MATH 250A LECTURE RECAPS (RINGS)

PATRICK OARE

1. 9/19 (Rings)

- A **ring** is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations on R, **addition** and **multiplication**, such that:
  (1) $(R, +)$ is an abelian group with identity 0 and inverse $-a$.
  (2) $\cdot$ associates.
  (3) $\cdot$ distributes over $+$, i.e. $a(b+c) = ab + ac$.

  If multiplication has an identity 1, then we say the ring has **unity**. If multiplication commutes, we say the ring is **commutative**.
- Analogy between groups and rings:

Groups	Rings
Set S	Vector space, basis S
Symmetric Group S_n	$M_{m\times n}(K)$
Group Actions	Actions of rings on K_n
Disjoint union, direct product	Vector space addition, tensor product
Normal subgroups	Ideals

- **Burnside Ring**: TODO
- **Group Ring**: The group ring is defined on the base set $R[G]$, where $R[G]$ is the set of all formal R-linear combinations of the elements of the group G. Addition is defined componentwise, and we define:

$$(\sum_{x\in G} a_x x) \cdot (\sum_{y\in G} b_y y) := \sum_{x,y\in G} a_x b_y xy = \sum_{z\in G}(\sum_{xy=z} a_x b_y) z$$

  The multiplication is a convolution of ring elements. Furthermore, we can define the obvious scalar multiplication on elements of $R[G]$, and so make it into a R-module, and hence an R-algebra.

  An example is to take $G := V_4$, the Klein 4-group. If we form the group ring $\mathbb{C}[G]$, we have a 4 dimensional vector space over $\mathbb{C}$. It also forms an algebra as we can internally multiply elements. Let $4e_1 := 1 + a + b + c$, $4e_2 := 1 + a - b - c$, $4e_3 = 1 - a + b - c$, and $4e_4 := 1 - a - b + c$. Then $e_i e_j = \delta_{ij}$, so these four elements are **idempotents** ($e^2 = e$, $e \in Z(R)$). If e is an idempotent in R, then $R = eR \bigoplus (1-e)R$, and if it splits as a product then $(1, 0)$ is an idempotent, so a ring splits as a product iff it has an idempotent.

- **Ideals** are subsets of R that function as normal subgroups; we can quotient by them. An ideal is:
  (1) A subgroup under $+$.
  (2) Closed under $\cdot$ from **all** elements in the ring.

  We may quotient rings additively by ideals and have a well defined addition and multiplication. Ideals correspond bijectively with the kernels of ring homomorphisms. If $S \subset R$ is any subset, then we can form the smallest ideal containing S:
$$(S) = \{\sum_{i=1}^{n} r_i s_i t_i \in R : s_i \in S, r_i, t_i \in R\}$$
- **Generator and Relations**:

  Form the free ring on S. For commutative, we first form the free commutative monoid on S. If $S = \{x, y, z\}$, then the free commutative monoid on S is the set $\{x^{n_1} y^{n_2} z^{n_3} : n_i \in \mathbb{Z}\}$. The free commutative ring is:
$$\{\sum_{a,b,c \geq 0} n_{abc} x^a y^b z^c\}$$
  where $n_{abc} \in R$. For non-commutative rings, just take all words on the set to be the free monoid, and the free ring is the group ring of this free monoid.
- Construction of coproduct/pushout in *Rng*. We can construct the coproduct as follows: Assume A, B are disjoint. Form the free ring on $A \times B$, $F = F(A \cup B)$. Quotient out by an ideal to force the map from A to F to be a homomorphism– quotient by the smallest ideal with $f(a+b) - f(a) - f(b)$, $f(ab) - f(a) - f(b)$ for all a, b in the ring. Do the same with all necessary relations, and then you have a coproduct.

2. 9/26 (Unique Factorization)

- **Domains**: A **domain** is a ring with no nonzero zero divisors. An **integral domain** is a commutative domain with $0 \neq 1$. A **Euclidean Domain** is an integral domain R with a norm $|\cdot| : R \to \mathbb{Z}_{\geq 0}$ such that for a and $b \neq 0$, there are $r, q \in R$ such that $a = bq + r$ with $|r| < |b|$. A **Principal Ideal Domain** is an integral domain in which every ideal is **principal**, i.e. generated by one element (a). A **Unique Factorization Domain** is an integral domain where every element has a unique (up to unit and permutation) factorization into irreducible elements.

  $\mathbb{Z}$ is a PID because the GCD exists.
- Every Euclidean Domain is a PID.

