Assignment 2: Polynomials and Stuff

Dr. Rocca

Due 6-16-2021

Instructions

Do two problems from each section. You may do two additional exercises from any section in order to earn an extra +10%. All your answers must be in complete sentences written using proper grammar and notation, and all details must be included. Overall presentation/professionalism of your work will count for up to 10% of your grade. You may work in a group if you like, however there can be no more than three students in a group and you need to include all of your names. All of your work must be your own, and you must be prepared to explain and answer questions about your work if asked.

1 Polynomials

1.1. For the first three parts of this question the polynomials are in $\mathbb{Z}_2[x]$, polynomials with coefficients from the field $\mathbb{Z}_2$. For the last part you need to try and generalize what you did to $\mathbb{Z}_p[x]$ for any prime p.

(a) How many distinct polynomials are there of degree 1, $f(x) = ax + b$?

(b) How many distinct polynomials are there of degree 2, $f(x) = ax^2 + bx + c$? How can we use the answer from the previous part to show that only one is irreducible?

(c) How many distinct polynomials are there of degree 3, $f(x) = ax^3 + bx^2 + cx + d$? How can we use the answers from the previous parts to show that only two are irreducible?

(d) Try and generalize the previous results to $\mathbb{Z}_p[x]$. It would be a good idea to try with $\mathbb{Z}_3[x]$ first and look for patterns. Also, it will be helpful to recall that the formula for choosing k objects from n with replacement is the binomial

$$\binom{n+k-1}{k}.$$

1.2. Let the rings R and S be defined by

$$R = \mathbb{Z}_2[x]/(x^2 + x + 1)$$

and

$$S = \left\{a + b\alpha \middle| a, b \in \mathbb{Z}_2, \alpha^2 = \alpha + 1\right\}.$$

Use these to answer the following.

(a) Write down the four elements of each ring.

(b) Create an addition table for each ring.

(c) Create a multiplication table for each ring.

(d) Looking at your previous answers, why are these rings isomorphic?

(e) Looking at your previous answers, why are these rings fields?

(f) Define $\phi : \mathbb{Z}_2[x] \longrightarrow S$ by $\phi(f(x)) = f(\alpha)$. What is the kernel of phi?

(g) How does your previous answer give another reason why R is isomorphic to S?

1.3. Suppose F is a field and that $q(x) \in F[x]$ is reducible, in particular $q(x) = p_1(x)p_2(x)p_3(x)$ where each $p_i(x)$ is irreducible. Prove that

$$F[x]/(q(x)) \cong F[x]/(p_1(x)) \oplus F[x]/(p_2(x)) \oplus F[x]/(p_3(x)).$$

(Hint: Use exercise 2.2b.)

2 Homomorphisms and Ideals

2.1. Assume that R is a commutative ring with unity and that $\gamma : R \longrightarrow R'$ is a surjective homomorphism with kernel K. For each of the following let $A' \subseteq R'$ be an ideal and $A = \{a \in R | \gamma(a) \in A'\}$.

(a) Prove that A is an ideal in R.

(b) Prove that $K \subseteq A$.

(c) Prove that A/K is isomorphic to A'. (Hint: What is $\gamma(A)$?)

(d) How does this show that there is a one-to-one correspondence between ideals in R' and ideals in R which contain the kernel of K?

2.2. Complete the following two parts and then explain why the second part is a generalization of the first.

(a) Define $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3$ by

$$\phi(z) = (z\,(mod\,2), z\,(mod\,3))\,.$$

Show that the kernel of ϕ is the ideal $6\mathbb{Z}$, the multiples of 6. Why does this tell us that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$.

(b) Let R be a ring and I and J be ideals in R. Define $\psi : R \longrightarrow R/I \oplus R/J$ by

$$\psi(r) = (r + I, r + J)\,.$$

Show that $I \cap J$ is the kernel of ψ. How do we know that $R/(I \cap J)$ is isomorphic to $R/I \oplus R/J$?

2.3. Show that

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \in \mathbb{R} \right\}$$

is a ring and that

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in \mathbb{R} \right\}$$

is an ideal. Now construct a surjective homomorphism from R to $\mathbb{R} \oplus \mathbb{R}$ such that I is the kernel of the homomorphism. How do we no know that R/I is isomorphic to $\mathbb{R} \oplus \mathbb{R}$?