Lecture 11

2.2 Rings: integral domains, subrings. The integers mod n. Units

The notion of subring is the obvious analogue of the notion of subgroup.

Def (subring) A subset $S \subset R$ is a subring if it is itself a ring with respect to the operations on R

Criterion A subset S of a ring R is a subring iff $0, 1 \in S$, S is closed with respect to addition and multiplication of R, and S contains the negative of each of its elements.
(alternatively, think of the conds on addition as: $(S,+) \leq (R,+)$)

Examples

- $(\mathbb{Z},+,\cdot)$ is a subring of $(\mathbb{Q},+,\cdot)$ which is in turn a subring of $(\mathbb{R},+,\cdot)$
- Let $\mathbb{Z}[x] :=$ polynomials in x with integer coefficients. Then $(\mathbb{Z}[x],+,\cdot)$ is a subring of $\mathbb{Q}[x]$
- Let $S = \left\{ \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \mid d_1, d_2 \in \mathbb{Z} \right\} \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{Z})$. Then S is a subring of $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$. Note that S is a commutative subring of $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

Example (The integers modulo n)

Consider $(\mathbb{Z}_n,+)$ the cyclic group of integers modulo n with operation the addition mod n.
We can further define on this set an operation: $a \cdot_n b :=$ the remainder of $a \cdot b$ (usual $\mathbb{Z}$ multiplication) divided by n.

For instance, in $\mathbb{Z}_{12}$ $(4)_{12}(7) = 4$ ($4 \cdot 7 = 28$, the remainder mod 12 is $28 - 2 \cdot 12 = 28 - 24 = 4$)

Fact $(\mathbb{Z}_n, +_n, \cdot_n)$ is a ring.
we won't write these indices if it's clear from the context what is n.

Again in $\mathbb{Z}_{12}$ consider the following

$3 \cdot 8 = (24 =) 0$ that is, 3 and 8 are zero divisors in $\mathbb{Z}_{12}$

This tells us that $\mathbb{Z}_{12}$ is not an integral domain

Can we find $b \in \mathbb{Z}_{12}$ such that

$5 \cdot b = 1$? That is, does there exist a multiplicative inverse of 5 mod 12?

... $5 \cdot 5 = (25 =) 1$

One can check: $1, 5, 7, 11$ have multiplicative inverses mod 12.
$2, 3, 4, 6, 8, 9, 10$ don't (and they are zero divisors)

We shall see that these properties are strictly related to arithmetic properties.

Definition • An element u in a ring R is a unit of R if it has a multiplicative inverse in R.

• We will denote $U(R)$ the units of the ring R.

Examples • $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$

• $U(Mat_{2\times 2}(\mathbb{R})) = GL_{2\times 2}(\mathbb{R})$ the set of invertible 2x2 matrices with real entries
↑ actually: group

Note that in $\mathbb{Z}_{12}$: $5\cdot 7 = 11$ $\quad$ $7\cdot 11 = 5$

$5^2 = 7^2 = 11^2 = 1$ $\quad$ $5\cdot 11 = 7$

(*)

That is, $U(\mathbb{Z}_{12})$ is closed under multiplication mod 12. The multiplicative identity $1 \in U(\mathbb{Z}_{12})$ and every element has multiplicative inverse in $U(\mathbb{Z}_{12})$ (*) (actually this is by def. of unit).

We have just proved that $(U(\mathbb{Z}_{12}), \cdot)$ forms an abelian group.

Note that $\mathbb{Z}_{12}$ does not form a group under multiplication.

What we have seen for the units mod 12 holds in general for the set of units of a ring:

Theorem If $(R, +, \cdot)$ is a ring then $(U(R), \cdot)$ is a group.

Associativity, existence of 1, existence of multiplicative inverses are clear from the properties of R / by def. of unit. But why is this set closed under multiplication?

Suppose $a, b \in U(R)$. This means, by def, that $\exists\ a_1, b_1 \in U(R)$ such that

$a\cdot a_1 = 1$ and $b\cdot b_1 = 1$
$(= a_1\cdot a)$ $\quad$ $(= b_1\cdot b)$

Showing that $a\cdot b \in U(R)$ means showing that the element ab has a multiplicative inverse. This is easy since:

$$(ab)(b_1 a_1) = a\cdot b\cdot b_1\cdot a_1 = 1$$

and

$$(b_1 a_1)(ab) = b_1\cdot a_1\cdot a\cdot b = 1$$

$\Rightarrow ab \in U(R)$.

Examples $U(\mathbb{Z}) = ?$

$U(\mathbb{R}) = ?$

Sometimes the notation $R^\times$ is also used for $U(R)$