LECTURE 7 : ~~FIELD OF FRACTIONS~~ DOMAIN EXPANSION!

Example 4.1.36. *Define* $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. *This is not a finite integral domain! Yet,*

$$(a + b\sqrt{2})(x + y\sqrt{2}) = ax + 2by + (ay + bx)\sqrt{2}$$

and of course $(a + b\sqrt{2}) + (x + y\sqrt{2}) = (a + x) + (b + y)\sqrt{2}$ *hence* $\mathbb{Q}[\sqrt{2}]$ *is closed under addition and multiplication. Furthermore, if* $a + b\sqrt{2} \neq 0$ *then we can solve* $(a + b\sqrt{2})(x + y\sqrt{2}) = 1$ *in* $\mathbb{R}$ *and derive*

$$x + y\sqrt{2} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

hence $(a+b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$ *and as* $a^2-2b^2 \neq 0$ *for* $a, b \in \mathbb{Q}$ *we note* $\frac{a}{a^2-2b^2}, -\frac{b}{a^2-2b^2} \in \mathbb{Q}$. *Therefore, we've shown every nonzero element in* $\mathbb{Q}[\sqrt{2}]$ *is a unit. The field* $\mathbb{Q}[\sqrt{2}]$ *is larger than* $\mathbb{Q}$ *but, still much smaller than* $\mathbb{R}$ *which contains many more irrational numbers.*

Definition 4.1.37. *The* **characteristic** *of a ring* R *is the smallest positive integer for which* $nx = 0$ *for all* $x \in R$. *We denote the character of* R *by* $char(R) = n$. *If no such integer exists then we say* $char(R) = 0$.

In practice, we usually can judge the character of a ring by how its identity behaves.

Theorem 4.1.38. *If* R *is a ring with unity* 1 *then* R *has characteristic zero if* 1 *has infinite order. If* 1 *has additive order* n *then* $char(R) = n$.

Proof: If 1 has infinite additive order then there is no positive n for which $n \cdot 1 = 0$ and hence R has characteristic zero. Otherwise, suppose $|1| = n$ in the additive sense. That is $n \cdot 1 = 0$ and n is the least positive integer for which we obtain 0. Calculate,

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n-summands} = 1x + 1x + \cdots + 1x = (1 + 1 + \cdots + 1)x = (n \cdot 1)x = 0x = 0.$$

therefore $\text{char}(R) = n$. □

Theorem 4.1.39. *The characteristic of an integral domain is either* 0 *or a prime.*

Proof: notice if 1 has infinite order than $\text{char}(R) = 0$ and we're done. So, suppose $n \cdot 1 = 0$ where $|1| = n$ in the additive sense. Let us suppose $n = st$ for some $1 \leq s, t \leq n$. Calculate,

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$$

hence either $s \cdot 1 = 0$ or $t \cdot 1 = 0$ thus either $s = n$ and $t = 1$ or $s = 1$ and $t = n$ since $|1| = n$. We've determined factors of n are 1 and n hence n is prime. □

Remark: these notes are lifted from my 2018 Math 421 Lecture Notes. We should probably discuss how § 7.5 of Dummit & Foote is a bit more general, I'll push that to start of LECTURE 8.

4.4 Lecture 24: ring homomorphism and field of fractions

We saw the concept of homomorphism allowed us connect groups which seemed the same in terms of their group structure. In the same way, the concept of ring homomorphism gives us a precise method to describe when two rings share similar structure. Or, in the case of isomorphism, the rings in question are, from the viewpoint of algebraic structure, the same. Much of this section directly echoes our previous work on groups, as such I will omit some proofs. In contrast, the field of quotients construction at the end of this Lecture is fascinating and new.

Definition 4.4.1. *A* **ring homomorphism** ϕ *from a ring* R *to a ring* S *is a function* $\phi : R \to S$ *which preserves the ring operations:*

(i.) $\phi(a+b) = \phi(a) + \phi(b)$ *for all* $a, b \in R$,

(ii.) $\phi(ab) = \phi(a)\phi(b)$ *for all* $a, b \in R$.

(iii.) $\phi(1_R) = 1_S$.

If ϕ *is a bijective ring homomorphism then* ϕ *is a ring isomorphism and we write* $R \cong S$

The meaning of $R \cong S$ should be clear from the context. We use $\cong$ to indicate an isomorphism of groups or rings as appropriate.

