Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 16, 2020

Problems in Section 3.3 - 3.4.

1. If U is an ideal of R and $1 \in U$, prove that $U = R$.

Proof. Choose $r \in R$. Since $1 \in U$ and U is an ideal, $r \cdot 1 = r \in U$. This shows that $U = R$. $\square$

2. If F is a field, prove its only ideals are (0) and F itself.

Proof. Let U be an ideal. If $U = (0)$, there is nothing to prove. If $U \neq (0)$, as $U \subset F$, for any $u \neq 0 \in U$, there exists its multiplicative inverse so that $u^{-1} \cdot u = 1 \in U$. Now by Problem 1, $U = R$. $\square$

3. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.

Proof. Let $\phi : F \to F'$ be a homomorphism where F and F' are fields. Note that

$$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$$

so that either $\phi(1) = 1$ or $\phi(1) = 0$. If former was the case, then $\phi(x) = 0$ if and only if $x = 0$ so that ϕ is an isomorphism. If later was the case, then ϕ is a zero-map. $\square$

4. If R is a commutative ring and $a \in R$,
a) Show that $aR = \{ar : r \in R\}$ is a two-sided ideal of R.

Proof. We first show that aR is a subgroup of R under addition operation. Choose $ar_1, ar_2 \in aR$. Then $ar_1 + ar_2 = a(r_1 + r_2) \in aR$ so that aR is closed under addition. We have the additive identity $0 = a \cdot 0 \in aR$, and the additive inverse $a(-r) \in aR$ for each $ar \in aR$. Hence, aR is a subgroup of R under addition.
Now we show that aR swallows up the multiplication from left and right by arbitrary ring elements. Choose $r \in R$. Since R is commutative, for any $u = ar' \in aR$, $ru = r(ar') = (ra)r' = (ar)r' = a(rr') \in aR$. Also, $ur = (ar')r = a(r'r) \in aR$. Therefore, aR is now a two-sided ideal of R. $\square$

b) Show by an example that this may be false if R is not commutative.

Proof. Suppose we take R to be the ring of all rational matrices of size 2×2. Set $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Then

$$aR = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \, a, b \in \mathbb{Q} \right\}.$$

But for $r = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$,

$$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \notin aR$$

so that aR is not necessarily a two sided ideal if R is not commutative. □

5. If U and V are ideals of R, let $U + V = \{u + v \mid u \in U, v \in V\}$. Prove that $U + V$ is also an ideal.

Proof. Just merely observing U and V as subgroups of abelian group R under addition, $U+V$ is also a subgroup of R under addition. Now, we choose $r \in R$. Then, for any $u \in U$, $v \in V$, $r(u + v) = ru + rv \in U + V$ since $ru \in U$ and $rv \in V$ as U and V are ideals of R. So, $(u + v)r \in U + V$ holds similarly. Thus, $U + V$ is an ideal in R. □

6. If U, V are ideals of R let UV be the set of all elements that can be written as finite sums of elements of the form uv whre $u \in U$ and $v \in V$. Prove that UV is an ideal of R.

Proof. It is possible to express UV as

$$UV = \left\{ \sum_{i=1}^{n} u_i v_i \,\middle|\, u_i \in U, v_i \in V, n \in \mathbb{Z}^+ \right\}.$$

Note that $\sum_i^n u_i v_i + \sum_j^m u_j v_j = \sum_k^{n+m} u_k v_k \in UV$ so that UV is closed under addition. Also, it clearly contains the additive identity 0, and the additive inverse $-\sum_i^n u_i v_i = \sum_i^n (-u_i) v_i$ for each $\sum_i^n u_i v_i$ in UV. Thus, UV is a subgroup of R under addition. Now choose $r \in R$. Consequently,

$$r \cdot \sum_{i=1}^{n} u_i v_i = \sum_{i=1}^{n} (r u_i) v_i = \sum_{i=1}^{n} (u_i') v_i \in UV$$

with some $u_i' \in U$ for each $i = 1, 2, \cdots, n$. Similar argument holds for the right multiplication of r, so that UV is an ideal of R. □

7. In Problem 6 prove that $UV \subset U \cap V$.

Proof. Note that since U and V are ideals,

$$\sum_{i=1}^{n} u_i v_i = \sum_{i=1}^{n} (u_i') \in U, \quad \sum_{i=1}^{n} u_i v_i = \sum_{i=1}^{n} (v_i') \in V$$

for some $u_i' \in U$ and $v_i \in V$. Hence, $UV \subset U \cap V$. $\square$

8. If R is the ring of integers, let U be the ideal consisting of all multiples of 17. Prove that if V is an ideal of R and $R \supset V \supset U$ then either $V = R$ or $V = U$. Generalize!