  Sketch of proof: Take the element a of smallest norm (need not be unique) in the ideal I. Then $I = (a)$, as you can Euclidean divide by a with a remainder that must be 0.

  The converse is not true: A PID that is not Euclidean is $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$
- **Irreducible elements**: Let $a \in R$. a is **irreducible** if $a \neq 0$ or a unit and $a = bc \implies b \in R^*$ or $c \in R^*$. a is **prime** if $a|bc \implies a|b$ or $a|c$.

- Every PID is a UFD.

  Sketch of proof: Given $a \in R$, set $a = bc$ with c irreducible dividing a. If b is irreducible, stop. If not, continue on forever. This cannot last forever because we have an ascending chain of ideals. However, note that a PID is **Noetherian**, i.e. there is no infinite strictly increasing chain of ideals $I_1 \subset I_2 \subset ....$ To show uniqueness, we show that **in a PID, irreducibles are prime**. You should know how to do this proof. To complete the proof, we can essentially pair off p_i's and p_j's because they are prime.
- **Gaussian Integers**:

  The Gaussian integers $\mathbb{Z}[i]$ are Euclidean; they are a square lattice in $\mathbb{C}$. If we use the norm $|a+bi| := a^2+b^2$, then the problem is equivalent to finding $r, q \in \mathbb{Z}[i]$ with $\frac{a}{b} = q + \frac{r}{b}$ with $|\frac{r}{b}| < 1$. This holds because the unit balls centered on the lattice cover $\mathbb{C}$.

  We also have unique factorization in $\mathbb{Z}[i]$. If $a+bi$ is prime in $\mathbb{Z}[i]$, then $(a+bi)(a-bi) = a^2+b^2$ is prime in $\mathbb{Z}$. This is not an iff; 2 and 5 are not prime in the Gaussian integers, but 3 is. The factorizations in $\mathbb{Z}[i]$ are the same as the number of ways we can write the number as a^2+b^2.

  The smallest quadratic integer subring of $\mathbb{C}$ that is not Euclidean is $\mathbb{Z}[\sqrt{-3}]$, and this is not a UFD, as $2 \times 2 = (1+\sqrt{3}i)(1-\sqrt{3}i)$. 2 is an irreducible because $|2| = 2$ cannot be divided. The only units are ± 1. The ideals of this ring are $z \mapsto az$, which multiplies $|z|$ by $|a|$ and rotates z by $arg(a)$. Non-principal ideals are diamond lattices, not rectangular lattices.
- UFDs need not be PIDs: $\mathbb{Z}[x]$ is a UFD, and $(2, x) \subset \mathbb{Z}[x]$ is a non-principal ideal.
- Any prime $p \in \mathbb{Z}$, $p > 0$, $p \equiv 1 \mod 4$ is the sum of 2 squares.

  Let $p \equiv 1 \mod 4$. Then $G := (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, and $p-1 = 4n$ for $n \in \mathbb{Z}$. G has an element of order 2, which is -1. Let g be a generator for G, so $g^{4n} = 1$. Then $g^{2n} = -1$ as it has order 2 and -1 is the unique element of order 2, so -1 is a square mod p, thus $-1 = a^2 - kp \implies kp = a^2+1$. Viewing this in $R := \mathbb{Z}[i]$, $kp = (a+i)(a-i)$ in R. These are irreducibles, so p does not divide either of them, and thus p is not prime in $\mathbb{Z}[i]$, so $p = (x+iy)(x-iy) \implies p = x^2+y^2$.

  https://math.stackexchange.com/questions/594/how-do-you-prove-that-a-prime-is-the-sum-of-two-squares-iff-it-is-congruent-to-1

3. 9/28 (Localization)

Let R be a commutative ring.

- **Types of Ideals**: Let I be an ideal of R. I is **maximal** if R/I is a field, and **prime** if R/I is an integral domain.

  We see that maximal ideals must be prime. An equivalent definition of prime is $ab \in I \implies a \in I$ or $b \in I$. If F is a field, then $F/\{0\}$ is a field, so $\{0\}$ is a maximal ideal. Thus F has no proper nontrivial ideals.

  Prime ideals differ from maximal ideals (in a lot of common examples, prime ideals are just all maximal ideals plus the trivial ideal) significantly in $\mathbb{C}[x, y]$. The maximal ideals are $(x-a, y-b)$, while the prime ideals are these ideals and also ideals of the form (f) for any irreducible f. These irreducible (f)'s correspond to irreducible curves in the plane.

