M 431: Assignment 12

Nathan Stouffer

Page 139 — Problem 3

Problem. Let p be an odd prime and let $1 + 1/2 + \cdots + 1/(p-1) = a/b$ where $a, b \in \mathbb{Z}$. Show that $p \mid a$.

Proof. Before beginning this homework, I had a busy week so I didn't get to as much of this as I wanted, sorry! For this problem, we gain from the hint that for any $k \in \mathbb{Z}_p$ we have some $n_k \in \mathbb{Z}$ and a unique $l_k \in \mathbb{Z}_p$ such that $kl_k = 1 + n_k p$ (this is gained from the fact that $(k, p) = 1$). Now, in the context of rational numbers, this means that $1/k = l_k/(1 + n_k p)$. Then our desired sum is

$$\sum_{k=1}^{p-1} \frac{1}{k} = \sum_{k=1}^{p-1} \frac{l_k}{1 + n_k p}$$

But l_k runs over all elements of U_p so when we multiply the sumation by 1 in the form of the least common multiple of the terms $1 + n_k p$ divided by itself, each term in the numerator will contain a p for maybe the constant terms. But then we have the same denominator in all the polynomials so the constant terms of each numerator sum to $-1 - 2 - \cdots - (p-1)$. But this is a multiple of p (odd) since there are an even number of terms (so each natural number cancels and we sum a number of p's). Thus, each term in the numerator is divisible by p so the numerator is divisible by p. But then we have a rational form the sum of $1/k$ where p divides the numerator as desired.

$\square$

Page 150 — Problem 3

Problem. In example 3, show that $M = \{x(2+i) \mid x \in R\}$ is a maximal ideal of R.

Proof. First note that $R := \{a + ib \mid a, b \in \mathbb{Z}\}$ and $M := \{x(2+i) \mid x \in R\}$. Now let's show that M is an ideal of R. That M is nonempty is satisfied because $1(2+i) = 2+i \in M$. M is an additive subgroup of R as verified by the aesthetic definition: for any $x(2+i), y(2+i) \in M$ we have that $x(2+i) - y(2+i) = (x-y)(2+i) \in M$. M is closed by left multiplication: for any $a + bi \in R$ and $x(2+i) \in M$ we have $(a+bi)x(2+i) = x'(2+i) \in M$ where $x' = (a+bi)x'$. Closure from right multiplication holds since R with multiplication is abelian.

I could not find a direct proof that M is maximal so I rest on the result of the previous problem that $R/M \cong \mathbb{Z}_5$ a field which implies that M is maximal.

□

Page 150 — Problem 4

Problem. In Example 3, show that $R/M \cong \mathbb{Z}_5$.

Proof. Here we use the first isomorphism theorem. To do this, we must find a surjective homomorphism φ from $R \longrightarrow \mathbb{Z}_5$ that has $M = \ker\varphi$. Consider the map $\varphi : R \longrightarrow \mathbb{Z}_5$ defined by taking $r = a+bi \mapsto a+3b$ modulo 5. We verify the three properties.

Homomorphism: pick any $a + ib, a' + ib' \in R$. For $+$, we have $\varphi(a + ib) + \varphi(a' + ib') = a + 3b \mod 5 + a' + 3b' \mod 5 = (a+a') + 3(b+b') \mod 5 = \varphi(a+a'+i(b+b')) = \varphi((a+ib)+(a'+ib'))$. For $*$, we have

$$\varphi(a + ib)\varphi(a' + ib') = (a + 3b \mod 5)(a' + 3b' \mod 5) = aa' + 3ab' + 3a'b + 4bb' \mod 5$$

and

$$\varphi((a+ib)(a'+ib')) = \varphi(aa'-bb'+i(ab'+a'b)) = aa'-bb'+3(a'b+ab') \mod 5 = aa'+3a'b+3ab'+4bb' \mod 5$$

where the crucial simplification steps were made with congruence/arithmetic modulu 5.

Onto: this is checked easily, for $m \in \mathbb{Z}_5$ pick $m + i0 \in R$.

Kernel: we wish to show that $\ker\varphi = M$. Going to the left, pick any $r = a + ib \in \ker\varphi \subset R$. Then $\varphi(r) = \varphi(a + ib) = 0 \mod 5 \implies a + 3b \equiv 0 \mod 5 \implies a \equiv -3b \mod 5 \implies a \equiv 2b \mod 5 \iff 5 \mid (a - 2b)$ which means there exists some $k \in \mathbb{Z}$ such that $5k = a - 2b \iff a = 5k + 2b$. Then we can rewrite $r = a + bi = 5k + 2b + ib = (2 + i)(2 - i)k + b(2 + i)$. Both terms are members of M so their sum is a member of M, which is to say $r \in M$.

