Section 17: Subrings, Ideals and Quotient Rings

The first definition should not be unexpected:

Def: A nonempty subset S of a ring R is a *subring* of R if S is closed under addition, negatives (so it's an additive subgroup) and multiplication; in other words, S inherits operations from R that make it a ring in its own right.

Naturally, $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$. Also, $\mathbb{R}$ is a subring of $\mathbb{R}[x]$, which is a subring of $\mathbb{R}[x,y]$, etc. The additive subgroups $n\mathbb{Z}$ of $\mathbb{Z}$ are subrings of $\mathbb{Z}$ — the product of two multiples of n is another multiple of n. For the same reason, the subgroups $\langle d\rangle$ in the various $\mathbb{Z}_n$'s are subrings. Most of these latter subrings do not have unities. But we know that, in the ring $\mathbb{Z}_{24}$, 9 is an idempotent, as is $16 = 1 - 9$. In the subrings $\langle 9\rangle$ and $\langle 16\rangle$ of $\mathbb{Z}_{24}$, 9 and 16 respectively are unities. The subgroup $\langle 1/2\rangle$ of $\mathbb{Q}$ is not a subring of $\mathbb{Q}$ because it is not closed under multiplication: $(1/2)^2 = 1/4$ is not an integer multiple of $1/2$.

Of course the immediate next question is which subrings can be used to form factor rings, as normal subgroups allowed us to form factor groups. Because a ring is commutative as an additive group, normality is not a problem; so we are really asking when does multiplication of additive cosets $S + a$, done by multiplying their representatives, $(S + a)(S + b) = S + (ab)$, make sense? Again, it's a question of whether this operation is well-defined: If $S+a = S+c$ and $S+b = S+d$, what must be true about S so that we can be sure $S + (ab) = S + (cd)$? Using the definition of cosets: If $a-c, b-d \in S$, what must be true about S to assure that $ab-cd \in S$? We need to have the following element always end up in S:

$$ab - cd = ab - ad + ad - cd = a(b - d) + (a - c)d \ .$$

Because $b - d$ and $a - c$ can be any elements of S (and either one may be 0), and a, d can be any elements of R, the property required to assure that this element is in S, and hence that this multiplication of cosets is well-defined, is that, for all s in S and r in R, sr and rs are also in S. If this condition holds, then we don't need to assume separately that the product of two elements of S is again in S, so:

Def and Prop: An additive subgroup A of a ring R is an *ideal* in R if it "captures multiplication", i.e., for all a in A and r in R, $ar, ra \in R$. If A is an ideal in R, then the multiplication $(A+r)(A+s) = A + (rs)$ is well-defined on the additive factor group R/A and makes R/A a ring, called the *factor ring of R by A.*

Pf: Suppose A is an additive subgroup of R that captures multiplication, and that $A + r = A + u$ and $A + s = A + v$, i.e., $r - u, s - v \in A$. Then

$$rs - uv = rs - rv + rv - uv = r(s - v) + (r - u)v \in A \ ,$$

so $A + rs = A + uv$. Checking that this multiplication of cosets is associative and satisfies the distributive laws is easy.//

Some people also call R/A the quotient ring of R by A, but there is another meaning of quotient ring, so I will try to avoid using that term. Two obvious ideals in any ring R are R itself and the set $\{0_R\}$, which we also denote by 0 if there is no confusion. Of course a "ring homomorphism" is a function φ from one ring R to another ring T that respects both addition and multiplication. It is easy to check that the kernel of a ring homomorphism (still, the set of elements in R that are taken to 0_T by φ) is an ideal in R.

Exs: (1) Though $\mathbb{Z}$ is a subring of $\mathbb{Q}$, it is not an ideal: $1 \in \mathbb{Z}$, so if $\mathbb{Z}$ were to capture multiplication by elements of $\mathbb{Q}$, then all of $\mathbb{Q}$ would be in $\mathbb{Z}$. More generally, if a ring R with unity has an ideal A that contains one unit in R, then $A = R$. *(Pf:* If a in A has a multiplicative inverse a^{-1} in R, then for all r in R, $r = a(a^{-1}r) \in A$ because A captures multiplication.//)

(2) The subset

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

of the ring $M_{2\times 2}(\mathbb{R})$ is a subring, but it is not an ideal because if $a \neq 0$, then

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & d \\ a & b \end{pmatrix} \notin S \ .$$

General Exs: Let R be a commutative ring with unity. Then:

- for any subset X of R, the family of all finite sums $\sum_{i=1}^{n} r_i x_i$, where each r_i is in R and each x_i is in X, is an ideal, the smallest ideal that contains the set X. It is called "the ideal generated by X." In particular, if $X = \{x_1, x_2, \ldots, x_m\}$ is finite, then we can write this ideal in the form $Rx_1 + Rx_2 + \cdots + Rx_m$. If X is a single element, Rx is called a "principal ideal."

