School of Mathematical Sciences
PURE MTH 3007
Groups and Rings III, Semester 1, 2009

Week 10 Summary

We are about a lecture ahead of where I was planning to be so I will start recalibrating the lecture plan.

On Friday of Week 9 we covered:

10.3. **Polynomial functions.** Let R be a ring and $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ a polynomial over R. Then the function $\overline{f} : R \to R$ given by $\overline{f}(r) = a_0 + a_1r + a_2r^2 + \cdots$ is called the *polynomial function* associated to f.

The set $\mathcal{P}(R)$ of all polynomial functions over R is a ring under the operations $(\overline{f} + \overline{g})(r) = \overline{f}(r) + \overline{g}(r)$ and $(\overline{f}\overline{g})(r) = \overline{f}(r).\overline{g}(r)$. It is then easy to show that

$$\overline{f} + \overline{g} = \overline{f+g}, \quad \overline{f}\,\overline{g} = \overline{fg}.$$

If R is a commutative ring with identity then so is $\mathcal{P}(R)$, but note that $\mathcal{P}(R)$ is not necessarily isomorphic to $R[x]$.

10.3.1. *Zeros of polynomials.* Let F be a field.

Definition 10.3. An element $a \in F$ is a *zero* of $f(x) \in F[x]$ if $\overline{f}(a) = 0$.

Theorem 10.4 (Factor Theorem)**.** *The element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a \mid f(x)$.*

Corollary 10.5. *A polynomial of degree n over a field F has at most n zeros in F.*

Definition 10.6. A non-constant polynomial $f(x) \in F[x]$ is *irreducible over F* if

$f(x) \neq g(x)h(x)$ for any polynomials $g(x), h(x)$ of degree less than $f(x)$.

Week 10 — Lecture 25 — Tuesday 19th May.

---

11. Ideals

11.1. **Introduction.**

Definition 11.1. A subring I of a ring R is called an *ideal* of R if for all $r \in R$ and $i \in I$ we have $ir \in I$ and $ri \in I$.

11.2. **The Factor Ring.**

Theorem 11.2 (The Factor Ring)**.** *Let I be an ideal of the ring R. Then the set R/I of all cosets of I in R is a ring under the operations*

$$\begin{aligned}(r+I) + (s+I) &= (r+s) + I \\ (r+I).(s+I) &= rs + I.\end{aligned}$$

If R is a commutative ring, or a ring with identity, then so is R/I.

Lemma 11.3. *Let $\phi : R \to S$ be a ring homomorphism. Then* $\ker \phi$ *is an ideal of R.*

Theorem 11.4 (Homomorphism Theorem)**.** *If $\phi : R \to S$ is a ring homomorphism then*

$$R/ker\,\phi \simeq \phi(R).$$

Lemma 11.5. *If I and J are ideals of R then so are $I + J$ and $I \cap J$.*

Theorem 11.6 (Isomorphism Theorem)**.**

(i) *Let I be an ideal of R. Then there is a $1-1$ correspondence between subrings S of R containing I and subrings S/I of R/I. Here S is an ideal of R if and only if S/I is an ideal of R/I.*
(ii) *Let $I \subset J \subset R$ with I and J ideals of R. Then*

$$R/J \simeq (R/I)/(J/I).$$

(iii) *Let I and J be ideals of R. Then*

$$(I+J)/J \simeq I/(I \cap J).$$

Week 10 — Lecture 26 — Friday 22nd May.

11.3. **Ideals in commutative rings with identity.** Let R be a commutative ring with identity.

Definition 11.7. An ideal of the form $\langle a \rangle = \{ar \mid r \in R\}$ is called a *principal* ideal of R.

An ideal M of R is called a *maximal* ideal if there is no ideal I of R such that $M \subset I \subset R$.

Theorem 11.8. *Let R be a commutative ring with identity. Then M is a maximal ideal of R if and only if R/M is a field.*

12. Factorization in Integral Domains

12.1. **Irreducibles and associates.**

Definition 12.1. An element c of an integral domain, not zero or a unit, is called *irreducible* if, whenever $c = df$, one of d or f is a unit.

Elements c and d are called *associates* if $c = du$ for a unit u.

12.2. **Euclidean domains.**

Definition 12.2. A *Euclidean domain* is an integral domain D together with a function $\delta : D^* \to \mathbb{N}$ satisfying

(i) $\delta(a) \le \delta(ab)$ for all non-zero $a, b \in D$
(ii) for all $a, b \in D$, $b \ne 0$ there exist $q, r \in D$ such that

$$a = bq + r$$

with either $r = 0$ or $\delta(r) < \delta(b)$.

The function δ is called a *Euclidean valuation*.

Examples:

(1) $\mathbb{Z}$ with $\delta(n) = |n|$.
(2) $F[x]$ with $\delta(f(x)) = \deg f(x)$, where F is a field.