MATH H113: Honors Introduction to Abstract Algebra

2016-03-30

- Ex. 24 p. 249
- Principal, Maximal, Prime Ideals

For Friday, read App. I, Sect. 2 (Zorn's Lemma)

Excercise 24, p. 249

Let $\phi : R \to S$ be a ring homomorphism.

a. If J is an ideal in S then $\phi^{-1}(J)$ is an ideal in R **Proof**: By group theory, it's an additive subgroup. Let $r \in R$ and $a \in \phi^{-1}(J)$. Then $\phi(ar) = \phi(a)\phi(r) \in J$ because $\phi(a) \in J$ and $\phi(r) \in S$. $\therefore$ $ar \in \phi^{-1}(J)$. Similarly, $ra \in \phi^{-1}(J)$. $\therefore$ J is an ideal (of R).
As a corollary, if R is a *subring* of S and J is an ideal of S then $J \cap R$ is an ideal of R.
This follows from the excercise by letting $\phi : R \to S$ be the inclusion map ($\phi(r) = r\ \forall r \in R$).

b. If ϕ is surjective and I is an ideal in R then $\phi(I)$ is an ideal in S.
Proof: Let $s \in S$ and $b \in \phi(I)$. Write $s = \phi(r)$ and $b = \phi(a)$ with $r \in R$ and $a \in I$. Then $ar \in I$, so $bs = \phi(a)\phi(r) = \phi(ar) \in \phi(I)$ and similarly $sb \in \phi(I)$. $\therefore$ $\phi(I)$ is an ideal in S (also known from the fourth isomorphism theorem because $S = R/\ker\phi$.
Give an example in which ϕ is not surjective and $\phi(I)$ is not an ideal of S.
Let $\phi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map, and let $I = 2\mathbb{Z}$. Then I is an ideal in $\mathbb{Z}$ but not in $\mathbb{Q}$, because $2 \in 2\mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q}$ but $\frac{1}{2} \cdot 2 = 1 \notin 2\mathbb{Z}$.

Recall: If A and B are subsets of a ring R, then $AB = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{N} \text{ and } a_i \in A, b_i \in B\ \forall i = 1, \ldots, n\}$. Let R be a ring with 1.
Proposition: Let A be a susbset of R, and let $I = RAR = \{\sum_{i=1}^{n} r_i a_i r_i' : n \in \mathbb{N} \text{ and } a_i \in A, r_i, r_i' \in R\ \forall i\}$. Then:

a. I is an ideal of R
b. $I \supseteq A$
c. all ideals J of R that contain A also contain I

Proof:

a. I contains 0 (the empty sum), so $I \neq \emptyset$. If $x, y \in I$ then $x = \sum_{i=1}^{n} r_i a_i r_i', y = \sum_{i=n+1}^{m} r_i a_i r_i', x - y = r_1 a_1 r_1' + \ldots + r_n a_n r_n' + (-r_{n+1}) a_{n+1} r_{n+1}' + \ldots + (-r_m) a r_m' \in I$. $\therefore$ I is an additvie subgroup. Let $x \in I$ (as above) and $r \in R$. Then $rx = \sum_{i=1}^{n} (r r_i) a_i r_i' \in I$ and similarly $xr \in I$.
b. Let $a \in A$. Then $a = 1 \cdot a \cdot 1$, so $a \in I$.
c. If J is an ideal of R and $J \supseteq A$, then for any $x = \sum_{i=1}^{n} r_i a_i r_i' \in I$, $a_i \in A \implies a_i \in J \implies r_i a_i r_i' \in J$ (J is an ideal) $\implies \sum_{i=1}^{n} r_i a_i r_i' \in J$. $\therefore$ $J \supseteq I$. $\therefore$ I is the smallest ideal of R that contains A.

Corollary: I is the smallest ideal of R that contains A, and $I = \bigcap_{J \text{ an ideal of } R J \supseteq A} J$.
Proof: (c) $\implies I \subseteq \bigcap_{J \text{ an ideal of } R J \supseteq A} J$
I is among the ideals of J in the intersection (by (a) and (b)), so $I \supset \bigcap_{J \text{ an ideal of } R J \supseteq A} J$

Definition: Let A be a subset of R. Then:

a. $I = RAR$ is called *the ideal* (of R) *generated by* A, and is denoted by (A).
b. An ideal is *principal* if it can be generated by a one-element subset $\{a\}$ of R. This is denoted (a).
c. An ideal is *finitely generated* if it can be generated by a finite subset $\{a_1, \ldots, a_n\}$. This is denoted $(a_1, a_2, \ldots, a_n)$. (Similarly, the left ideal in R generated by A is RA, principal left ideal, finitely generated left ideal are defined. Same for right ideals AR).
If R is commutative, then left ideals = right ideals = two-sided ideals and $RA = AR = RAR = (A)$.

Examples:

1. In $\mathbb{Z}$, let's find all the ideals. If $I \subseteq \mathbb{Z}$ is an ideal, then it's a subgroup, equal to $m\mathbb{Z} = \{n \in \mathbb{Z} : m \mid n\}$, with $m \in \mathbb{N}$. All of these subgroups are ideals, because if $j \in \mathbb{Z}$ and $n \in m\mathbb{Z}$ then $m \mid nj$ so $nj \in m\mathbb{Z}$. (Incidentally, $m\mathbb{Z}$ is the principal ideal (m) $\forall m \in \mathbb{N}$.) So sometimes $\mathbb{Z}/m\mathbb{Z}$ is written $\mathbb{Z}/(m)$.
2. In any ring R (with $1 \neq 0$), principal ideal (0) is the ideal $\{0\}$, and the principal ideal (1) is the whole ring. This is called the *unit ideal.*

3. Non-principal ideals:
   Let $R = \mathbb{R}[x][y]$ (usually written $\mathbb{R}[x, y]$)
   Let $I = \ker \phi$ with $\phi : \mathbb{R}[x, y] \to \mathbb{R}$ given by taking the constant term.
   $I = \{f \in \mathbb{R}[x, y] : f(0, 0) = 0\} = \{f \in \mathbb{R}[x, y] : \text{constant term} = 0\}$. Then I is not principal. (Proof later) $I = (x, y)$.
   Another non-principal ideal: $\{f \in \mathbb{Z}[x] : \text{const. term is even}\}$ this equals $(2, x)$.

Proposition: Let I be an ideal of R. Then

a. $I = R \iff I$ contains a unit.
b. Assume that R is commuative: $(u) = R \iff u$ is a unit.
c. R is a field $\iff R$ is commutative and the only ideals of R are (0) and (1)

Proof:

a. See book
b. "$\Longleftarrow$" follows from (a) because $u \in (u)$
   "$\Longrightarrow$": $1 \in (u)$ so $1 = uv$ for some $v \in R$. $\therefore u$ is a unit (it has inverse v).
c. R is a field $\iff R$ has $1 \neq 0$ (already assumed), R is commutative, $R^\times = R \setminus \{0\}$. If R is a field and I is a nonzero ideal of R, then $I \supseteq (a)$ with $a \neq 0$. Then a is a unit, so $(a) = R$, $\therefore I = R$.
   "$\Longleftarrow$": need to show all nonzero $a \in R$ are units.
   $a \neq 0 \implies (a) \neq (0) \implies (a) = R \implies a \in R^\times$ by (b).

Definition: Let S be any ring (need not have 1). Then an ideal M in S is maximal if $M \neq S$ and the only ideals of S that contain M are M and S. Maximal among proper ($\neq S$) ideals of S.