Mat220 portifolio

Fromsa Hera
student nr: 250487

April 24, 2018

1. - $p \sim q$ if it is;
     - **Refleksiv**
       Let $a \in \mathbb{Q}$ then $a - a = 0 \in \mathbb{Z}$. ✓
     - **Symmetric**
       Let $a, b \in \mathbb{Q}$. If $a - b \in Z$ then $b - a = -(a - b) \in \mathbb{Z}$ ✓
     - **Transitiv**
       Let $a, b, c \in \mathbb{Q}$. If $a - b \in Z$ and $b - c \in \mathbb{Z}$ then $a - c = a - b + b - c = (a - b) + (b - c) \in \mathbb{Z}$ ✓

     $\therefore p \sim q$
   - The equivalence class of $\frac{1}{2} = \{\frac{k}{2} | \, k \in \mathbb{Z}\}$
   - The equivalence class of $1 = \frac{1}{1} = \{\frac{k}{k} | \, k \in \mathbb{Z}\}$

2. - $gcd(n, n+2) \implies n + 2 = n \cdot 1 + 2 \implies$
     $(n \text{ is even } \implies n = 2 \cdot k + 0) \vee (n \text{ is odd } \implies n = 2 \cdot k + 1)$
     $\therefore$ possible solutions of $\gcd(n, n+2)$ are 2 and 1
   - $gcd(n, n+3) \implies n + 3 = n \cdot 1 + 3 \implies$
     $(n \text{ is even } \implies (n = 3 \cdot k + 0 \text{ if } k \text{ is even } \vee n = 3 \cdot k + 1 \text{ if } k \text{ is odd }))$
     $\vee$
     $(n \text{ is odd } \implies (n = 3 \cdot k + 0 \text{ if } k \text{ is odd } \vee n = 3 \cdot k + 1 \text{ if } k \text{ is even }))$
     $\therefore$ possible solutions of $\gcd(n, n+3)$ are 3 and 1

3. Since $\mathbb{Z}_7[x]$ is a field, $2x^2 + 1 \in \mathbb{Z}_7[x]$ and $x^4 - zx + 1 = x^4 + 1 \in \mathbb{Z}_7[x]$
   $x^4 + 1 = (2x^2 + 1)(4x^2 + 5) + 6$
   The quotient is $(4x^2 + 5)$ and the reminder is 6.

4. - **Homomorphism:**
     - $\varphi(\sum a_i X^i + \sum b_i X^i)$
       $= \varphi(\sum (a_i + b_i) X^i)$
       $= ((a_0 + b_0), (a_1 + b_1))$
       $= (a_0, a_1) \oplus (b_0, b_1)$
       $= \varphi(\sum a_i X^i) \oplus \varphi(\sum b_i X^i)$ ✓
     - $\varphi(\sum a_i X^i \times \sum b_i X^i)$
       $= \varphi(\sum c_i X^i)$ where $c_i = \sum_{n=0}^{i} a_i b_{i-n}$ where $n = 1$ because $\mathbb{Z}_2$ has to elements
       $= (c_0, c_1)$, where $c_0 = a_0 b_0$ and $c_1 = a_0 b_1 + a_1 b_0$
       $= (a_0 b_0, a_0 b_1 + a_1 b_0)$
       $= (a_0, a_1) \odot (b_0, b_1)$
       $\varphi(\sum a_i X^i) \odot \varphi(\sum b_i X^i)$ ✓

     $\therefore \varphi$ is homomorphic. $\square$
   - **Injective?**
     assume φ is injective then
     $\varphi(\sum a_i X^i) = \varphi(\sum b_i X^i)$

$\iff (a_0, a_1) = (b_0, b_1)$
$\iff a_0 = b_0$ and $a_1 = b_1$
$\iff (\sum a_i X^i) = (\sum b_i X^i)$
$\therefore \varphi$ is injective. $\square$

- **Surjetive?**
  assume $(a_0, a_1) \in R$ and that φ is surjective then there exists $\sum b_i X^i \in \mathbb{Z}_2[x]$ such that $\varphi(\sum b_i X^i) = (a_0, a_1) \iff (b_0, b_1) = (a_0, a_1) \iff b_0 = a_0$ and $b_1 = a_1$
  $\therefore \varphi$ is surjective $\square$
- **kernel**
  $0_R = (0, 0) \implies$ kernel of $\varphi = \sum a_i X^i \in \mathbb{Z}_2[x]$, where $a_0 = a_1 = 0$.

