Notes 2

Will Magrath

December 2025

1 Direct Sums of Rings

(Similar to direct products of groups) Suppose R_1 and R_2 are two rings, the direct sum $R_1 \oplus R_2 is (a, b) + (c, d) = (a + c, b + d) \wedge (a, b) * (c, d) = (a * c, b * d)$

Proof is the Chinese Remainder Theorem

Not always useful with rings

2 Characteristic of Rings

If R is a ring, we define the characteristic of R ($char(R)$) to be the order of 1 in the additive group if the group is finite. If the order is infinite, the characteristic is said to be 0

Examples: char($\mathbf{Z}_3$) = 3, char($\mathbf{Z}_3[x]$) = 3, char($\mathbf{Z}_6$) = 6

Proposition: if F is a field, then char(F) is 0 or prime. Proof: Suppose F is a field where char(F) is neither 0 or prime. We will show this results in a contradiction. char(F) not being prime or 0 implies that char(F) is 1 or a composite number. Case 1: char(F) is 1. This means "one added to itself one times" is zero, so 1 = 0, and fields can't have the multiplicative identity equal the additive identity, so it is not a field. Case 2: char(F) is a composite number, n. This means there exists two integers, a and b, whose product is equal to n. Because $a < n \wedge b < n$, then $a * 1 = (1 + 1 + ... + 1) = / = 0$. Similarly, $b * 1 = (1 + 1 + ... + 1) = / = 0$. You can multiple these together to get $(1 + ... + 1) * (1 + ... + 1) = 0$, but this would imply a or b are zero divisors, which contradicts F being a ring.

3 Ideals

If R is a ring, an ideal, I, is a nonempty subset of R such that $\forall a, b \in I, a + b \in I$ and $\forall a \in I, \forall r \in R, r * a \in I$.

Example: an ideal of $\mathbf{Z}$ is $2 * \mathbf{Z}$

Every ring has two trivial ideals, 0 and R itself

Proposition: IF I is an ideal of R, then it is a subgroup of the additive group of R.

Remark: If I is an ideal of R, then I is not a subring unless I = R. This is because the ideal never has a multiplicative identity otherwise.

4 Principal Ideals

If R is a ring, and $a \in R$, we call the ideal ¡a¿ $= ra | r \in R$ a principal ideal

Proof: $a \in < a > - >< a >$ is nonempty. Let $r_1 * a, r_2 * a \in < a >$ then $r_1 a + r_2 a = (r_1 + r_2)a \in < a >$. Let $r_3 \in R$, then $r_3 * r_1 * a = (r_3 * r_1)a \in < a >$

A ring is a Principal Ideal Domain (PID) if every ideal is a principal ideal.

The integers are an example of this. We already proved this near the beginning of the semester when we showed every subgroup of the integers under addition is just a number times every integer.

An Example of an Ideal that is not principal is all the polynomials with integer coefficients. The set I = every polynomial with an even constant term is an ideal, but is not a principal ideal. Proof it can't be a Principal Ideal: we will do this by contradiction. Suppose an ideal existed that was equal to ¡f(x)¿ Because 2 is in I, then there exists a g(x) such that 2 = g(x)f(x). 2 has order 0, so g(x) and f(x) has order 0. More specifically, we know f(x) must be 2, -2, 1, or -1 because those are the integer factors of 2. An integer to the power of anything can't equal a polynomial, so this is a contradiction.

5 Additive Factor Groups

If I is an ideal of R, the additive factor group is written as R/I which is the cosets of I in R. Despite I not necessarily being a ring, R/I is.

Proof: Suppose (a + I) = (a' + I) and (b + I) = (b' + I). a and a' are said to be equal iff a - a' is in I. This works the same for b and b'. Because any element times an element of an ideal is in an ideal, then (a-a')*b is in I, and (b - b')a is in I. Their sum must be in I, so $(a-a')b+a'(b-b') = ab-a'b+a'b-a'b' = ab-a'b'$. Therefore, R/I is well-defined under multiplication. Obviously, multiplication is closed (by definition) and associativity is inherited. It is easily seen that (1 + I) is the multiplicative identity. This implies that multiplication is a monoid, and distributivity is fairly trivial to prove. This included with the fact that addition is a group, and acknowledging the fact that R/I is nonempty because I is in R/I, then R/I must be a ring.