

Math 547, Exam 1 Information.

2/10/10, LC 303B, 10:10 - 11:00.

Exam 1 will be based on:

- Sections 5.1, 5.2, 5.3, 9.1;
- The corresponding assigned homework problems
(see <http://www.math.sc.edu/~boylan/SCCourses/547Sp10/547.html>)
At minimum, you need to understand how to do the homework problems.
- Lecture notes: 1/11 - 2/5.

Topic List (not necessarily comprehensive):

You will need to know: theorems, results, and definitions from class.

§5.1: Commutative rings; integral domains.

A set $(R, +, \times)$ is a **ring** if and only if it is an additive abelian group, a multiplicative monoid, and it is distributive. More precisely, the ring axioms for multiplication are:

- **closure:** For all $r, s \in R$, we have $rs \in R$.
- **associativity:** For all $r, s, t \in R$, we have $(rs)t = r(st)$.
- **identity:** The ring R has an identity, $1 \in R$: For all $r \in R$, we have $1 \cdot r = r = r \cdot 1$.

For R to be **distributive**, we must have: $\forall r, s, t \in R$, $r(s+t) = rs+rt$; $(r+s)t = rt+st$.

Note: Multiplication in a ring R :

- Need not have inverses.
- Need not be commutative.

Definition. A ring R is **commutative** if and only if its multiplication is commutative.

Example. The ring of $n \times n$ matrices with entries in a field or ring R , $\text{Mat}_{n \times n}(R)$ is not commutative.

Definition. An element $r \neq 0$ in R is a **zero divisor** if and only if $\exists s \neq 0$ in R for which $rs = 0 = sr$.

Definition. A ring R is an **integral domain** if and only if

- It is commutative.
- It has no zero divisors.

Notes:

1. Cancellation holds in an integral domain: $\forall a, b, c \in R$ with $a \neq 0$, we have $ab = ac \iff b = c$.
2. Let $n \in \mathbb{Z}$, not prime. Then \mathbb{Z}_n is not an integral domain.
3. $\text{Mat}_{n \times n}(R)$ is not an integral domain.

Definition. An element $r \in R$ is a **unit** if and only if $\exists s \in R$ with $rs = 1 = sr$.

Note: The set of units in R is denoted by R^\times ; it is a multiplicative group.

Definition. A ring R is a **division ring** if and only if $R^\times = R \setminus \{0\}$. I.e., all non-zero ring elements are units.

Example. The real quaternions, $\mathbb{H}(\mathbb{R})$ is a non-commutative division ring.

Definition. A ring R is a **field** if and only if it is a commutative division ring. In particular, a field has:

- $(R, +)$: abelian group.
- $(R^\times = R \setminus \{0\}, \times)$: abelian group
- R : distributive.

Example.

1. \mathbb{Q} , \mathbb{R} , and \mathbb{C} are fields; \mathbb{Z} is not.
2. Let p be prime. Then \mathbb{Z}_p is a finite field.

Facts:

1. If R is a field, then R is an integral domain. The converse is not true in general.
2. If R is a *finite* integral domain, then R is a field.

Definition. Let $(S, +, \times)$ be a ring. Then $R \subseteq S$ is a **subring** if and only if $(R, +, \times)$ is a ring and $1_R = 1_S$.

Proposition. Let S be a ring. Then $R \subseteq S$ is a subring if and only if the following hold:

- $(R, +)$ is closed and has inverses. (Hence, it is a subgroup).
- (R, \times) is closed.
- $1_R = 1_S \in R$.

Example. Let i have $i^2 = -1$. Then the **Gaussian integers** are a subring of \mathbb{C} given by $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. More generally, let $m \neq 1$ in \mathbb{Z} be square-free. Then $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ is a subring of \mathbb{C} .

Example. Let $m \neq 1$ in \mathbb{Z} be square-free, and let $m' = (1 + \sqrt{m})/2$. Then $\{a + bm' : a, b \in \mathbb{Z}\}$ is a subring if and only if $m \equiv 1 \pmod{4}$.

Example. Let p be prime. Then

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} : m \text{ and } n \in \mathbb{Z}, p \nmid n \right\}$$

is a subring of \mathbb{Q} .

§5.2, 5.3: 5.2: Ring homomorphisms; 5.3: Ideals and factor rings.

Definition. Let R and S be rings. Then $\phi : R \rightarrow S$ is a **ring homomorphism** if and only if:

- For all $a, b \in R$, we have $\phi(a + b) = \phi(a) + \phi(b)$.
- For all $a, b \in R$, we have $\phi(ab) = \phi(a)\phi(b)$.
- $\phi(1_R) = 1_S$.

Notes: If $\phi : R \rightarrow S$ is a ring homomorphism, then:

- By group theory, we have:
 - $\phi(0_R) = 0_S$.
 - $\forall n \in \mathbb{Z}$, and $\forall r \in R$, $\phi(nr) = n\phi(r)$.
- $\phi : R^\times \rightarrow S^\times$. I.e., ϕ maps units to units.
- $\phi(R)$ is a subring of S .