5. 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. ✓

6. Let $a := x^4 + x^3 + 1$ and $b := x^2 + x + 1$

   - $$a = b(x^2 + 1) + x$$
     $$b = x(x + 1) + 1$$
     Gives $\gcd(a, b) = 1$, meaning b is relatively prime to a, by theorem 5.9, it follows that $[b]$ is a unit in $\mathbb{Z}_2[x]/(b)$.
   - The inverse of a in $\mathbb{Z}_2[x]/(b)$ is a polynomial a^{-1} such that $aa^{-1} \equiv 1 \mod b$, or equivalently $aa^{-1} + mb = 1 \iff mb = 0$ for some $m \in \mathbb{Z}_2[x]$. The extended Euclidean algorithm gives:
     $$1 = b - x(x + 1) \wedge x = a - b(x^2 + 1) \implies$$

$$
\begin{aligned}
1 &= b - (a - b(x^2+1))(x+1) \\
&= b - a(x+1) + b(x^2+1)(x+1) \\
&= b(1 + (x^2+1)(x+1)) - a(x+1) \\
&= b(x^3 + x^2 + x + 2)) - a(x+1) \\
&= -a(x+1), \qquad b(x^3+x^2+x+2)) = 0 \\
a^{-1} &= -(x+1)
\end{aligned}
$$

$\therefore a^{-1} = -(x+1) = (x+1) \in \mathbb{Z}_2[x]$

7. Let $P_m = \{p_1, p_2, \dots p_n\}$ such that $m = p_1 \cdot p_2 \cdots p_n$ where $p_i \in \{\text{prime}\}$.

- Given $S = \{\frac{x}{y} | \text{when } \frac{x}{y} \text{ is reduced } = \frac{a}{b} \implies b = \text{odd}\}$. $b = \text{odd} \iff p_i \neq 2$, in P_b
  Given $\frac{a}{b}, \frac{c}{d} \in S$. S is a subring of $\mathbb{Q}$ if;
  - **S is closed under subtraction.**
    $\frac{a}{b} \cdot \frac{c}{d} = \frac{ad-bc}{bd}$
    Since $b, d = \text{odd} \implies bd = \text{odd}$ and therefore any subset of P_{bd} is also odd
    $\implies$ when $\frac{ac}{bd}$ is reduced, say $\frac{ad-bc}{bd} = \frac{r}{s}$, then $s = \text{odd}$, because P_s is a subset of P_{bd}.
    $\therefore S$ is closed under subtraction
  - **S is closed under multiplication.** $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
    The same argument as for the closure under subtraction applies here.
    $\therefore S$ is closed under multiplication

  $\therefore S$ is a subring of $\mathbb{Q}$
- Given $I \subset J, I = \{\frac{x}{y} | \text{when } \frac{x}{y} \text{ is reduced } = \frac{a}{b} \implies b = \text{odd} \wedge a = \text{even}\}$.
  $b = \text{odd} \iff p_i \neq 2$, in P_b
  $a = \text{even} \iff 2 * q_1 \cdot q_2 \cdots q_k$ where $q_i \in \{\text{prime}\}$
  Given $\frac{a}{b}, \frac{c}{d} \in S$. Then I is an ideal if;
  - **I is closed under subtraction**
    $\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$
    Form our earlier argument, bd is odd. and
    $ad - cd$
    $= (2 \cdot q_1 \cdot q_2 \cdots q_k)d - (2 \cdot t_1 \cdot t_2 \cdots t_l)b$
    $= 2((q_1 \cdot q_2 \cdots q_k)d - (t_1 \cdot t_2 \cdots t_l)b)$
    $\implies ad - cb$ is even, also when reduced, because the 2 does not get removed.
    $\therefore \frac{a}{b} - \frac{c}{d} \in I$
  - **And I absorbs products.** Given $\frac{r}{s} \in S$, then