Now the other direction, pick any $(a + ib)(2 + i) \in M$. We have $(a + ib)(2 + i) = 2a - b + i(a + 2b) \implies \varphi(2a-b+i(a+2b)) = 2a-b+3(a+2b) \mod 5 = 2a+3a-b+5b \mod 5 = 5a+5b \mod 5 = 0 \mod 5$.

So we have verified everything we need to and the first isomorphism theorem shows says that $R/M \cong \mathbb{Z}_5$.

$\square$

Page 150 — Problem 5

Problem. In Example 3, show that $R/I \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Proof. Here R is the same as in the previous two problems and $I := \{a + bi \in R \mid 5 \mid a \text{ and } 5 \mid b\}$. Note that I meets all the requirements to be an ideal so it makes sense to consider R/I. For this problem, I would like to use the first isomorphism thereom again. Consider $\psi : R \longrightarrow \mathbb{Z}_5 \oplus \mathbb{Z}_5$ defined by taking $a - ib \mapsto (a + b \mod 5, a - b \mod 5)$ (note the $-$ instead of the $+$ in the definition of R, we still have every member of R just in a different form). I found that ψ is a homomorphism but I failed to verify the onto and kernel properties for the first isomorphism thereorm. If these hold, then the two groups are isomorphic.

Homomorphism: pick any $a - ib, x - iy \in R$. Addition holds by an easy check that I omit. Multiplication is preversed since $\psi((a-ib)(x-iy)) = \psi(ax+by-i(ay+bx)) = (ax+by+(ay+bx), ax+by-(ay+bx)) = (a(x+y)+b(x+y), a(x-y)-b(x-y)) = (a+b, a-b)(x+y, x-y) = \varphi(a-ib)\varphi(x-iy)$ where I omit the $\mod 5$ in the co-domain to reduce clutter.

Onto: I could not quite verify this property but here is what I have. For $(m, n) \in \mathbb{Z}_5 \oplus \mathbb{Z}_5$ we could require that for $a + ib$ we have $a + b = m$ and $a - b = n$. We know solutions for a, b since the matrix $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is invertible but our solutions for a, b punch out of the integers so this does not seem like the right route. I look forward to the solution on this problem!

Kernel: I also could not verify this.

$\square$

Page 163 — Problem 1

Problem. If F is a field, show that the only invertible elements in $F[x]$ are the nonzero elements of F.

Proof. We will show that an element of $p(x) \in F[x]$ is invertible if and only if $p(x)$ is nonzero in F. Going to the left, pick a $p(x) \in F[x]$ such that $p^{-1}(x)$ exists. That is $p * p^{-1} = p^{-1} * p = 1 \in F[x]$. For a contradiction, let $\deg p = n > 0$. This implies that $m = \deg p^{-1} > 0$ as well since a polynomial of degree $n > 0$ times a polynomial of degree 0 would still be a polynomial of degree n, which would not be the identity. But then multiplying p and p^{-1} gives a polynomial of degree $m + n$, which is not the identity. So we reached a contradction and must have that $p(x) \in F$. Further, it is not 0 since 0 has no multiplicative inverse.

Now going the right, any polynomial in $f \in F[x]$ that is a nonzero element of F has the inverse $f^{-1} \in F$.

□

Page 163 — Problem 3

Problem. Find the greatest common divisor of the following polynomials over $\mathbb{Q}$, the field of rational numbers.

(a) $x^3 - 6x + 7$ and $x + 4$
(b) $x^2 - 1$ and $2x^7 - 4x^5 + 2$
(c) $3x^2 + 1$ and $x^6 + x^4 + x + 1$
(d) $x^3 - 1$ and $x^7 - x^4 + x^3 - 1$

Proof. I'm running short on time, so I didn't show much work on these ones.

(a) Here, $x + 4$ is irreducible so we only need to test if $x + 4$ divides $x^3 - 6x + 7$. Using long division, I found that this was not the case. So the greatest common divisor is the polynomial 1.

(b) Here $x^2 - 1 = (x + 1)(x - 1)$. Using long divion again, I found that $x - 1$ divides $2x^7 - 4x^5 + 2$ but $x + 1$ does not so the greatest common divisor is $x - 1$.

(c) $3x^2 + 1$ is irreducible in $\mathbb{R}[x]$ so it is certainly irreducible in $\mathbb{Q}$. For this problem, I found the zeros of $3x^2 + 1$ in the comple plane then computed their output in the polynomial $x^6 + x^4 + x + 1$. Neither resulted in 0, so $3x^2 + 1$ does not divide $x^6 + x^4 + x + 1$ and the greatest common divisor is 1.

(d) For this one, $x^7 - x^4 + x^3 - 1 = x^4(x^3 - 1) + 1(x^3 - 1) = (x^4 + 1)(x^3 - 1)$ so $x^3 - 1$ is the greatest common divisor!

$\square$