Definition. A ring homomorphism $\phi : R \rightarrow S$ is a **ring isomorphism** if and only if ϕ is one-to-one (injective) and onto (surjective).

Notes: Let $\phi : R \rightarrow S$ be a ring isomorphism. Then we have:

- $(R^\times, \times) \cong (S^\times, \times)$. I.e., the units are isomorphic as multiplicative groups.
- R is commutative if and only if S is commutative.
- R is a division ring if and only if S is a division ring.
- R is a field if and only if S is a field.

Definition. Let R be a ring. A subset $I \subseteq R$ is an **ideal** (we write $I \triangleleft R$ if and only if

1. I is non-empty.
2. $(I, +)$ is a subgroup.
3. $\forall r \in R$ and $\forall a \in I$, we have
 - $ra \in I$; as sets, we have $RI \subseteq I$.
 - $ar \in I$; as sets, we have $IR \subseteq I$.

Notes:

1. Let R be commutative. To show that I is an ideal, it suffices to show:
 - $\forall a, b \in I$, we have $a \pm b \in I$.
 - $\forall a \in I, \forall r \in R$, we have $ar \in I$ **or** $ra \in I$.
2. Analogy: an ideal I in a ring R plays the role of a normal subgroup N in a group G .

Ideal arithmetic: Let R be a commutative ring, and let $I, J \triangleleft R$.

1. $I \cap J \triangleleft R$.
2. $I + J = \{i + j : i \in I, j \in J\} \triangleleft R$.
3. $IJ = \{i_1j_1 + \cdots + i_nj_n : i_k \in I, j_k \in J, n \text{ is finite}\} \triangleleft R$.

Definition. Let $\phi : R \rightarrow S$ be a ring homomorphism. The **kernel** of ϕ is

$$\ker\phi = \{a \in R : \phi(a) = 0_S\}.$$

Proposition. Let $\phi : R \rightarrow S$ be a ring homomorphism. Then $\ker\phi \triangleleft R$.

Definition. Let R be a ring and let $I \triangleleft R$. The **factor ring** or **quotient ring** of R by I is $R/I = \{a+I : a \in R\}$ together with the operations of $+$ and \times defined $\forall a+I, b+I \in R/I$ by $(a+I) + (b+I) = a+b+I$, $(a+I) \cdot (b+I) = ab+I$.

Notes:

1. Multiplication is well-defined.
2. The zero element in R/I is $I = 0 + I$; the identity element is $1 + I$.

Proposition. Let R be a ring and let $I \triangleleft R$. Then the **natural projection** $\phi : R \rightarrow R/I$ defined for all $r \in R$ by $\phi(r) = r + I$ is an onto homomorphism with $\ker\phi = I$.

Theorem (Fundamental homomorphism theorem). Let $\phi : R \rightarrow S$ be a ring homomorphism. Then we have $R/\ker\phi \cong \phi(R)$.

Definition. Let R be a commutative ring, and let $a \in R$. Then the **principal ideal** generated by a is $(a) = \{ra : r \in R\} = Ra = aR$. Moreover, an ideal $I \triangleleft R$ is **principal** if and only if $\exists a \in R$ with $I = (a)$.

Notes:

1. A principal ideal (a) in a ring R is analogous to a cyclic subgroup $\langle a \rangle$ in a group G .
2. The improper ideals in a ring are principal: $(0) = \{0\}$; if $u \in R^\times$, then $(u) = R$. In particular, we have $(1) = R$.

Proposition. Let R be a commutative ring. Then R is a field if and only if R has no proper ideals.

Definition. Let R_1, \dots, R_n be commutative rings. Then the direct sum of the R_i 's is

$$R = R_1 \oplus \dots \oplus R_n = \{(r_1, \dots, r_n)\}.$$

It is a commutative ring with $+$ and \times defined $\forall (r_1, \dots, r_n), (r'_1, \dots, r'_n) \in R$ by

$$\begin{aligned} (r_1, \dots, r_n) + (r'_1, \dots, r'_n) &= (r_1 + r'_1, \dots, r_n + r'_n), \\ (r_1, \dots, r_n) \cdot (r'_1, \dots, r'_n) &= (r_1 r'_1, \dots, r_n r'_n). \end{aligned}$$

Note: The units in R are given as $R^\times = R_1^\times \times \dots \times R_n^\times$.

Definition. Let R be an integral domain. Then R has **characteristic** m if and only if m is the least positive integer such that $m \cdot 1_R = 0$. If no such m exists, then R has characteristic zero.

Example. Let p be prime. Then \mathbb{Z}_p has characteristic p . \mathbb{Z} has characteristic zero.

Proposition. Let R be an integral domain. Then either the characteristic of R is zero, or it is a prime, p .

Definition. Let R be commutative and let $I \triangleleft R$. Then $I \neq R$ is a **prime ideal** if and only if $\forall a, b \in R$, if we have $ab \in I$, then we must have either $a \in I$ or $b \in I$.

Definition. Let R be a commutative ring and let $I \triangleleft R$. Then $I \neq R$ is a **maximal ideal** of R if and only if $\forall J \triangleleft R$ with $I \subseteq J \subseteq R$, we have either $J = I$ or $J = R$.

