MATH H113: Honors Introduction to Abstract Algebra

2016-03-30

- Rings of fractions
- Chinese remainder theorem

See pictures **Theorem**: Let R be a commutative ring. Let D be a subset of R such that:

- $D \neq \emptyset$,
- $0 \notin D$,
- D contains no zero divisors, and
- D is closed under multiplication

Let $F = R \times D$ and let $\sim$ be the relation of G given by $(r, d) \sim (s, e) \iff re = sd$.
Then:

a. $\sim$ is an equivalence relation on F.
b. Let Q be the set of $\sim$-equivalence classes in F
Write $(r, d) = \frac{r}{d}$. Then $\frac{r}{d} + \frac{s}{e} = \frac{re+sd}{de}$ and $\frac{r}{d} \cdot \frac{s}{e} = \frac{rs}{de}$ given well-defined binary operations on Q, and they make Q into a commutative ring with 1. Moreover, $1\frac{d}{d}\forall d \in D$.
c. Let $i : R \to Q$ be the map $r \mapsto \frac{rd}{d}$ for any $d \in D$. Then i is independent of the choice of d and is an injective ring homomorphism
d. For all $d \in D$, $i(d)$ is a unit in Q, and every element of A equals $i(d)^{-1}i(r)$ for some $r \in R$ and $d \in D$.
e. Q is the smallest ring with 1 containing a subgring isomorphic to R, in which all elements of D are units in A, in the following sense: for all rings Q' with 1 and all homomorphisms $\phi : R \to Q'$ such that $\phi(d)$ is a unit of Q' $\forall d \in D$, there is a unique ring homomorphism $\Phi : Q \to Q'$ such that $\phi = \Phi \circ i$.

$$\begin{tikzcd} R \arrow[d, "i"'] \arrow[dr, "\phi"] & \\ Q \arrow[r, "\Phi"'] & Q' \end{tikzcd}$$

Proof:

a. Already done.

b. We showed that $(r,d) \sim (s,e) \iff$ you can get from (r,d) to (s,e) by finitely many steps using only the relation $\overline{(r,d)} = \overline{(rd',dd')}$ (or it's opposite). This is left as an exercise, *except* I'll show the distributive law:
$\frac{r}{d}(\frac{s}{e} + \frac{t}{f}) \stackrel{?}{=} \frac{r}{d} \cdot \frac{s}{e} + \frac{r}{d} \cdot \frac{t}{f}$
We may assume $e = f$ ($\frac{s}{e} = \frac{sf}{ef}$ and $\frac{t}{f} = \frac{te}{fe}$; then $\frac{s}{e} + \frac{t}{e} = \frac{se+te}{e^2} = \frac{s+t}{e}$).
Then the LHS is $\frac{r}{d} \cdot \frac{s+t}{e} = \frac{r(s+t)}{de} = \frac{rs+rt}{de} = \frac{rs}{de} + \frac{rt}{de} = \frac{r}{d} \cdot \frac{s}{e} + \frac{r}{d} \cdot \frac{t}{e}$.

c. Again, i is a ring homomorphism (same kind of checking). Its kernel is 0 because $r \in \ker i \iff i(r) = i(0) \iff \frac{rd}{d} = \frac{0d}{d} \iff rd^2 = 0d^2 \iff rd = 0d \iff r = 0$.
(Can cancel d because $d \neq 0$ and it's not a zero divisor.)
$\frac{rd}{d'} = \frac{rd'}{d'}$ because both $= \frac{rdd'}{dd'}$.

d. $i(d)$ has inverse $\frac{1}{d}$ because $\frac{d^2}{d} \cdot \frac{1}{d} = \frac{d^2}{d} = 1 \in Q$
every element of Q ... is true because $\frac{r}{d} = i(d)^{-1}i(r) = \frac{1}{d} \cdot \frac{rd}{d} = \frac{rd}{d^2} = \frac{r}{d}$.