Proof. Note that every subgroup of cyclic group is cyclic, hence, $V \supset U$ must be a form of (m) where $m > 0$ is an integer, dividing 17. Thus, either $m = 1$ or $m = 17$. That is, equivalently, $V = R$ or $V = U$. This argument holds even if we change 17 into any prime number. $\square$

9. If U is an ideal of R, let $r(U) = \{x \in R : xu = 0 \text{ for all } u \in U\}$. Prove that $r(U)$ is an ideal of R.

Proof. Choose $x, y \in r(U)$. Then $(x+y)u = xu+yu = 0+0 = 0$ for all $u \in U$ so that $r(U)$ is closed under addition. Clearly, $0 \in r(U)$. Also, $(-x)u = -(xu) = 0$ so that $-x \in r(U)$ for each $x \in r(U)$. Thus, $r(U)$ is a subgroup of R under addition.
Now choose $r' \in R$. Then $(r'x)u = r'(xu) = 0$ so that $r'x \in r(U)$ and $(xr')u = x(r'u) = xu' = 0$ for some $u' \in U$ so that $xr' \in r(U)$. Therefore, $r(U)$ is an ideal of R. $\square$

10. If U is an ideal of R let $[R : U] = \{x \in R : rx \in U \text{ for every } r \in R\}$. Prove that $[R : U]$ is an ideal of R and that it contains U.

Proof. Choose $x, y \in [R : U]$. Then $r(x + y) = rx + ry \in U$ for all $r \in R$ so that $[R : U]$ is closed under addition. Clearly, $0 \in [R : U]$. Also, $r(-x) = -(rx) \in U$ so that $-x \in [R : U]$. Hence, $[R : U]$ is a subgroup of R under addition.
Now choose $r' \in R$. Then $r(r'x) = (rr')x \in U$ so that $r'x \in [R : U]$. Also, $r(xr') = (rx)r' \in U$ since $rx \in U$ and U is an ideal. Therefore, we conclude that $[R : U]$ is an ideal of R. $\square$

11. Let R be a ring with unit element. Using its elements we define a ring $\tilde{R}$ by defining $a \oplus b = a + b + 1$, and $a \cdot b = ab + a + b$, where $a, b \in R$ and where the addition and multiplication on the right-hand side of these relations are those of R.
a) Prove that $\tilde{R}$ is a ring under the operations $\oplus$ and $\cdot$.

Proof. (Closedness of $\oplus$) For all $a, b \in R$, $a \oplus b = a + b + 1 \in R$.
(Associativity) For all $a, b, c \in R$,

$$a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + (b + c + 1) + 1 = (a + b + 1) + c + 1 = (a \oplus b) \oplus c.$$

(Commutativity) For all $a, b \in R$, $a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$.
(Additive identity) For all $a \in R$, $a \oplus -1 = a = -1 \oplus a$.
(Additive inverse) For all $a \neq -1 \in R$, $a \oplus (-a - 2) = -1 = (-a - 2) \oplus a$.
(Closedness of $\cdot$) For all $a, b \in R$, $a \cdot b = ab + a + b \in R$.
(Associativity) For all $a, b, c \in R$,

$$\begin{aligned} a \cdot (b \cdot c) &= a \cdot (bc + b + c) = a(bc + b + c) + a + (bc + b + c) \\ &= abc + ac + bc + ab + a + b + c \\ &= (ab + a + b)c + (ab + a + b) + c = (a \cdot b) \cdot c. \end{aligned}$$

(Distributive properties) For all $a, b, c \in R$,

$$\begin{aligned} a \cdot (b \oplus c) &= a \cdot (b + c + 1) \\ &= a(b + c + 1) + a + (b + c + 1) \\ &= ab + ac + 2a + b + c + 1, \end{aligned}$$

where

$$\begin{aligned} (a \cdot b) \oplus (a \cdot c) &= (ab + a + b) \oplus (ac + a + c) \\ &= (ab + a + b) + (ac + a + c) + 1 \\ &= ab + ac + 2a + b + c + 1 \end{aligned}$$

so that $a \cdot (b \oplus c) = (a \cdot b) \oplus (a \cdot c)$. Further,

$$\begin{aligned} (a \oplus b) \cdot c &= (a + b + 1) \cdot c \\ &= (a + b + 1)c + (a + b + 1) + c \\ &= ac + bc + 2c + a + b + 1, \end{aligned}$$

where

$$\begin{aligned} (a \cdot c) \oplus (b \cdot c) &= (ac + a + c) \oplus (bc + b + c) \\ &= (ac + a + c) + (bc + b + c) + 1 \\ &= ac + bc + 2c + a + b + 1 \end{aligned}$$

so that $(a \oplus b) \cdot c = (a \cdot c) \oplus (b \cdot c)$. Therefore, $\tilde{R}$ is a ring. $\square$

b) What act as the zero-element of $\tilde{R}$?