* $\frac{r}{s} \cdot \frac{a}{b} = \frac{ra}{sd}$
  Form our earlier argument, sb is odd. $ra = r \cdot 2(q_1 \cdot q_2 \cdots q_n)$ is even also when reduced, because the 2 does not get removed.
  $\therefore \frac{r}{s} \cdot \frac{a}{b} = \frac{ra}{sd} \in I$. and
* $\frac{a}{b} \cdot \frac{r}{s} = \frac{ar}{bs}$
  Form our earlier argument, bs is odd. $ar = 2(q_1 \cdot q_2 \cdots q_n) \cdot r$ is even also when reduced, because the 2 does not get removed.
  $\therefore \frac{a}{b} \cdot \frac{r}{s} \in I$.

$\therefore I + J$ absorbs products.

$\therefore I$ is an Ideal, by theorem 6.1. Interesting to note is that I is just a principle Ideal generated by $\frac{2}{1} \in S$

- Show that $S/I \cong \mathbb{Z}_2$
  Given any element $\frac{a}{b} \in S$, consider the coset $\frac{a}{b} + I$. Then $\frac{a}{b}$ in reduced form is either a multiple of $\frac{2}{1}$, in which case $\frac{a}{b} \in I$, so that $\frac{a}{b} \equiv 0(mod\, I)$
  or $\frac{a}{b} - 1 \in I$, because $\frac{a}{b} - \frac{1}{1} = \frac{a+b}{b} \implies a + b$ is even, $\implies \frac{a}{b} \equiv 1(mod\, I)$
  Therefore S/I consists of two disjoint sets, (1+I) and (0+I).

  Let $f : S/I \to \mathbb{Z}_2$ where $f(a + I) = [a]$, for $a \in S/I$

  - Given $a + I, b + I \in S/I$, $f(a + I) = f(b + I) \iff [a] = [b]$
    $\therefore f$ is injective
  - For any given $[a]$ there exists $b+I \in S/I$ such that $f(b+I) = a \iff b = a$
    $\therefore f$ is surjective.
  - Given $a + I, b + I \in S/I$
    * **Closed under addition**
      $f((a+I)+(b+I)) = f((a+b)+I) = [a+b] = [a]+[b] = f(a+I)+f(b+I)$
      $\therefore f$ is closed under addition.
    * **Closed under multiplication**
      $f((a+I)\cdot(b+I)) = f((a\cdot b)+I) = [a\cdot b] = [a]\cdot[b] = f(a+I)\cdot f(b+I)$
      $\therefore f$ is closed under multiplication.

  $\therefore$ under f we get that $S/I \cong \mathbb{Z}_2$ $\square$

8. **(1)** Let $f : \mathbb{Z}_8 \to \mathbb{Z}_{15}$ be a group homomorphism

   (2) The additive groups $\mathbb{Z}_8$ and $\mathbb{Z}_{15}$ are cyclic groups with order 8 and 15 respectively. They are both generated by 1, meaning that $[a] = [1 + 1 + 1 + \cdots \text{(a times)}] = [1] + [1] + [1] + \cdots \text{(a times)} = a[1]$

   (3) Group homomorphism preseves identity, therefore $[0]_{15} \to [0]_8$

   (4) Let $f([1]) = [n]$ for some $[n] \in \mathbb{Z}_8$

$$f(15) = f([0])$$

$$f([7] + [8]) = f([0])$$

$$\iff \textbf{(2)}$$

$$f(7[1] + 8[1]) = f([0])$$

$$\iff \textbf{(1)}$$

$$f(7[1]) + f(8[1]) = f([0])$$

$$7f([1]) + 8f([1]) = f([0])$$

$$\iff \textbf{(4)}, \text{ and } \textbf{(3)}$$

$$7[n] + 8[n] = [0]$$

$$7[n] + [0] = [0]$$

$$7[n] + [n] = [0] + [n]$$

$$8[n] = [n]$$

$$[0] = [n]$$

Since $[n] = [0]$, it follows that $f([k]) = f(k[1]) = kf([1]) = k[n] = k[0] = [0]$ for any $k \in \mathbb{Z}_{15}$

$\therefore f \equiv 0$