LECTURE 3.

ALIREZA SALEHI GOLSEFIDY

Let's see a few new construction of rings:

Definition 1. Let $R_1, R_2, \ldots, R_n$ be rings. Similar to groups, we can consider their *direct sum*. Namely

$$R_1 \oplus \cdots \oplus R_n = \{(r_1, \ldots, r_n) | \ \forall\, i,\ r_i \in R_i\}$$

gives us a new ring (with componentwise addition and multiplication). It is again called the *direct sum* of $R_1, \ldots, R_n$.

Example 2. *Let* $(G, +)$ *be an abelian group. Then* $(\mathrm{Hom}(G, G), +, \circ)$ *is a ring. (It is easy to check all the properties. Notice that* $(\mathrm{Fun}(G, G), +, \circ)$ *is NOT a ring.)*

Remark 3. The above example is a generalization of the fact that $\mathrm{M}_n(\mathbb{Q}) = \mathrm{Hom}(\mathbb{Q}^n, \mathbb{Q}^n)$ or $\mathrm{M}_n(\mathbb{Z}) = \mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}^n)$ are rings!

Remark 4. Whenever you see a new object (structure) in math, you should ask about the maps which preserve its structure (usually called *homomorphisms*) and its subsets with similar structure (sub-, e.g. subgroups).

Let R be a ring. A non-empty subset S of R is called a *subring* if it is a ring with respect to operations of R.

Lemma 5. *Let S be anon-empty subset of R. Then S is a subring if and only if*

1. *it is closed under multiplication, i.e.* $\forall\, a, b \in S,\ ab \in S$.
2. *it is closed under subtraction, i.e.* $\forall\, a, b \in S,\ a - b = a + (-b) \in S$.

Proof. From group theory, we know that $(S, +)$ is a subgroup of $(R, +)$. By the assumption $(S, \cdot)$ is a semigroup. And since R is a ring, we have the distribution rules. Hence S is a subring. □

Example 6. $S \subseteq \mathbb{Z}$ *is a subring if and only if* $S = n\mathbb{Z}$ *for some* $n \in \mathbb{Z}$.

Proof. First let us check that for any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subring. By Lemma 5 it is enough to check the followings:

1. (Closed under multiplication) $\forall\, k, k' \in \mathbb{Z},\ (nk) \cdot (nk') = n(nkk') \in n\mathbb{Z}$.
2. (Closed under subtraction) $\forall\, k, k' \in \mathbb{Z},\ nk - nk' = n(k - k') \in n\mathbb{Z}$.

To see the other direction, we prove that even any subgroup of $(\mathbb{Z}, +)$ is of the above form. Let S be a (additive) subgroup of $\mathbb{Z}$. If $S = \{0\}$, we are done. So assume that there is $0 \neq a \in S$. Since S is a subgroup, $-a$ is also in S. Either a or $-a$ is a positive integer. So $S \cap \mathbb{N}$ is a non-empty subset of $\mathbb{N}$. Thus by the well-ordering principle there is a smallest element n in $S \cap \mathbb{N}$. We claim that $S = n\mathbb{Z}$. If not, there is $b \in S$ which is not a multiple of n. By division algorithm there is an integer q and a positive integer r such that

$$b = nq + r, \text{ and } r < n.$$

Hence $r = b - nq \in S \cap \mathbb{N}$ which contradicts the fact that n is the smallest element in $S \cap \mathbb{N}$. □

Example 7. *Let R be a unital ring. Then the group generated by 1_R is a subring of R.*

Date: 1/9/2012.

Proof. Clearly it is closed under subtraction. So by Lemma 5 it is enough to check that it is closed under multiplication, for any $k, k' \in \mathbb{Z}$, we have:

$$(k\ 1_R) \cdot (k'\ 1_R) = \sum_{i=1}^{|k|} (\operatorname{sgn} k)\ 1_R \cdot \sum_{j=1}^{|k'|} (\operatorname{sgn} k') 1_R = \sum_{i=1}^{|k|} \sum_{j=1}^{|k'|} (\operatorname{sgn}(k)\ 1_R) \cdot (\operatorname{sgn}(k')\ 1_R)$$
$$= \sum_{i=1}^{|kk'|} (\operatorname{sgn}(kk'))\ 1_R = (|kk'|)\ (\operatorname{sgn}(kk')) 1_R = (kk')\ 1_R,$$

where

$$\operatorname{sgn}(k) := \begin{cases} 1 & \text{if } k > 0, \\ 0 & \text{if } k = 0, \\ -1 & \text{if } k < 0. \end{cases}$$

□

Definition 8. Let R be a ring and $a \in R$. a is called a *right zero-divisor* (resp. *left zero-divisor*) if there is $0 \neq b \in R$ such that $ba = 0$ (resp. $ab = 0$). a is called a zero divisor if there are non-zero elements b and b' such that $ab = b'a = 0$.

Example 9. *If $a \in U(R)$, then a is not a left (or right) zero divisor.*

Definition 10. Let R be a commutative unital ring. It is called an *integral domain* if it has no zero-divisors.

Example 11.
(1) *$\mathbb{Z}$ is an integral domain.*
(2) *$\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ and it is an integral domain.*
(3) *$\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.*

Let's again look at the invertible elements.

Remark 12. 0 can never be invertible unless $R = \{0\}$. So $U(R) \subseteq R \setminus \{0\}$.

Definition 13. A unital ring R is called a *division ring* (or a skew field) if $U(R) = R \setminus \{0\}$. A commutative division ring is called a *field*.

Example 14.
(1) *$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.*
(2) *$\mathbb{Z}$ and $\mathbb{Z}[i]$ are not fields.*
(3) *$\mathbb{Q}[i] = \{a + bi |\ a, b \in \mathbb{Q}\}$ is a field.*
(4) *It is not easy to construct division algebras. Here is one of the easiest examples,*

$$\mathbb{H} := \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \mid a, b \in \mathbb{C} \right\}.$$

It is called a quaternion algebra. I will leave it as an exercise to show that $\mathbb{H}$ is a division ring.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: asalehigolsefidy@ucsd.edu