Example 4.4.2. *Consider* $\phi : \mathbb{Z} \to \mathbb{Z}_n$ *defined by* $\phi(x) = [x]_n$. *Observe,* ϕ *is a function since the domain is* $\mathbb{Z}$ *so there is no ambiguity in* $x \in \mathbb{Z}$[2].

$$\phi(x+y) = [x+y]_n = [x]_n + [y]_n = \phi(x) + \phi(y) \qquad \& \qquad \phi(xy) = [xy]_n = [x]_n[y]_n = \phi(x)\phi(y)$$

for all $x, y \in \mathbb{Z}$. *Thus* $\mathbb{Z}$ *and* $\mathbb{Z}_n$ *are homomorphic rings under the ring homomorphism* ϕ. *Incidentally, this is the* **natural homomorphism** *which also call the* **coset map** *since* $\mathbb{Z}_n$ *is the factor ring of* $\mathbb{Z}$ *by* $n\mathbb{Z}$ *and* $[x]_n = x + n\mathbb{Z}$, *so we could write* $\phi(x) = x + n\mathbb{Z}$.

Example 4.4.3. *The map* $\phi(z) = z^*$ *is a ring isomorphism from* $\mathbb{C}$ *to* $\mathbb{C}$ *with respect to the usual complex arithmetic where I intend the complex conjugate given by* $(x+iy)^* = x - iy$ *for* $x, y \in \mathbb{R}$. *You can check:*

$$(zw)^* = z^* w^* \qquad \& \qquad (z+w)^* = z^* + w^*$$

thus ϕ *is a ring homomorphism. In fact,* $\phi : \mathbb{C} \to \mathbb{C}$ *is an* **automorphism of** $\mathbb{C}$ *since* $\phi^{-1} = \phi$ *as* $(z^*)^* = z$ *for each* $z \in \mathbb{C}$. *You can verify,* $\phi^2 = Id$ *thus* ϕ *is an automorphism of order* 2.

My next example is an deeper version of Gallian's Example 3 on page 271.

Example 4.4.4. *The* **evaluation map** *is an important homomorphism which connects a ring* R *with polynomials* $R[x]$. *Pick* $a \in R$ *and define* $\phi_a(f(x)) = f(a)$ *for each* $f(x) \in R[x]$. *Observe,*

$$\phi_a((f+g)(x)) = (f+g)(a) = f(a) + g(a) = \phi_a(f(x)) + \phi_a(g(x))$$

and

$$\phi_a((fg)(x)) = (fg)(a) = f(a)g(a) = \phi_a(f(x))\phi_a(g(x))$$

thus $\phi_a : R[x] \to R$ *is a ring homomorphism.*

[2] in contrast, $g([x]_n) = x$ is rather disfunctional

Theorem 4.4.5. *Let $\phi : R \to S$ be a ring homomorphism from a ring R to a ring S. Let A be a subrng of R and B an ideal of S*

(i.) *for any $r \in R$ and $n \in \mathbb{N}$, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$,*

(ii.) *$\phi(A)$ is a subrng of S*

(iii.) *if A is an ideal and $\phi(R) = S$ then $\phi(A)$ is an ideal of S*

(iv.) *$\phi^{-1}(B)$ is an ideal of R*

(v.) *if R is commutative then $\phi(R)$ is commutative*

(vi.) *ϕ is an isomorphism iff ϕ is surjective and $Ker(\phi) = \{r \in R \mid \phi(r) = 0\} = \{0\}$.*

(vii.) *If $\phi : R \to S$ is a ring isomorphism of then $\phi^{-1} : S \to R$ is a ring isomorphism.*

Proof: similar to those given for groups. Main difference, for the multiplicative properties we cannot use the existence of inverses. However, if you study our proofs for the corresponding group claims then you'll see we can adopt those proofs with little modification. □

Notice the **additive** kernel determines injectivity of the ring homomorphism. This is not surprising as $(R, +)$ enjoys the structure of an abelian group so the injectivity from trivial kernel is precisely our group theoretic theorem.