- for any subset X of R, the set of all elements r of R for which $rx = 0$ for every element x of X is an ideal of R, called the "annihilator of X" and denoted $\mathrm{ann}(X)$ or $0 : X$.

- (generalizing the last example) for any subset X of R and ideal A of R, $\{r \in R : rx \in A \,\forall x \in X\}$ is an ideal of R, denoted $A : X$.

- if A, B are ideals in R, then $A + B = \{a + b : a \in A,\ b \in B\}$ and $A \cap B$ are also ideals in R.

Ex: Recall from high school algebra that a real number r is the root of a polynomial $p(x)$ if and only if $x - r$ is a factor of $p(x)$. Addition and multiplication of polynomials are defined as they are so that evaluation of a polynomial by replacing the variable(s) with some real number(s) respects the operations, i.e., is a ring homomorphism. Thus, for r in $\mathbb{R}$

$$\begin{aligned} \ker(\varepsilon_r : \mathbb{R}[x] \to \mathbb{R} : p(x) \mapsto p(r)) &= \{p(x) \in \mathbb{R}[x] : p(r) = 0\} \\ &= \{p(x) \in \mathbb{R}[x] : x - r \text{ is a factor of } p(x)\} \\ &= \mathbb{R}[x](x - r) \ , \end{aligned}$$

a principal ideal in $\mathbb{R}[x]$.

If p is a prime integer, then a product of two integers is a multiple of p only if one of them is a multiple of p. This fact is the inspiration for the first term in the next definition.

Def and Prop: Let R be a commutative ring with unity, and A be a proper ideal in R.

(a) The ideal A is a *prime* ideal iff, for $r, s \in R$, $rs \in A$ only if $r \in A$ or $s \in A$, or equivalently iff R/A is an integral domain.

(b) The ideal A is a *maximal* ideal iff there is no ideal properly between A and R, or equivalently iff R/A is a field.

Pf of equivalences: (a) A is a prime ideal

$$\begin{aligned}
A \text{ is a prime ideal} &\iff (rs \in A \Rightarrow r \in A \text{ or } s \in A)\\
&\iff (A + rs = A \Rightarrow A + r = A \text{ or } A + s = A)\\
&\iff R/A \text{ has no nonzero zerodivisors}\\
&\iff R/A \text{ is an integral domain}
\end{aligned}$$

(b)

$$\begin{aligned}
A \text{ is a maximal ideal} &\iff \forall\, r \in R - A,\ A + Rr = R\\
&\iff \forall\, r \in R - A,\ 1 \in A + Rr\\
&\iff \forall\, r \in R - A,\ \exists\ a \in A,\ \ s \in R \text{ such that } 1 = a + rs\\
&\iff \forall\, r \in R - A,\ \exists\ s \in A \text{ such that } A + 1 = (A + r)(A + s)\\
&\iff \text{every nonzero element of } R/A \text{ is a unit}\\
&\iff R/A \text{ is a field}
\end{aligned}$$

Because a field is an integral domain, it follows that a maximal ideal is prime. In $\mathbb{Z}$, the ideals generated by prime integers are, in fact, maximal and not just prime, but $\{0\}$ is a prime ideal that is not maximal. A more interesting example is in $\mathbb{R}[x, y]$: $x\mathbb{R}[x, y]$ is a prime ideal that is not maximal — $\mathbb{R}[x, y]/x\mathbb{R}[x, y]$ is isomorphic (next section!) to $\mathbb{R}[y]$, which is an integral domain that is not a field. ($x\mathbb{R}[x, y] \subseteq x\mathbb{R}[x, y] + y\mathbb{R}[x, y]$, which $\underline{\text{is}}$ a maximal ideal.)