Solution. -1 is clearly the zero-element. $\square$

c) What act as the unit-element of $\tilde{R}$?

Solution. Note that for all $a \neq -1 \in \tilde{R}$,

$$a \cdot u = a \iff au + a + u = a \iff u = 0.$$

Thus, 0 is the unit-element of $\tilde{R}$. $\square$

d) Prove that R is isomorphic to $\tilde{R}$.

Proof. Define a mapping $\phi : R \to \tilde{R}$ by $\phi(a) = a - 1$. Then it is a homomorphism since

$$\begin{aligned}
\phi(a+b) &= (a+b) - 1 = (a-1) + (b-1) + 1 = \phi(a) \oplus \phi(b), \\
\phi(ab) &= ab - 1 = (a-1)(b-1) + (a-1) + (b-1) = \phi(a) \cdot \phi(b).
\end{aligned}$$

Clearly ϕ is surjective. Also, $\phi(a) = -1 \iff a = 0$, so that the kernel of ϕ is trivial. Hence, ϕ induces an onto isomorphism between R and $\tilde{R}$. $\square$

12. In Example 3.1.6 we discussed the ring of rational 2×2 matrices. Prove that this ring has no ideals other than (0) and the ring itself.

Proof. Let U be a proper nontrivial ideal of R. If $U = (0)$, there is nothing to prove. Suppose U has a nonzero 2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $\det(A) \neq 0$, it has the inverse $A^{-1} \in R$ so that $A^{-1}A = I \in U$, so that $U = R$. If $\det(A) = 0$, for if $a \neq 0$,

$$\begin{aligned}
&\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U, \\
&\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1/a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in U, \\
\implies &\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U.
\end{aligned}$$

Hence $U = R$. If $a = 0$, since $ad = bc$, then $b = 0$ or $c = 0$. If both $b = c = 0$ and $d = 0$, then $U = (0)$. If $b = c = 0$ and $d \neq 0$,

$$\begin{aligned}
&\begin{pmatrix} 0 & 1/d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U, \\
&\begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1/d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in U, \\
\implies &\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U,
\end{aligned}$$

so that $U = R$. Now we assume that, WLOG, $b = 0$ and $c \neq 0$. Additionally we can assume that $d \neq 0$, since $d = 0$ is intrinsically the same case with above. So, we consider $a = b = 0$ and $c, d \neq 0$. Observe that

$$\begin{aligned} &\begin{pmatrix} 0 & 1/c \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in U, \\ &\begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1/c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in U, \\ \implies &\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in U, \end{aligned}$$

so that $U = R$. Hence we see that $U = (0)$ or either $U = R$. □

13. In Example 3.1.8 we discussed the real quaternions. Using this as a model we define the quaternions over the integers mod p, p an odd prime number, in exactly the same way; however, now considering all symbols of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where α_i are integers mod p.
a) Prove that this is a ring with p^4 elements whose only ideals are (0) and the ring itself.

Proof. There are p^4 different elements possible in R, and R is clearly a ring with the operations inherited from the quaternion ring over real. Now suppose U is an ideal of R. If $U = (0)$, there is nothing to prove. If $U \neq (0)$, there is a $a + bi + cj + dk \in I$ and WLOG, $a \neq 0$. Observe that:

$$\begin{aligned} &i(a + bi + cj + dk)i = -a - bi + cj + dk \\ &\implies (a + bi + cj + dk) - (-a - bi + cj + dk) = 2a + 2bi \implies a + bi \in I, \\ &j(a + bi)j = -a + bi \implies (a + bi) - (a - bi) = 2a \implies 1 \in I, \end{aligned}$$

so that $I = R$. □

b) Prove that this ring is not a division ring.