e. Given Q' and ϕ, define $\Phi(\frac{r}{d}) = \phi(d)^{-1}\phi(r)$ (because you have no choice) $\frac{r}{d} = i(d)^{-1}i(r) \implies \Phi(\frac{r}{d})$ must equal $\Phi(i(d)^{-1})\Phi(i(r)) = \Phi(i(d))^{-1}\Phi(i(r)) = \phi(d)^{-1}\phi(r)$ (need to check: $\Phi(1_Q) = 1_{Q'} \implies \Phi(u^{-1}) = \Phi(u)^{-1}\ \forall u \in Q^\times$). Also need to check: Φ is a ring homomorphism. Not assuming Q' is commutative.
Φ is well defined because
$\frac{r}{d} = \frac{s}{e}$
$\implies re = sd$
$\implies er = ds$
$\implies \phi(e)\phi(r) = \phi(d)\phi(s)$
$\implies \phi(d)^{-1}\phi(e)\phi(r) = \phi(s)$
$\implies \phi(e)\phi(d)^{-1}\phi(r) = \phi(s)$
$\implies \phi(d)^{-1}\phi(r) = \phi(e)^{-1}\phi(s)$
in a ring Q' with 1, if $u \in Q'^\times$ and $t \in Q'$ commute, then so do u^{-1} and t. Exercise.
Note: If ϕ is injective, then so is Φ. (Reverse the steps above).

Definition: For R and D as above, the ring A is denoted $D^{-1}R$ or $R[D^{-1}]$ (this does not mean polynomial ring or group ring).

Definition: If R is an integral domain, then we can let $D = R \setminus \{0\}$ in the theorem, and then $R[D^{-1}]$ is a field ($\frac{r}{d} \neq 0 \implies r \in D, so \frac{d}{r} \in Q$).
This is called the *quotient field* of R or the fraction field of R, or the field of fractions of R.
Example: $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$

Corollary (of the theorem): Every integral domain is a subring of a field (containing the field's "1").
$x = 1_R \implies x = x^2 \implies x(x-1) = 0 \implies \cancel{x = 0} \vee x = 1$

Corollary: A ring is an integral domain $\iff$ it is a subring of a field that contains (the field's) 1.

Chinese Remainder Theorem

Definition: Let $(R_i)_{i\in I}$ be a collection of rings. Then the *direct product* $\prod\limits_{i\in I} R_i$ (as a ring) is the abelian group given by the direct product of the additive groups of the R_i, with componentwise multiplication.
For the rest of today's lecture, let R be a commutative ring with 1.

Definition: Ideals I and J in R are comaximal if $I + J = (1)$.
Examples: Ideals in $\mathbb{Z}$:

- $(2), (3)$ are comaximal
- $(14), (10)$ are not comaximal (sum $= (2)$)
- $(m), (n)$ are comaximal $\iff$ $\gcd(m, n) = 1$.
  $1 = xm = yn \iff$
  $\in (m) + (n)$

Theorem (Special case of Chinese Remainder Theorem):
Let I and J be comaximal ideals in R. Then $\phi : R \to (R/I) \times (R/J)$ given by $r \mapsto (r + I, r + J)$ is a ring homomorphism with kernel $= I \cap J = IJ$. It is onto, and it induces an isomorphism $R/IJ = R/(I \cap J) \cong (R/I) \times (R/J)$.
Proof: Ring homomorphism: easy check. (each component of ϕ is a natural project $R \to R/I$ or $R \to R/J$).
$\ker\phi = I \cap J$: obvious.
$I \cap J = IJ$: $IJ \subseteq I$ and $IJ \subseteq J$ because they're ideal, so $IJ \subseteq I \cap J$.
Also let $a \in I \cap J$. Write $1 = x + y$ with $x \in I$ and $y \in J$ (using comaximality. $1 \in (1) = I + J$).
Then, $a = a(x + y) = ax + ay$
$ax \in IJ$ because $x \in I$ and $a \in J$
$ay \in IJ$ because $y \in J$ and $a \in I$.
$a \in IJ$
Onto: with x, y as above,
$\phi(x) = (0, 1)$ $x \in I$ so $x + I = 0 + I$
$x - 1 = -y \in J$ so $x + J = 1 + J$
Similarly $\phi(y) = (1, 0)$.
$\therefore$ given any $(a + I, b + J) \in (R/I) \times (R/J)$,
$(a + I, b + J) = \phi(ay + by)$ because $\phi(ay + bx)$
$= \phi(a)\phi(y) + \phi(b)\phi(x)$
$= (a + I, a + J)(1, 0) + (b + I, b + J)(0, 1)$
$= (a + I, 0) + (0, b + J)$
$= (a + I, b + J)$
Conclude by first isomorphism theorem.