Theorem 4.4.6. *Let $\phi : R \to S$ be a ring homomorphism from a ring R to a ring S. Then $Ker(\phi) = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R.*

Proof: suppose $\phi : R \to S$ is a ring homomorphism. Suppose $a, b \in \text{Ker}(\phi)$ then $\phi(a) = 0$ and $\phi(b) = 0$ consequently,

$$\phi(a - b) = \phi(a) - \phi(b) = 0 - 0 = 0,$$

and for $r \in R$,

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0 \qquad \& \qquad \phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0.$$

Thus $a - b \in \text{Ker}(\phi)$ and $ar, ra \in \text{Ker}(\phi)$ for all $a, b \in \text{Ker}(\phi)$ and $r \in R$. We find $\text{Ker}(\phi)$ is an ideal via Theorem 4.2.2. □

The first isomorphism theorem is also available for rings:

Theorem 4.4.7. *Let $\phi : R \to S$ be a ring homomorphism. Then the mapping from $R/Ker(\phi)$ to $\phi(R)$ given by $r + Ker(\phi) \mapsto \phi(r)$ is a ring isomorphism; $R/Ker(\phi) \cong \phi(R)$.*

Proof: exercise for the reader. □

The next theorem is also available for groups. This is Theorem 15.4 on page 274 of Gallian.

Theorem 4.4.8. *Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \mapsto r + A$ from R to R/A.*

Proof: if A is an ideal of R then the quotient ring R/A is well-defined and we construct $\pi : R \to R/A$ by $\pi(r) = r + A$. Observe,

$$\pi(r + s) = r + s + A = (r + A) + (s + A) = \pi(r) + \pi(s)$$

and

$$\pi(rs) = rs + A = (r + A)(s + A) = \pi(r)\pi(s)$$

for each $r, s \in R$. Morover, $\text{Ker}(\pi) = A$ hence A is the kernel of a ring homomorphism. □

Example 4.4.9. *Consider $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\phi(f(x)) = f(0)$. Since ϕ is a surjective ring homomorphism with $Ker(\phi) = \langle x \rangle$ we have by the first isomorphism theorem $\mathbb{Z}[x]/\langle x \rangle \approx \mathbb{Z}$. However, we know $\mathbb{Z}$ is an integral domain hence by Theorem 4.3.6 we find $\langle x \rangle$ is a prime ideal of $\mathbb{Z}[x]$. Indeed, by Theorem 4.3.7 we also see $\langle x \rangle$ is* **not** *maximal as $\mathbb{Z}$ is not a field.*

Theorem 4.4.10. *If R is a ring with unity 1 then the mapping $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$ is a ring homomorphism.*

Proof: recall $n \cdot 1$ is a notation for n-fold additions of 1 for $n \in \mathbb{N}$ or k-fold additions of -1 if $k = -n \in \mathbb{N}$. The proof is given on page 274-275 of Gallian. Essentially, this affirms that:

$$(m+n) \cdot 1 = m \cdot 1 + n \cdot 1 \qquad \& \qquad (m \cdot 1)(n \cdot 1) = (mn) \cdot 1 \qquad \square$$

Corollary 4.4.11. *If R is a ring and $Char(R) = n > 0$ then R contains a subring which is isomorphic to $\mathbb{Z}_n$. If $Char(R) = 0$ then R contains a subring which is isomorphic to $\mathbb{Z}$.*

Proof: Construct

$$S = \{k \cdot 1 \mid k \in \mathbb{Z}\}$$

in view of from Theorem 4.4.10 we note $\phi(k) = k \cdot 1$ is a homomorphism of $\mathbb{Z}$ and R and by construction $\phi(R) = S$. Suppose $\text{Char}(R) = n$, then $\text{Ker}(\phi) = \{k \in \mathbb{Z} \mid k \cdot 1 = 0\} = n\mathbb{Z}$. Hence, by the first isomorphism theorem, $\mathbb{Z}/\text{Ker}(\phi) \cong \phi(R)$ which gives $\mathbb{Z}/n\mathbb{Z} \cong S$. If R has characteristic zero then $S \cong \mathbb{Z}/\langle 0 \rangle \cong \mathbb{Z}$. $\square$

Corollary 4.4.12. *For any positive integer m, the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_m$ defined by $\phi(x) = [x]_m$ is a ring homomorphism.*

Proof: note $[x]_m = [1 + 1 + \cdots + 1]_m = x \cdot [1]_m$ hence $\phi(x) = [x]_m$ is a mapping with the same form as that given in Theorem 4.4.10. $\square$

The calculation in the Corollary above, the main point is that $[x]_m = x \cdot [1]_m$. We needed to make this same calculational observation in several past problems. For example, it is the heart of why homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_k$ have the form $[x]_n \mapsto [mx]_k$ where $k \mid mn$ (Problem 72).

