Math 521A

6.1 – Ideals and Congruence

Recall:

$$\text{(Ring) } \mathbb{Z} \xrightarrow{\text{congruence modulo } n} \mathbb{Z}_n \text{ (New Ring)}$$

Congruence modulo n: $a \equiv b \pmod{n} \iff a - b \in n\mathbb{Z}$.

- $\mathbb{Z}_n = \{[0] = n\mathbb{Z}, [1] = 1 + n\mathbb{Z}, \ldots, [n-1] = (n-1) + n\mathbb{Z}\}$.
- We showed that $\equiv$ is an equivalence relation on $\mathbb{Z}$: Either

$$[a] = [b] \text{ or } [a] \cap [b] = \emptyset \quad \forall\, a, b \in \mathbb{Z}.$$

- Let $x \in \mathbb{Z}$. Then: $x \in [a] \iff x - a \in n\mathbb{Z}$.
- Let $a, b \in \mathbb{Z}$. Then: $[a] = [b] \iff a - b \in n\mathbb{Z}$.
- $[a] + [b] \overset{\text{def'n.}}{=} [a + b]$ and $[a] \cdot [b] \overset{\text{def'n.}}{=} [ab]$. We showed that both operations ($+$ and $\cdot$) are well-defined, i.e., the results are independent of the choice of the representatives of the classes.

Our next objective: In general, given a ring R and $I \subseteq R$, we would like to define congruence in R via I: Given $r, s \in R$,

$$r \equiv s \pmod{I} \iff r - s \in I.$$

The question is: What properties should I satisfy?

In order for $\equiv$ to be an equivalence relation, we must have:

(R) $r \equiv r \pmod{I}$ for all $r \in R$, so $0_R \in I$.

(S) $r \equiv s \pmod{I} \Rightarrow s \equiv r \pmod{I}$, so $x \in I \Rightarrow -x \in I$.

(T) $r \equiv s \pmod{I}, s \equiv t \pmod{I} \Rightarrow r \equiv t \pmod{I}$, so $r - s \in I, s - t \in I \Rightarrow r - t \in I$. In other words, $x, y \in I \Rightarrow x + y \in I$.

Finally, to insure that $[r][s] = [rs]$ is well-defined, we want:

$$r \equiv t \pmod{I}, \quad s \equiv u \pmod{I} \Rightarrow rs \equiv tu \pmod{I}.$$

From $r - t = a \in I$ and $s - u = b \in I$, we have

$$rs = (t + a)(u + b) = tu + tb + au + ab.$$

Thus, in order for $rs \equiv tu \pmod{I}$, we must have:

$$tb \in I, \ au \in I, \ ab \in I \ \text{ for all } a, b \in I, \text{for all } t, u \in R.$$

In summary, in order to define congruence modulo I in R (just like we defined congruence in $\mathbb{Z}$), we want I to satisfy the following properties:

1. $0_R \in I$;
2. $x \in I \Rightarrow -x \in I$;
3. $x, y \in I \Rightarrow x + y \in I$;
4. $x, y \in I, r \in R \Rightarrow xy \in I, xr \in I, rx \in I$.

- A subset $I \subseteq R$ satisfying the above properties is called an ideal in R.
- I is a subring of R and $\forall\, r \in R$ and $\forall\, a \in I$, we have $ar \in I$ and $ra \in I$.
- Alternatively, a nonempty subset I of R is an ideal provided:
  1. $a - b \in I \ \ \forall\, a, b \in I$;
  2. $ar \in I$ and $ra \in I \ \ \forall\, a \in I, r \in R$. These two conditions are sometimes referred to as *absorption properties*.

Example

- $2\mathbb{Z}$, $3\mathbb{Z}$, $4\mathbb{Z}$, $10\mathbb{Z}$, etc. are all ideals in $\mathbb{Z}$.
- $\{0\} \subset \mathbb{Z}$ is an ideal in $\mathbb{Z}$ (the *trivial* ideal).
- $\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal in $\mathbb{Z}$ (the *improper* ideal).

Theorem

Let R be a commutative ring with identity and let $c \in R$. The set

$$(c) \overset{def'n.}{=} \{rc \mid r \in R\} \quad \textit{(multiples of } c\textit{)}$$

is an ideal in R, called the principal ideal generated by c.

The proof is on the board.

Remarks:

- In any commutative ring with identity R, $(1_R) = R$.
- One can prove that every ideal in $\mathbb{Z}$ is principal. The proof uses the division algorithm.

The purpose of the next example is to show that some ideals are not principal.

Example

Consider $R = \mathbb{Z}[x]$ and

$$I = \{\text{all polynomials in } R \text{ with an even constant term}\}.$$

Note that $p(x) = x + 4 \in I, q(x) = x + 2 \in I$. By way of contradiction, assume I is principal, that is, $I = (f(x))$ for some $f(x) \in \mathbb{Z}[x]$ with an even constant term.
Then $p(x) - q(x) = 2 \in I$, so $2 = f(x)g(x)$. The latter implies that $f(x) = \pm 2$. But then $x \in I$ is not a multiple of $f(x)$. This contradition shows that I is not principal.