Example. In the ring $\mathbb{Z}[i]$, the ideal $(3) = 3\mathbb{Z}[i]$ is maximal, but $(5) = 5\mathbb{Z}[i]$ is not. Let p be prime. Then $(p) \triangleleft \mathbb{Z}[i]$ is maximal if and only if $p \equiv 3 \pmod{4}$.

Theorem. Let R be a commutative ring and let $I \triangleleft R$.

1. R/I is a field if and only if I is maximal.
2. R/I is an integral domain if and only if I is prime.
3. If I is maximal, then I is prime.

Note: The converse of part (3) is true in some situations, but not in general.

Example. In the ring $\mathbb{Z}[i]$, (3) is maximal, so $\mathbb{Z}[i]/(3) = \{a + bi + (3) : 0 \leq a, b \leq 2\}$ is a field of size 9; (5) is not maximal, so $\mathbb{Z}[i]/(5) = \{a + bi + (5) : 0 \leq a, b \leq 4\} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Definition. A ring R is a **principal ideal domain (PID)** if and only if

1. It is an integral domain.
2. Every ideal in R is principal.

Theorem. Let R be a PID. Then $I \triangleleft R$ is maximal if and only if it is prime.

Example. \mathbb{Z} is a PID. The maximal (hence prime) ideals in \mathbb{Z} are: $\{(p) = p\mathbb{Z} : p \text{ is prime}\}$.

§9.1: Principal ideal domains.

Definition. A ring R is a **Euclidean ring** if and only if it is an integral domain for which there exists a **norm function** $\delta : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ with the following properties:

1. $\forall a, b \neq 0$ in R , we have $\delta(a) \leq \delta(ab)$
2. $\exists q, r \in R$ such that $a = bq + r$ and either $\delta(a) < \delta(b)$ or $r = 0$.

Example. \mathbb{Z} is Euclidean with norm function $|\cdot| : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$.

Example. The ring $\mathbb{Z}[i]$ is Euclidean with norm function given in terms of complex conjugation in \mathbb{C} . The norm function is $\delta : a + bi \mapsto (a + bi) \cdot (a - bi) = a^2 + b^2$.

Theorem. Let R be a Euclidean ring. Then R is a PID. The converse is not true in general.

Example. The ring $\mathbb{Z}[i]$ is Euclidean; therefore, it is a PID. Hence, it must also be true that the prime and maximal ideals in $\mathbb{Z}[i]$ agree.

Definition. Let R be a commutative ring. Let $a, b \in R$ with $a \neq 0$. Then a **divides** b ($a \mid b$) if and only if $\exists c \in R$ with $b = ac$.

Notes:

- $u \in R^\times \iff (u) = R$.
- $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$.
- $a \mid b$ and $b \mid a \iff (a) = (b)$.

Definition. Elements a and $b \in R$ are **associates** ($a \sim b$) if and only if $\exists u \in R^\times$ with $b = ua$.

Notes:

- The relation \sim is an equivalence relation on R .
- $a \sim b \implies (a) = (b)$.
- Let R be an integral domain. Then $a \sim b \iff (a) = (b)$.

Definition. Let R be a commutative ring. Then $d \neq 0$ in R is the **greatest common divisor** (gcd) of $\{a_1, \dots, a_n\} \subseteq R$ if and only if the following are true:

1. $\forall i, d \mid a_i$.
2. Suppose that $\exists c \in R$ such that $\forall i, c \mid a_i$. Then we have $c \mid d$.

Notes:

- The gcd of $\{a_1, \dots, a_n\}$ may not exist in R .
- If a gcd of $\{a_1, \dots, a_n\}$ exists in R it is well-defined (unique) up to multiplication by units.

Proposition. Let R be a PID, and let $a, b \neq 0$ in R . Then we have:

1. gcd(a, b) exists in R ; it is unique up to multiplication by units.
2. If $d = \text{gcd}(a, b)$, then $\exists s, t \in R$ with $d = as + bt$.

Notes: Let R be a PID. Then the following rules of ideal arithmetic hold:

- $(a) + (b) = (\text{gcd}(a, b))$.
- $(a) \cap (b) = (\text{lcm}(a, b))$.
- $(a)(b) = (ab)$.

Definition. Let R be an integral domain. Then $q \in R$ is **irreducible** if and only if

- q is a non-zero, non-unit.
- If $\exists a, b \in R$ with $q = ab$, then one of a, b is a unit, and the other is associated to q .

Definition. Let R be an integral domain. Then p is **prime** if and only if

- p is a non-zero, non-unit.
- If $\exists a, b \in R$ with $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Theorem. *Let R be an integral domain.*

1. *$p \in R$ is prime if and only if $(p) = pR \triangleleft R$ is a prime ideal.*
2. *$c \in R$ is irreducible if and only if $(c) = cR \triangleleft R$ is maximal in the set of all principal ideals in R .*
3. *Let $p \in R$ be prime. Then p is irreducible.*

Note: The converse of part (3) is not true in general.

Proposition. *Let R be a PID, and let $p \in R$. Then p is irreducible if and only if p is prime.*