RINGS INTRO

COLTON GRAINGER (MATH 6130 ALGEBRA)

10. Assignment due 2018-11-14

10.1. **[1, No. 7.1.7].** *Given.* R, a ring; Z, the center of R.

To prove. The center Z is a subring. If a R is a division ring, then Z is a field.

Proof. Let $r \in R$. Let $x, y \in Z$. Observe that the center is closed under subtraction.

$$r(y - x) = ry - rx = yr - xr = (y - x)r.$$

Observe that a product of elements in the center is also in the center.

$$rxy = xry = xyr.$$

Thus the center is a subring. □

Given. Now suppose our ring is a division ring.

To prove. Z is a field.

Proof. The center is a commutative ring by above. Let $r \in R$. Then there's $a \in R$ such that $a = r^{-1}$. Let $z \in Z$.

$$az = za \quad \text{implies} \quad (az)^{-1} = (za)^{-1} \quad \text{implies} \quad z^{-1}r = rz^{-1}.$$

So the center of the ring is closed under inverses. Thus the center is a division ring. □

10.2. **[1, No. 7.1.11].** *Given.* Suppose R is an entire ring. Suppose $x \in R$.

To prove. If $x^2 = 1$, then $x = \pm 1$.

Proof. Consider $x^2 = 1$ if and only if $(x - 1)(x + 1) = 0$. Since R has no zero divisors, the conclusion follows. □

10.3. **[1, No. 7.1.14].** *Given.* Let R be a commutative ring with unity. Let $x \in R$ be a nilpotent element such that

$$m = \min\{n \in \mathbf{N} : x^n = 0\}.$$

To prove. (a) Either x is zero or a zero divisor. (b) The element rx is nilpotent for all $r \in R$. (c) The element $1 + x$ is a unit in R. (d) The sum of any unit u and a nilpotent element is a unit in R.

Proof. (a) If $m = 1$, then $x = 0$. If $m > 1$, then x and x^{m-1} are both nonzero. (b) Observe

$$\begin{aligned}(rx)^m &= \underbrace{rx \cdots rx}_{m \text{ times}} \\ &= r^m x^m \\ &= r^m 0 \\ &= 0.\end{aligned}$$

Date: 2018-11-09.
Compiled: 2018-11-13.

(c) Follows from (d) which is verified by

$$(u+x)\left(\sum_{n=0}^{m-1}\frac{(-1)^n x^n}{u^{n+1}}\right)=1.$$

□

10.4. **[1, No. 7.2.2].** *Given.* Let R be a commutative ring with unity $1 \neq 0$ and let $p(x)$ be an element of the polynomial ring $R[x]$.

To prove. The polynomial $p(x)$ is a zero divisor if and only if there is a nonzero $b \in R$ such that $bp(x) = 0$.

Proof. ($\Rightarrow$) Clear. If $b \in R[x]$ is nonzero and $bp(x) = 0$, then p is a zero divisor. ($\Leftarrow$) Suppose g is a polynomial of minimal degree such that $g(x)p(x) = 0$. As a base case for induction consider a_n, b_m leading coefficients of $p(x)$ and $q(x)$ respectively. Then $a_n b_m = 0$. So

$$\underbrace{a_n g(x)}_{\deg m-1} p(x) = 0.$$

But g was a minimal zero divisor of $p(x)$, so $a_n g(x) = 0$. We proceed by strong induction on i. Suppose $a_{n-k}g(x) = 0$ for all $k < i$, where a_j is the coefficient of the jth term of $p(x)$. Because $g(x)p(x) = 0$, distributing we see $b_m a_{n-i} = 0$. As

$$\underbrace{a_{n-i}g(x)}_{\deg\leqslant m-1} p(x) = 0$$

we have $a_{n-i}g(x) = 0$.

Since for all $i < n$, $a_{n-i}g(x) = 0$ implies $a_{n-i}b_m = 0$, we conclude $b_m p(x) = 0$. □

10.5. **[1, No. 7.2.7].** *Given.* Let R be a commutative ring with unity, let $\mathscr{M}_n(R)$ be the ring of square n by n matrices with entries in the ring R, let Z be the center of $\mathscr{M}_n(R)$. Suppose $(z_{ij}) \in Z$.

To prove. The center Z is the ring of scalar matrices isomorphic to R.

