Math 151 - Important Ideas and Examples about Polynomials, Commutative Rings, and Fields

1. Important definitions and results pertaining to polynomials:

   (a) A polynomial $p(x) \in F[x]$ is *irreducible over F* if it cannot be factored into polynomials in $F[x]$ of *strictly lower* degree. Note that

      i. Every non-zero polynomial over a field F can be factored as a constant polynomial times a polynomial of the same degree. For instance, $x^2 + 1 = 2 \cdot \left(\frac{1}{2}x^2 + \frac{1}{2}\right)$. In order to be considered reducible, it must have an "interesting" factorization in the sense described above.

      ii. It does not make sense to speak of a polynomial's irreducibility without specifying the field over which potential factorizations of the polynomial are being considered. For instance, $x^2 + 1$ is irreducible over $\mathbb{Q}$ and $\mathbb{R}$, but not over $\mathbb{C}$.

   (b) The *greatest common divisor* of $f(x)$, $g(x) \in F[x]$ is the unique **monic** polynomial $d(x) \in F[x]$ of largest degree which divides both $f(x)$ and $g(x)$. Again, discussion of gcd must be given in terms of a ground field F.

   (c) Rational Root Theorem. The polynomial must have **integer** coefficients. The theorem can find all possible rational roots.

   (d) Eisenstein's irreducibility criterion. The polynomial must have **integer** coefficients. The criterion can decide if such a polynomial is irreducible over $\mathbb{Q}$.

   (e) Being *reducible* over $\mathbb{Q}$ is **not the same** as *having roots* in $\mathbb{Q}$, unless the polynomial is of degree 3 or less! For example, $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ is certainly reducible over $\mathbb{Q}$, but it has no rational roots. The following statements hold for $f(x) \in \mathbb{Q}[x]$:

      - $f(x)$ has a root $c \in \mathbb{Q} \Rightarrow f(x)$ has a factor $x - c$ and is hence reducible over $\mathbb{Q}$
      - $f(x)$ is irreducible over $\mathbb{Q} \Rightarrow f(x)$ has no rational roots

      However, the converse statements are **false** (unless the polynomial has degree 3 or less):

      - $f(x)$ is reducible over $\mathbb{Q} \not\Rightarrow f(x)$ has a rational root
      - $f(x)$ has no roots in $\mathbb{Q} \not\Rightarrow f(x)$ is irreducible over $\mathbb{Q}$

2. A *field* is a set F equipped with two commutative binary operations, addition and multiplication, such that

   - $(F, +)$ is an abelian group under addition
   - Every non-zero element of F has a multiplicative inverse (in the notation of #4, below, $F^* = F \setminus \{0_F\}$), and $(F^*, \cdot)$ is an abelian group under multiplication
   - $0_F \neq 1_F$
   - The distributive law holds: $(a + b)c = ac + bc$ for all a, b, $c \in F$.

   Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ for p prime.

3. A *commutative ring* is just like a field, except that not every non-zero element need have a multiplicative inverse.

   Examples: $\mathbb{Z}$, $\mathbb{Z}_n$, $F[x]$ for F a field. Any field is a commutative ring.

4. An element of a ring R with a multiplicative inverse in R is called a *unit*. The set of units of R, denoted R^* or $R^\times$, is a multiplicative group under the multiplication of R.

   Examples: $\mathbb{Z}^* = \{\pm 1\} \cong \mathbb{Z}_2$, $\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n \mid (a, n) = 1\}$, $F[x]^* = F^* = F \setminus \{0_F\}$ for F a field.

5. A *zero-divisor* of a ring R is a (non-zero) element $r \in R$ such that $rs = 0$ for some non-zero $s \in R$. In other words, it is something you can multiply with a non-zero element and still get 0. A commutative ring *without* zero-divisors is called an *integral domain.*

   Examples of rings *with* zero-divisors: $\mathbb{Z}_n$ for n not prime, *e.g.* in $\mathbb{Z}_{24}$, $[6] \cdot [8] = [0]$. A non-commutative example: $\mathbb{M}_2(\mathbb{Q})$, *e.g.*

$$\begin{bmatrix} 2 & -2 \\ 2 & -2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

   Handy fact: Any element that is a *unit* of a ring will never be a zero-divisor. For instance, notice that all the matrices in the above example are not invertible. Exercise: Prove this handy fact.

   Examples of integral domains: any field (see #2, above), $\mathbb{Z}$, $F[x]$ where F is any field

6. A *ring homomorphism* is a function $\varphi\colon R \to S$, where R and S are rings, such that for all a, $b \in R$,

   - $\varphi(a + b) = \varphi(a) + \varphi(b)$
   - $\varphi(ab) = \varphi(a)\varphi(b)$

   Any ring homomorphism sends 0_R to 0_S. *However*, 1_R is **not** always sent to 1_S! For example, recall the ring homomorphism $\varphi\colon \mathbb{Z}_8 \to \mathbb{Z}_{12}$ defined by $\varphi([x]_8) = [9x]_{12}$ discussed in class.

   A *ring isomorphism* is a ring homomorphism as above which is also one-to-one and onto. If $\varphi\colon R \to S$ is a ring isomorphism, then we say R is *isomorphic* to S and we write $R \cong S$. In that case R and S are essentially the same ring in every way (they have the same addition and multiplication tables; if one is an integral domain, then so is the other, etc.). This is because any ring isomorphism sends units to units, zero-divisors to zero-divisors, and so on. Every property that an element in R has is sent to a corresponding element of S with that same property. In particular, 1_R *is* sent to 1_S.

7. An *ideal* I of a commutative ring R is a subset which is closed under $+$ and $-$ and under multiplication by things in R. We write $I \lhd R$.

   Important Ideas and Examples:

   (a) If $I \lhd R$ then $R/I := \{a + I \mid a \in R\}$ is a ring with operations

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (ab) + I.$$

   (b) If $\varphi\colon R \to S$ is a ring homomorphism, then $\ker\varphi \lhd R$ (note that $\ker\varphi$ is the set of things that get sent to 0_S under φ).

   (c) If $I \lhd R$ and $1_R \in I$, then $I = R$.
   Proof. $r \in R$, $1_R \in I$ implies $r \cdot 1_R = r \in I$ by definition of ideal. □

   (d) Corollary. A field has no interesting ideals.
   Proof. If $I \lhd F$ is non-zero, then let $a \neq 0$ in I. a is a unit since F is a field; hence $a^{-1} \in F$. Thus by definition of ideal, $a^{-1}a = 1 \in I$. By the above result, $I = F$. □

8. *First Isomorphism Theorem for Rings.* Also known as the Fundamental Homomorphism Theorem for rings. If $\varphi\colon R \to S$ is a ring homomorphism, then

$$R/\ker\varphi \cong \text{im}\varphi.$$

   Example: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, since $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(x) = [x]_n$ is an *onto* ring homomorphism (check yourself) whose kernel is $n\mathbb{Z}$ (check).