Dartmouth College

Mathematics 81

The following is a summary of useful concepts, conventions, and definitions that are intended to remind you (and perhaps refine your understanding) of material from Math 71. We shall review most of this on the first day of class.

1 Conventions and Definitions:

- **Rings:** All rings with be commutative with identity.
- **Ring homomorphisms:** If $\varphi : R \to S$ is a ring homomorphism, we know that $\varphi(1_R) = 1_S$ or is a zero divisor in S. In general, most of the rings we consider will be integral domains, so we shall simply assume $\varphi(1_R) = 1_S$ for all ring homomorphisms.
- **Ideals:** Let $I \subseteq R$ be an ideal of a ring (commutative with identity). Recall this simply means that I is an additive subgroup of R with the additional property that for all $r \in R$, $rI \subseteq I$ and $Ir \subseteq I$, though the second inclusion is redundant since R is commutative. The ideal is principal if there is an $a \in I$ so that $I = (a) = \{ra \mid r \in R\}$.
- **Prime/Maximal ideals:** Let R be a ring.
  - An ideal $P \subseteq R$ is a *prime* ideal if $P \neq R$ and if whenever $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$.
  - An ideal $M \subseteq R$ is a *maximal* ideal if $M \neq R$ and if whenever $I \subseteq R$ is an ideal with $M \subseteq I \subseteq R$, either $I = M$ or $I = R$.
- **Quotient Rings:** Let R be a ring and I an ideal in R. The set of cosets $R/I = \{r + I \mid r \in R\}$ is a ring under the usual operations: $(r + I) + (s + I) = (r + s) + I$, and $(r + I)(s + I) = rs + I$, with additive and multiplicative identities $0 + I$ and $1 + I$ respectively. Recall $r + I = s + I$ if and only if $r - s \in I$.

2 Basic facts, examples, and theorems:

- **Hierarchy:** $\{Euclidean\ Domains\} \subset \{PID's\} \subset \{UFD's\} \subset \{Integral\ Domains\}$.

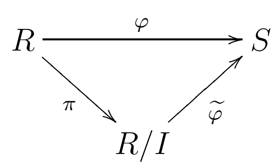
  Some standard examples:
  - Euclidean Domains: $\mathbb{Z}$; $k[x]$, k a field
  - PID's (not E.D.'s): $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$; recall $R[x]$ a PID implies R is a field, and hence $R[x]$ is a Euclidean domain (see 8.2 corollary 8)
  - UFD's (not PID's): $\mathbb{Z}[x]$, $k[x_1, \ldots, x_n]$, k a field, $n \geq 2$.

  - Integral Domains (not UFD's): $\mathbb{Z}[\sqrt{-5}]$.

- If P and M are proper ideals of a ring (commutative with 1) R, then
  - P is a prime ideal if and only if R/P is an integral domain.
  - M is a maximal ideal if and only if R/M is a field.

- Induced homomorphisms and isomorphisms (the "zeroth homomorphism" and first isomorphism theorems).

  Let $\varphi : R \to S$ be a ring homomorphism. Let I be an ideal of R with $I \subseteq ker(\varphi)$, and $\pi : R \to R/I$ the canonical projection ($\pi(a) = a + I$). Since $I \subseteq ker(\varphi)$, there is a well-defined induced homomorphism $\widetilde{\varphi} : R/I \to S$ making the diagram below commute: that is, $\widetilde{\varphi} \circ \pi = \varphi$. Because π is surjective, the images of φ and $\widetilde{\varphi}$ are the same; that $\widetilde{\varphi}$ exists is the content of the zeroth homomorphism theorem. Going further, $\widetilde{\varphi}$ is injective if and only if $I = ker(\varphi)$ in which case $R/ker(\varphi) \cong Im(\varphi)$, which is known as the first isomorphism theorem.



- Two useful theorems for characterizing quotient rings.
  - Let k be a field, and $f, g \in k[x]$ be relatively prime nonconstant polynomials. Then $k[x]/(fg) \cong k[x]/(f) \times k[x]/(g)$. This is a special case of the Chinese Remainder theorem (see Proposition 16 of section 9.5).
  - Let R be a ring, $I \subset R$ and ideal, and $f \in R[x]$. Let $\overline{f}$ denote the element of $(R/I)[x]$ obtained from f by reducing the coefficients of f mod I, i.e., if $f = a_0 + \cdots + a_n x^n$, $\overline{f} = (a_0 + I) + \cdots + (a_n + I)x^n$. Then

$$R[x]/(I, f) \cong (R/I)[x]/(\overline{f}).$$

    This is a refinement of Proposition 2 section 9.1.