Proof. Let E_{ij} be a "unit" matrix in $\mathscr{M}_n(R)$ with i, jth entry equal to 1, and all other entries 0. For all $i \in \{1, \dots, n\}$, we have

$$E_{ii}(z_{ij}) = (z_{ij})E_{ii} \text{ implies } z_{ij} = 0 \text{ if } |i-j| > 0.$$

For all $k \in \{1, \dots, n\}$, we have

$$E_{1k}(z_{ij}) = (z_{ij})E_{1k} \text{ implies } z_{11} = z_{kk}.$$

So Z is in the subring of scalar diagonal matrices. It's trivial to check that λI, a scalar diagonal matrix, commutes with any element of $\mathscr{M}_n(R)$. Moreover, the homomorphism $\varphi\colon R \to \mathscr{M}_n(R)$ given by $\lambda \mapsto \lambda I$ is an embedding and surjective onto the center Z. □

10.6. **[1, No. 7.2.13].** *Given.* Let $\mathscr{K}$ be one of the conjugacy classes (which will be denoted $\mathscr{K}_1, \dots, \mathscr{K}_r$) of the finite group G. Let R be a commutative ring with unity. Consider the group ring RG, with center $Z = Z(RG)$.

To prove. (a) $K = \sum_{k_i \in \mathscr{K}} k_i \in Z$. (b) $\alpha \in Z$ if and only if $\alpha = \sum a_i K_i$ for $a_i \in R$.

Proof.

(a) Each element $\sum r_g g \in RG$ commutes with K if and only if $gK = Kg$ for all $g \in G$. The conjugation action of G on its powerset $\mathscr{P}(G)$ is an inner automorphism on elements, so the conjugacy class $\mathscr{K}$ is fixed. Because G is finite, conjugation permutes the elements in $\mathscr{K}$. Thus $gKg^{-1} = K$.

(b) ($\Rightarrow$) Suppose $\alpha = \sum a_i K_i$. Then

$$\sum_i a_i K_i \sum_g r_g g = \sum_i \left(\sum_g r_g a_i K_i g \right) = \sum_i \left(\sum_g r_g a_i g K_i \right) = \sum_g r_g g \sum_i a_i K_i$$

so $\alpha \in Z$. ($\Leftarrow$) Say $\alpha \in Z$. We can write α as the sum over conjugacy classes $\{k_{n_i}\}$ of elements in G:

$$\alpha = \sum_i \left(\sum_{n_i} a_{n_i} k_{n_i} \right).$$

For each i, G acts transitively on by conjugation on $\{k_{n_i}\}$. Fix i. For all n_i, transitivity of conjugation implies $a_{n_i} = a_i$ for some $a_i \in R$. We conclude $\alpha = \sum a_i K_i$. □

10.7. **[1, No. 7.3.22].** *Given.* A ring R, an element $a \in R$, the sets $M = \{x \in R : ax = 0\}$ and $N = \{x \in R : xa = 0\}$, and a left ideal L.

To prove. (a) M is a right ideal, N is a left ideal. (b) I is an ideal.

Proof.

(a) First to argue that M is a subring.

- Nonempty: $0 \in M$.
- Closed under subtraction and multiplication: If $x, y \in M$, then $a(x - y) = ax - ay = 0$ and also $a(xy) = (ax)y = 0$.

Moreover, if $r \in R$, then $a(xr) = 0$, so $xr \in M$. Thus M is a right ideal. That N is a left ideal follows similarly.

(b) For each $a \in L$, let M_a be the right ideal of left annihilators of a. Observe

$$I = \bigcap_{a \in L} M_a$$

is a subring. Moreover, I is closed under right multiplication as the M_a are right ideals. Now let $r \in R$, $x \in I$, and $a \in L$. Because $rxa = 0$, $rx \in \cap M_a = I$. □

10.8. **[1, No. 7.3.25].** *Given.* Let R be a commutative ring with unity.

To prove. The binomial theorem: for all $a, b \in R$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Proof. Here's the crux of the argument: For all $k < n$, we have

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

We can proceed by induction and reindex the sums to exploit the above identity.

Base. Consider $(a+b)^1 = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0$.

Inductive step. Suppose true for $n \in \mathbf{N}$. Then

$$\begin{aligned}
(a+b)^{n+1} &= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b) \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} + b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.
\end{aligned}$$

□

10.9. **[1, No. 7.3.29].** *Given.* Let R be a commutative ring with unity $1 \neq 0$, let $\mathfrak{N}(R)$ be its nilradical.

To prove. $\mathfrak{N}(R)$ is an ideal.