Corollary 4.4.13. *(Steinitz, 1910): If $\mathbb{F}$ is a field of characteristic p then $\mathbb{F}$ contains a subfield which is isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ is a field of characteristic 0, then $\mathbb{F}$ contains a subfield isomorphic to the rational numbers.*

Proof: if $\mathbb{F}$ is a field of characteristic p then as a field is also a ring by Corollary 4.4.11. Thus $\mathbb{F}$ contains a subring isomorphic to $\mathbb{Z}_p$. If $\mathbb{F}$ has characteristic 0 then $\mathbb{F}$ has a subring S isomorphic to $\mathbb{Z}$ and we can construct a copy of $\mathbb{Q}$ from S as follows:

$$S_{\mathbb{Q}} = \{ab^{-1} \mid a, b \in S \text{ with } b \neq 0\} \quad \square$$

Definition 4.4.14. *Given a field $\mathbb{F}$ the subfield of $\mathbb{F}$ which is contained in all other subfields of $\mathbb{F}$ is called the* **prime** *subfield of $\mathbb{F}$.*

We can argue from Steinitz Theorem that the prime subfield of $\mathbb{F}$ is either $\mathbb{Q}$ or $\mathbb{Z}_p$. Any field of characteristic zero has $\mathbb{Q}$ as its *smallest* subfield. Any field of prime p characteristic has $\mathbb{Z}_p$ as its smallest subfield.

Theorem 4.4.15. *Let D be an integral domain. Then, there exists a field F that contains a subring isomorphic to D.*

Proof: an explicit and beautiful construction, see page 277-278 of Gallian. I may change the notation a bit. The notation which Gallian uses is the notation we wish to use in eventuality, but, to begin we should divorce our thinking from the familar so we don't assume more than we ought from the notation.

Let D be an integral domain with 1 the unity in D. Let $S = \{(a,b) \mid a,b \in D.\ b \neq 0\}$. Define $(a,b) \sim (c,d)$ if[3] $ad = bc$. We prove $\sim$ forms an equivalence relation on S:

(i.) let $(a,b) \in S$ then $(a,b) \sim (a,b)$ since $ab = ba$ (D is a commutative ring)

(ii.) if $(a,b) \sim (c,d)$ then $ad = bc$ hence $cb = da$ thus $(c,d) \sim (a,b)$.

(iii.) if $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ then $ad = bc$ and $cf = de$. Consider, by associativity of multiplication and the known data on a,b,c,d,e,f,

$$(ad)f = (bc)f = b(cf) = b(de)$$

Thus $(af)d = (be)d$ where $(c,d) \in S$ hence $d \neq 0$ and by the cancellation property of integral domains we find $af = be$ hence $(a,b) \sim (e,f)$

Therefore, $\sim$ is a reflexive, symmetric and transitive relation on S. Denote the equivalence class containing (a,b) by $[a,b] = \{(c,d) \mid (c,d) \sim (a,b)\}$. We claim that $S/\sim$ the set of equivalence classes of S under $\sim$ forms a field with respect to the following operations of addition and multiplication:

$$[a,b] + [c,d] = [ad + bc, bd] \qquad \& \qquad [a,b][c,d] = [ac, bd].$$

We must show these operations are well-defined since we used a representative to define the rule for an equivalence class. Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$ hence $ab' = ba'$ and $cd' = dc'$. Observe that

$$[ad + bc, bd] = [a'd' + b'c', b'd'] \qquad \text{if and only if} \qquad (ad + bc)b'd' = bd(a'd' + b'c').$$

Thus consider:

$$(ad + bc)b'd' = (ab')(dd') + (cd')(bb') = (ba')(dd') + (dc')(bb') = bd(a'd' + b'c').$$

Therefore addition on $S/\sim$ is well-defined. Next, observe that

$$[ac, bd] = [a'c', b'd'] \qquad \text{if and only if} \qquad (ac)(b'd') = (bd)(a'c')$$

Consider then,

$$(ac)(b'd') = (ab')(cd') = (ba')(dc') = (bd)(a'c')$$

Therefore, multiplication on $S/\sim$ is well-defined. It remains to verify addition and multiplication satisfy the field axioms. I'll begin by noting the operations are commutative since D is a commutative ring:

$$[a,b] + [c,d] = [ad + bc, bd] = [cb + da, db] = [c,d] + [a,b]$$

[3] yes, intuitively, we want (a,b) to model the fraction a/b whatever that means... surely $a/b = c/d$ gives $ad = bc$ hence this definition

likewise,

$$[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b].$$

Let $x \in D$ be nonzero, and $[a,b] \in S/\sim$. Note:

$$[a,b] + [0,x] = [ax + b(0), bx] = [ax,bx] = [a,b]$$

as $(ax,bx) \sim (a,b)$ is easy to verify (remember $x \neq 0$). We find $[0,x]$ serves as the additive identity of $S/\sim$. Next, consider $[1,1]$ and $[a,b] \in S/\sim$,

$$[a,b][1,1] = [a(1),b(1)] = [a,b]$$

hence $[1,1]$ is the unity of $S/\sim$. Multiplicative inverse is easy $[a,b] \neq 0$ has $a,b \neq 0$ hence $[b,a]$ is in $S/\sim$ and

$$[a,b][b,a] = [ab,ba] = [1,1]$$

as $(ab,ba) \sim (1,1)$ is easy to verify. Associativity,

$$[a,b] + \big([c,d] + [e,f]\big) = [a,b] + [cf + de, df] = [a(df) + (cf + de)b, bdf]$$

and

$$\big([a,b] + [c,d]\big) + [e,f] = [ad + bc, bd] + [e.f] = [(ad + bc)f + e(bd), bdf]$$

Thus addition is associative. I leave it to the reader to prove associativity of multiplication as well as the needed distributive properties linking addition and mulitplication. In summary, we have shown $S/\sim$ is a field. It remains to explain how it contains a subring which is isomorphic to D. You should not be surprised when I tell you that $\phi : D \to S/\sim$ defines an injective ring homomorphism if we set $\phi(x) = [x,1]$. Notice, $\phi(x) = [x,1] = 0$ implies $x = 0$ hence $\mathrm{Ker}(\phi) = \{0\}$. Moreover,

$$\phi(x + y) = [x + y, 1] = [x(1) + 1(y), 1(1)] = [x,1] + [y,1] = \phi(x) + \phi(y)$$

and

$$\phi(xy) = [xy,1] = [xy,1(1)] = [x,1][y,1] = \phi(x)\phi(y)$$

for all $x,y \in D$. Thus $D/\{0\} \cong\cong \phi(D)$ by the first isomorphism theorem of rings and hence $D \cong \phi(D)$. □

Definition 4.4.16. *The field F constructed from an integral domain D as in the proof above is called the* **field of quotients of** *D. We use the notation a/b or $\frac{a}{b}$ for the equivalence class $[a,b]$. We have shown,*

$$\mathbb{F} = \left\{ \frac{a}{b} \mid a,b \in D, b \neq 0 \right\}$$

is a field where we **define**

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

You can trace back through the proof of the field of quotients construction to see we have proved all the usual properties of rational numbers:

$$\frac{0}{a} = 0, \quad \frac{a}{b} \cdot \frac{b}{a} = 1, \quad \frac{ax}{bx} = \frac{a}{b}.$$

So, on the one hand, this proof we went over just now proves that $\mathbb{Q}$ exists if we are given $\mathbb{Z}$. On the other hand, it allows us to construct abstract fields which play the same role for a given integral domain as does $\mathbb{Q}$ for $\mathbb{Z}$. Personally, I view this construction and the clarity it can bring to **what** rational numbers **are** as a high point of abstract algebra. Is $1/2$ and $3/6$ the same number? I say emphatically **yes**. We have shown $1/2 = 3/6$ because the rigorous definition of $\mathbb{Q}$ says $a/b = c/d$ only if $ad = bc$ and surely we can agree $1(6) = 2(3)$. Now, does a given rational number have many different **fractions** which represent the same number? Yes. We also can agree about that. The pair $(1, 2) \neq (3, 6)$. In any event, we should keep in mind, equivalence classes are always with us whether we understand them or not. You might read this post by Paul Garrett.

Example 4.4.17. *If $D = \mathbb{Z}[x]$ then the field of quotients for D is the set $\{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}[x], g(x) \neq 0\}$*

Example 4.4.18. *If $D = \mathbb{F}[x]$ then the field of quotients for D is the set $\{f(x)/g(x) \mid f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0\} = \mathbb{F}(x)$ the rational functions over $\mathbb{F}$. For $\mathbb{F} = \mathbb{R}$ this is just the usual rational functions.*

Example 4.4.19. *The notation $\mathbb{Z}_p[x]$ is polynomials with $\mathbb{Z}_p$-coefficients. In contrast, $\mathbb{Z}_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}_p[x], g(x) \neq 0\}$. This gives an example of an infinite field with characteristic p.*

Outside this conversation, I might be tempted to agree that fields with finite characteristic are finite fields. This is clearly false by our last example !