Zorn's Lemma: We need some definitions. A **partially ordered set** S is a set S with a **partial order** $\leq$ such that if $a \leq b$ and $b \leq c$, then $a \leq c$. It is not necessary for $a \leq b$ or $b \leq a$ for each $a, b \in S$ for a poset (i.e. set inclusion). A set is **totally ordered** if it is partially ordered and for all $a, b \in S$, either $a \leq b$ or $b \leq a$. The lemma states that if a set S has:

(1) A partial order $\leq$.
(2) $S \neq \emptyset$.
(3) The property that given any totally ordered subset $T \subset S$, then T has an upper bound.

Then S has a **maximal element**, i.e. an element $a \in S$ such that no element $b \in S$ satisfies $a < b$.

- Every proper ideal is contained within a maximal ideal.

  Reasoning: Let I be an ideal. The set of ideals containing I under inclusion form a poset that satisfies the properties of Zorn's Lemma. Then, this set has a maximal element, which is a maximal ideal.
- The **nilradical** of R is the set of all nilpotent elements of R, i.e. it is

$$\eta(R) := \{x \in R : x^n = 0, n \in \mathbb{N}\}$$

  Then the nilradical is the intersection of all the prime ideals of R, which we will denote by P.

  For the forward containment, $x^n = 0 \in p$ for any prime ideal p. As p is prime, we can easily induct and show $x \in p$. Thus, we have $\eta(R) \subset P$. Conversely, we wish to show $P \subset \eta(R)$, or that $\eta(R)^C \subset P^C$. Suppose x is not nilpotent. We want to find a prime ideal not containing x. Let $M := \{1, x, x^2, ...\}$ ($0 \notin M$ as x is not nilpotent). Let S be the set of ideals disjoint from M. Then S is a poset by $\subset$, and $S \neq \emptyset$ as $\{0\} \in S$. As before, any totally ordered subset has an upper bound, so S has a maximal element I. Suppose $a, b \in R$ are not contained in I. Then $I \subset (I, a)$ is strict, and so $(I, a) \cap M \neq \emptyset$ as I is maximal with respect to this. So, $x^n = i_1 + sa$. Similar for (I, b), so $x^m = i_2 + tb$. Then $x^{m+n} = i_1 i_2 + i_2 tb + i_2 sa + stab$, so (I, ab) contains x^{n+m}. But then $a \notin I$ and $b \notin I \implies ab \notin I$, so I is prime, and $x \notin M$, so we are done.
- **Localization**: Let $S \subset R$ be a multiplicative subset (so S is closed under $\cdot$ and $1 \in S$) not containing 0. We may **localize** the ring by S and construct a universal ring R may be embedded in, in which all the elements of S are units. We define an equivalence relation $\equiv$ on $R \times S$ by:

$$(r_1, s_1) \equiv (r_2, s_2) \iff \exists t \in S s.t. t(r_1 s_2 - r_2 s_1) = 0$$

  We may quotient by this equivalence relation, and we denote:

$$R[S^{-1}] := R \times S / \equiv$$

We denote the cosets of $\equiv$ by fractions, so $\frac{r}{s} := (r,s)/\equiv$. We make $R[S^{-1}]$ into a ring by defining:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

and

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

Then $R[S^{-1}]$ is a ring, and we have a canonical homomorphism:

$$\iota : r \mapsto \frac{r}{1}$$

This is an embedding iff S has no zero divisors. Furthermore, the images of all elements of S are invertible in this new ring. $R[S^{-1}]$ has the universal property that if X is any ring with a homomorphism $\phi : R \to X$ that sends all elements of S to units in x, then ϕ factors uniquely through $R[S^{-1}]$, i.e. $\exists! \Phi : R[S^{-1}] \to X$ such that

$$\phi = \Phi \circ \iota$$

- Localizing is a way to study specific prime ideals of a ring. We can think of it as "getting rid of unnecessary information" that comes from the elements that we do not wish to study. For example, take $R = \mathbb{Z}$, where we are interested in 2. For S to be multiplicatively closed, we take $S = p^C$ where p is a prime ideal. So, we take $p = (2)$ and localize by inverting all elements of $\mathbb{Z}$ not in (2). We get a ring:

$$\mathbb{Z}_{(2)} = \{\frac{a}{b} : a \in \mathbb{Z}, b \text{ odd}\}$$

The units of this rings are all rationals $\frac{a}{b}$ with b odd. We can see that 2 is a prime element of this ring, and any element can be written as 2^n times a unit. Thus, this ring is a UFD with one irreducible element 2. We see that localizing by a prime ideal kills off the other primes in the ring that we are not interested in.