Proof. $0 \in \mathfrak{N}(R)$, so its nonempty. Let $x, y \in \mathfrak{N}(R)$. There exist $m, n \in \mathbf{N}$ such that $x^n = y^m = 0$. Let $\ell = 2\max\{m, n\}$. Applying the binomial theorem,

$$(x+y)^\ell = \sum_{k=1}^{\ell} \binom{\ell}{k} x^k y^{\ell-k} = \underbrace{0 + \cdots + 0}_{\ell \text{ times}}$$

as for all $k \in \{0, \ldots, \ell\}$ either x^k or $y^{\ell-k}$ will be 0. Observe also $(xy)^{\min\{m,n\}} = 0$. So $\mathfrak{N}(R)$ is an ideal. □

10.10. **[1, No. 7.3.34].** *Given.* Let R be a ring with unity $1 \neq 0$. Let I, J be ideals of R.

To prove. (a) If K is an ideal such that $I \cup J \subset K \subset I + J$, then $K = I + J$. (b) IJ is an ideal contained in $I \cap J$. (c) The containment in (b) may be proper. (d) If R happens to be commutative, then we have equality in (b).

Proof.

(a) $I, J \subset I + J$. Suppose K is as above. Let $x + y \in I + J$. Observe $x, y \in K$. So $x + y \in K$ and thus $I + J \in K$.

(b) Immediately from its definition, IJ is nonempty and closed under addition. Let $\sum_1^n x_i y_i \in IJ$ an $r \in R$. Then

$$r \sum_1^n x_i y_i \sum_1^n \underbrace{(rx_i)}_{\in I} y_i \in IJ.$$

So IJ is an ideal. Moreover, I, J are ideals, so $\sum_1^n \underbrace{x_i y_i}_{\in I \cup J} \in I \cup J$. Thus $IJ \subset I \cup J$.

(c) Consider $I = J = n\mathbf{Z}$ for $n \in \mathbf{Z}_{\geqslant 2}$. Observe $IJ = n^2\mathbf{Z}$, yet $I \cap J = n\mathbf{Z}$.

(d) Suppose R is a commutative[1] unital ring with comaximal ideals I and J. Let $z \in I \cap J$. Now $z \in I + J$ also, so there are x, y in I, J respectively such that $x + y = z$. Then $z = x1 + 1y \in IJ$. □

[1] Is this hypothesis necessary?

10.11. **[1, No. 7.4.10].** *Given.* Let R be commutative unital ring, let P be a prime ideal of R. Suppose P is entire (i.e., contains no zero divisors).

To prove. R is entire.

Proof. Say $ab = 0$. Then with $ab + P = (a + P)(b + P) = 0$. Since P is prime, R/P is entire. Wlog, $a + P = P$, so $a \in P$. As P is an ideal we have $ab \in P$. As P is entire $ab = 0$ implies $b = 0$. □

10.12. **[1, No. 7.4.30].** *Given.* Let R be a commutative unital ring, let I be an ideal of R, let rad$I$ be the radical of I.

To prove. (a) rad I is an ideal containing I. (b) rad $I/I = \mathfrak{N}\,(R/I)$.

Proof. (a) $I \subset$ rad I by definition. Let $x, y \in$ rad I. Say that n and m are the minimal powers required such that $x^n, y^m \in$ rad I. Let $\ell = \min\{n, m\}$ and $k = 2\max\{n, m\}$. Observe

$$(xy)^\ell = x^\ell y^\ell \in I, \quad (x + y)^k = \sum_{j=0}^{k} \binom{k}{j} x^j y^{k-j} \in I.$$

So rad I is a subring. Moreover, if $r \in R$, then $(rx)^n = r^n x^n \in I$. So rad I is an ideal. (b) Let $x + I \in$ rad I/I. Then $(x + I)^n = x^n + I = I$. So $x + I \in \mathfrak{N}\,(R/I)$. To show the other containment, run the same argument in reverse. □

10.13. **[1, No. 7.4.37].** *Given.* Let R be a commutative unital ring.

To prove. R is a local ring with maximal ideal $\mathfrak{m}$ if and only if $R \setminus \mathfrak{m} = R^*$ is the multiplicative group of units.

Proof. ($\Rightarrow$) Say $R \setminus \mathfrak{m}$ is not a unit. Then the principal ideal generated by x is contained in another maximal ideal $\mathfrak{n} \neq \mathfrak{m}$, which is a contradiction, as R is a local ring. So x is a unit. ($\Leftarrow$) Suppose $R \setminus R^*$ is an ideal $\mathfrak{m}$. Consider $\mathfrak{a}$ a proper ideal of R. We have

$$\mathfrak{a} \cap R^* = \varnothing \quad \text{implies} \quad R \setminus R^* \supset \mathfrak{a}.$$

Thus $\mathfrak{m} \supset \mathfrak{a}$, demonstrating $\mathfrak{m}$ is the unique maximal ideal of R. □

References

[1] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed. Hardcover; Prentice Hall, 2004 [Online]. Available: http://www.worldcat.org/isbn/0471433349