the only possible factorization of $y(x)$ is as a product of two quadratics, by theorem 4.2.
      In this case theorem 4.23 shows that there is such a factorization in $\mathbb{Z}[x]$. Furthermore , there is a factorization as a product of monic quadratics in $\mathbb{Z}[x]$. Say

$$(x^2 + ax + b)(x^2 + ax + b) = y(x), \quad a, b, c, d \in \mathbb{Z}$$

$$\iff x^4 + (a + c)x^3 + (ac + b + d = x^2 + (bc + ad)x + bd = y(x)$$

$$\iff a + c = 0 \quad ac + b + d = -2, \quad bc + ad = 0, \quad bd = 1$$

$$\iff a = -c \implies -c^2 + b + d = -2, \quad bc - cd = 0$$

$$\iff bd = 1 \iff b = d = 1 \vee -1$$

$b = d = 1 \implies$

$$-c^2 + 1 + 1 = -2 \iff c = \pm 2$$

$c = 2 \implies$

$$bc - cd = 1 * 2 - 2 * 1 = 0 \neq 8$$

$c = -2 \implies$

$$bc - cd = 1 * (-2) - (-2) * 1 = 0 \neq 8$$

$b = d = -1 \implies$

$$-c^2 + (-1) + (-1) = -2 \iff c = 0$$

$c = 0 \implies$

$$bc - cd = (-1) * 0 - 0 * (-1) = 0 \neq 8$$

$\therefore$ There are no such $a, b, c, d \in \mathbb{Z}$ such that $y(x)$ can be factorized as a product of quadratics in $\mathbb{Z}[x]$, hence in $\mathbb{Q}[x]$.

$\therefore$ This is a contradiction. Thus $y(x)$ is irreducible, hence by theorem 5.10
$\mathbb{Q}[x]/(x^4 - 2x^2 + 8x + 1)$ is a field. $\square$

(b) $6x^8 + 14x^5 + 28x + 42$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion with $p = 7$
$\therefore$ By theorem 5.10 $\mathbb{Q}[x]/(6x^8 + 14x^5 + 28x + 42)$ is a field. $\square$

(c) $x^3 + 2x + 1$ is irreducible in $\mathbb{Z}_3[x]$ by corollary 4.19, because it has no roots in $\mathbb{Z}_3$.
$\therefore$ By theorem 5.10 $\mathbb{Z}_2[x]/(x^3 + 2x + 1)$ is a field. $\square$

8. Since $x^4 + x^3 + 1$ is relatively prime to $x^2 + x + 1$, by theorem 5.9, it follows that $[x^4 + x^3 + 1]$ is a unit in $\mathbb{Z}_2[x]/(x^2 + x + 1)$.
Let $u := x^4 + x^3 + 1$ and $v := x^2 + x + 1$. The inverse of v in $\mathbb{Z}_2[x]/(u)$ is a polynomial v^{-1} such that $uv^{-1} \equiv 1 (modv)$, or equivalently $vv^{-1} + ku = 1$ for some $k \in \mathbb{Z}_2[x]$. The Euclidean algorithm gives:

DOWN

$$u = vx^2 + (x^2 + 1)$$

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

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

UP

$$1 = (x^2 + 1) - x * x$$
$$1 = (x^2 + 1) - (v - (x^2 + 1)) * x$$
$$1 = (u - vx^2) - (v - (u - vx^2)) * x$$
$$1 = u - vx^2 - vx + ux - vx^3$$
$$1 = (u + ux) + (-vx^2 - vx - vx^3)$$
$$1 = u(1 + x) + v(x^3 + x^2 + x)$$

So, $v^{-1} = (x^3 + x^2 + x)$? I don't think this is right!