Math 494

Yiwei Fu

Jan 13, 2022

1

FACT: If G is a finitely generated subgroup of $\mathbb{C}^*$, then $\forall n \in \mathbb{N}$, the equation $x_1+x_2+\ldots+x_n=1$ has only finitely many solutions with $x_1, x_2, \ldots, x_n \in G$, in which no nonempty subset of x_i's sums to 0.

Extra credit: does $\exists$ such a G for which $\exists$ solutions as above for infinitely many n?

Example 1.1. 0 ring: $0 = 1$.

0 homomorphism: for any ring $R, f : R \to$ "zero ring", $r \mapsto 0$.

Definition 1.1. If $f : R \to S$ is a ring homomorphism, then the kernel of f is

$$\ker f = \{r \in R : f(r) = 0\}.$$

We know $\ker f$ is a subgroup of R under $+$. Also: if $r \in \ker f$ and $r' \in R$ then $rr' \in \ker f$ since $f(rr') = f(r)f(r') = 0 \cdot f(r') = 0$.

Definition 1.2. Suppose R is a ring. An ideal of R is a subgroup of $(R, +)$ which is closed under multiplication by R.

Ideals are great.

From NOW ON: ALL rings are commutative.

Example 1.2. Ideals in $\mathbb{Z}$: $n\mathbb{Z}, (n \in \mathbb{Z}_{\geq 0})$

NOTE: A nonempty subset of R is an ideal $\iff \forall n \geq 0, \forall r_1, \ldots, r_n \in R, i_1, i_2, \ldots, i_n \in I, r_1 i_1 + r_2 i_2 + \ldots + r_n i_n \in I$.

Definition 1.3. For $r \in R$ the principal ideal (r) (also denoted as rR) is $\{rr' : r' \in R\}$.

Unit ideal of R is $(1) = 1R = R$. Zero ideal of R is $(0) = \{0\}$.

A "proper ideal" of R is an ideal which is not (0) or (1).

NOTE: If $f : R \to S$ is a homomorphism then $\ker f$ is an ideal of R. $\ker f = (1) \iff S =$ "0 ring", $\ker f = (0) \iff f$ is injective.

Suppose R is a ring and I is an ideal. Then R/I is a group under addition.

Proposition 1.1. *R/I is a ring.*

Proof. Define $(r + I)(r' + I) := rr' + I$. Note that if $i, i' \in I$ then $(r + i)(r' + i') = rr' + ri' + ir' + ii' \in rr' + I$.

Rest is easy. ∎

Example 1.3. $R = \mathbb{Z}, I = 3\mathbb{Z}, R/I = \mathbb{Z}/3\mathbb{Z}$.

In general, $\mathbb{Z}/n\mathbb{Z}$ is the quotient of the ring R by the ideal $n\mathbb{Z}$.

Definition 1.4. A field is a nonzero ring in which every nonzero element has a multiplicative inverse.

Example 1.4. $\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$ where p is prime.

NON-EXAMPLES: $\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$.

Definition 1.5. An integral domain is a nonzero ring R with no zero divisors ($a, b \in R, ab = 0 \implies a = 0$ or $b = 0$).

If R is a field, what are the ideals of R?

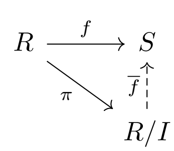
Only (0) and (1). since if an ideal I contains a nonzero $r \in R$, then $I \ni rr^{-1} = 1 \implies I = (1)$.

Proposition 1.2. *If $f : R \to S$ is a ring homomorphism andd R is a field. then either f is injective or $S =$ "0 ring".*

Notation: often $R =$ ring, $I =$ ideal. for $r \in R$ we denote the element $r + I$ of R/I by $\overline{r}$.

Theorem 1.1. *$f : R \to S$ is a ring homomorphism with kernel K. Let I be an ideal of R. Let $\pi : R \to R/I$ be the quotient map.*

1. *If $I \subseteq K$ then $\exists$ a unique homomorphism $\overline{f} : R/I \to S$ s.t. $\overline{f} \circ \pi = f$.*



2. *If $I = K$ and f is surjective then $\overline{f}$ is $\cong$.*

Theorem 1.2. *(Correspondence Theorem) $f : R \to S$ is a surjective ring homomorphism with kernel K. Then the maps $I \mapsto f(I)$ and $J \mapsto f^{-1}(J)$ are inverse bijections {ideals of R containing K} {ideals of S}.*

Proof. We know that these maps induce bijections between subgroups of $(R, +)$ containing K and subgroups between $(S, +)$. Check:

1. $I =$ ideal of R containing $K \implies f(I) =$ ideal of S since every $s \in S$ is $f(r), r \in R$, so $i \in I \implies s \cdot f(i) = f(r)f(i) = f(ri) \in f(I)$.
2. $J =$ ideal of S then (from group result) $f^{-1}(J)$ is a subgroup of $(R, +)$ which contains K, and $f^{-1}(J)$ is an ideal since $r \in J, i \in f^{-1}(J) \implies f(ri) = f(r)f(i) \in SJ = J$. ■

SUPPLEMENT: same notation, $R/I \cong S/f(I)$.