MA 521
Test 3 Study Guide
Rings

Zachary D. Clawson

November 23, 2010

1 Definition of a Ring

Gaussian integers. Ring: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

Smallest subring of $\mathbb{C}$ containing $\alpha \in \mathbb{C}$ is denoted $\mathbb{Z}[\alpha] = \{a_n\alpha^n + \cdots + a_1\alpha + a_0 \mid a_i \in \mathbb{Z}\}$ and called the subring *generated by* α

Algebraic complex number. $\alpha \in \mathbb{C}$ is *algebraic* if it is a root of a polynomial with integer coefficients

Transcendental number. If $\alpha \in \mathbb{C}$ is not algebraic then it is *transcendental*

Ring. A ring R is a set with the two laws of composition $+$ and $\times$, called addition and multiplication, which satisfy these axioms:

1. With the law of composition, $+$, R is an abelian group, with identity denoted by 0. This abelian group is denoted by R^+
2. Multiplication is associative and has an identity denoted by 1
3. *Distributive laws:* For all $a, b, c \in R$,

$$(a + b)c = ac + bc \quad \text{and} \quad c(a + b) = ca + cb$$

Subring. Subset of a ring closed under operations of addition, subtraction, multiplication, and contains 1.

Assume all rings are commutative unless otherwise states. I.e. $ab = ba$ for all $a, b \in R$.

Polynomial rings. $R[x] = \{a_nx^n + \cdots + a_1x + a_0 \mid a_i \in R\}$ for all $n \in \mathbb{N}_0$ where R is a ring.

Unit. Elements with multiplicative inverses are called *units*.

2 Formal Construction of Integers and Polynomials

Polynomial multiplication. $f(x)g(x) = \sum_{i,j} a_ib_jx^{i+j} = \sum_k p_kx^k$ with $p_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 = \sum_{i+j=k} a_ib_j$.

Monomial. Formal product of variables of the form $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$

Polynomial. Finite linear combination of monomials

3 Homomorphisms and Ideals

Homomorphism. A homomorphism $\varphi : R \to R'$ where R, R' are rings is a map such that

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1_R) = 1_{R'}$$

for all $a, b \in R$. An *isomorphism* of rings is a bijective homomorphism. If there is an isomorphism $R \to R'$, the two rings are said to be *isomorphic*.

Examples. Evaluation of polynomials at a value is a homomorphism. That is, $\mathbb{R}[x] \to \mathbb{C}$ defined by $p(x) \mapsto p(c)$ for some $c \in \mathbb{C}$.

Proposition. Substitution principle: Let $\varphi : R \to R'$ be a ring homomorphism.

1. Given an element $\alpha \in R'$, there is a unique homomorphism $\Phi : R[x] \to R'$ which agrees with the map φ on constant polynomials and which sends $x \mapsto \alpha$.
2. More generally, given elements $\alpha_1, \ldots, \alpha_n \in R'$, there is a unique homomorphism $\Phi : R[x_1, \ldots, x_n] \to R'$ from the polynomial ring in n variables to R', which agrees with φ on constant polynomials and which sends $x_v \mapsto \alpha_v$ for $v = 1, \ldots, n$.

Example. Map extending $\mathbb{Z}[x] \to \mathbb{F}_p[x]$ where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a field (p is prime). This map has $f(x) = a_n x^n + \cdots + a_0 \mapsto \bar{a}_n x^n + \cdots + \bar{a}_0 = \bar{f}(x)$ where $\bar{a}_i = a_i \bmod p$.

Remark. $R[x, y] \cong R[x][y]$.

Proposition. Let $\mathcal{R}$ denote the continuous real-valued functions on $\mathbb{R}^n$. The map $\varphi : \mathbb{R}[x_1, \ldots, x_n] \to \mathcal{R}$ sending a polynomial to its associated polynomial function is an injective homomorphism.

Proposition. There is exactly one homomorphism $\varphi : \mathbb{Z} \to R$ from the ring of integers to an arbitrary ring R. It is the map defined by $\varphi(n) = \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}$ if $n > 0$ and $\varphi(-n) = -\varphi(n)$.

Kernal. Let $\varphi : R \to R'$ where R, R' are rings. Then $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$ is a subgroup of R^+ but not a subring of R as $1_R \notin \ker\varphi$. The kernal is closed under addition and muliplication. Further, it is closed under multiplication by the whole group: $a \in \ker\varphi$ and $r \in R \implies ra \in \ker\varphi$. If $\ker\varphi = R$ then $\varphi \equiv 0 \implies R' = \{0\}$ since then $1 = 0$.

Ideal. A subset of a ring R with the properties:

1. I subgroup of R^+
2. $a \in I$ and $r \in R \implies ra \in I$

Principal ideal. The principal ideal generated by a is the set of multiplies of a particular element $a \in R$. That is, the elements divisible by a. We notate it as $(a) = aR = Ra = \{ra \mid r \in R\}$.

Example. Consider $\varphi : \mathbb{R}[x] \to \mathbb{R}$ where $\varphi(f(x)) = f(2)$. Then $\ker\varphi = \{f(x) \in \mathbb{R}[x] \mid f(2) = 0\} = (x-2) = (x-2)\mathbb{R}[x]$.

Remark. The zero ideal (0) and the unit ideal $(1) = R$ are always ideals in a ring R.

Characteristics. The *characteristic* of a ring R is the nonnegative integer n which generated the kernal of the homomorphism $\varphi : \mathbb{Z} \to R$. That is, n is the smallest positive integer such that $n \times 1_R = 0$ or if $\ker\varphi = \{0\}$ then $n = 0$.

Remark. If $\mathbb{Z}$ is a subring of R, then $\text{char} R = 0$.

4 Quotient Rings and Relations in a Ring

Cosets. Let I be an ideal in R. The cosets of the additive subgroup I^+ of R^+ are the subsets $a+I$, $a \in R$.

Theorem. Let I be an ideal of a ring R.

1. There is a unique ring structure on the set of cosets $\bar{R} = R/I$ such that the canonical map $\pi : R \to \bar{R}$ sending $a \mapsto \bar{a} = a + I$ is a homomorphism.
2. The kernal of π is I.

Proposition. *Mapping property of the quotient rings:* Let $f : R \to R'$ be a ring homomorphism with kernal I and let J be an ideal which is contained in I. Denote the residue ring R/J by $\bar{R}$.

1. There is a unique homomorphism $\bar{f} : \bar{R} \to R'$ such that $\bar{f}\pi = f$:

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \pi \searrow & & \nearrow \bar{f} \\ & \bar{R} = R/J & \end{array}$$

2. *First isomorphism theorem:* If $J = I$, then $\bar{f}$ maps $\bar{R}$ isomorphically to the image of f.

Proposition. *Correspondence theorem:* Let $\bar{R} = R/J$, and let π denote the canonical map $R \to \bar{R}$.

1. There is a bijective correspondence between the set of ideals of R which contain J and the set of all ideals of $\bar{R}$, given by
$$I \mapsto \pi(I) \quad \text{and} \quad \pi^{-1}(I) \mapsto \bar{I}$$
2. If $I \subseteq R$ corresponds to $\bar{I} \subseteq \bar{R}$, then R/I and $\bar{R}/\bar{I}$ are isomorphic rings.

5 Adjunction of Elements