Proof. Note that

$$qq' = (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

for $a, b, c, d \in Z_p$. In general, a, b, c, d need not be all 0 to satisfy $a^2 + b^2 + c^2 + d^2 = 0$. Hence this admits a zero divisor in R. Therefore, R is not a division ring. We can also make use of Wedderburn's Theorem, which states that every finite division ring must be commutative. □

14. For $a \in R$ let $Ra = \{xa : a \in R\}$. Prove that Ra is a left-ideal of R.

Proof. Ra is clearly a subgroup of R under addition. Choose $r \in R$. Then $r(xa) = (rx)a \in Ra$ so that Ra is a left ideal of R. $\square$

15. Prove that the intersection of two left-ideals of R is a left-ideal of R.

Proof. Let U and V be the left-ideals of R. We know that intersection of two subgroup is again a subgroup. Now choose $r \in R$. Then for $w \in U \cap V$, $rw \in U, V$ so that $uw \in U \cap V$. Hence, $U \cap V$ is a left-ideal of R. $\square$

16. What can you say about the intersection of a left-ideal and right-ideal of R?

Solution. Intersection of a left-ideal and right-ideal need not be a left-ideal of right-ideal. For instance, suppose R is the ring of 2×2 rational matrices. Consider the ideals

$$U_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Q} \right\}$$

and

$$U_2 = R \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \middle| a, c \in \mathbb{Q} \right\}$$

so that the intersection is given by

$$U_1 \cap U_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{Q} \right\}.$$

But this is neither a left ideal nor a right ideal, since

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \notin U, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin U.$$

$\square$

17. If R is a ring and $a \in R$ let $r(a) = \{x \in R : ax = 0\}$. Prove that $r(a)$ is a right-ideal of R.

Proof. Choose $x, y \in r(a)$. Then $a(x + y) = ax + ay = 0$ so that $r(a)$ is closed under addition. Also, $0 \in r(a)$. Further, $a(-x) = -(ax) = 0$ for all $x \neq 0$ so that $-x \in r(a)$. Therefore, $r(a)$ is a subgroup of R under addition.
Now choose $r' \in R$. Then $a(xr) = (ax)r = 0$ so that $xr \in r(a)$. Hence, $r(a)$ is now a right-ideal of R. $\square$

18. If R is a ring and L is a left-ideal of R let $\lambda(L) = \{x \in R : xa = 0 \text{ for all } a \in L\}$. Prove that $\lambda(L)$ is a two-sided ideal of R.

Proof. Choose $x, y \in \lambda(L)$. Then $(x+y)a = xa + ya = 0$ for all $a \in L$ so that $\lambda(L)$ is closed under addition. Also, $0 \in \lambda(L)$. Further, $(-x)a = -(xa) = 0$ so that $-x \in \lambda(L)$ for all $x \in \lambda(L)$. Hence $\lambda(L)$ is a subgroup of R under addition.
Now choose $r' \in R$. Then $(r'x)a = r'(xa) = 0$ so that $r'x \in \lambda(L)$. Also, $(xr')a = x(r'a) = x(a') = 0$ where $a' \in L$, so that $xr' \in \lambda(L)$. Therefore, $\lambda(L)$ is a two-sided ideal of R. □

19. Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is a commutative ring.

Proof. First note that $(2x)^3 = 2x \implies 6x = 0$ for all $x \in R$. Computing $(x+y)^3$ and $(x-y)^3$,

$$\begin{aligned}(x+y)^3 = x+y &\implies x^2y + xyx + xy^2 + yx^2 + yxy + y^2x = 0,\\ (x-y)^3 = x-y &\implies x^2y + xyx - xy^2 + yx^2 - yxy - y^2x = 0.\end{aligned}$$

so that on adding, $2x^2y + 2xyx + 2yx^2 = 0$. Multiplying x on left and right, we obtain

$$2xy + 2x^2yx + 2xyx^2 = 0, \quad 2x^2yx + 2xyx^2 + 2yx = 0$$

so that $2(xy - yx) = 0$. Now we calculate $(x + x^2)^3$. Consequently,

$$(x+x^2)^3 = 4(x+x^2) = x + x^2 \implies 3(x+x^2) = 0.$$

Moreover,

$$3(x + y + (x+y)^2) = 3(x+x^2) + 3(y+y^2) + 3(xy+yx) = 3(xy+yx) = 0.$$

Since $6xy = 0$, $3(xy - yx) = 0$. Now from $2(xy - yx) = 0$, we have $xy - yx = 0$ and hence R is commutative. □

20. If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' prove that $\phi(1)$ is the unit element of R'.

Proof. Since ϕ is onto, for any $a \in R'$ there is $x \in R$ so that $a = \phi(x)$. Consequently, $a = \phi(x) = \phi(x \cdot 1) = \phi(x)\phi(1) = a\phi(1)$ and $a = \phi(x) = \phi(1 \cdot x) = \phi(1)\phi(x) = \phi(1)a$, so that $\phi(1)$ is the unit element of R'. □

21. If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that $I(\phi) \neq R$, prove that $\phi(1)$ is the unit element of R'.

Proof. Note that $\phi(1) = \phi(1 \cdot 1) = \phi(1)^2$ so that either $\phi(1) = 0$ or $\phi(1) = 1$. If former was the case, $I(\phi) = R$. Hence, $\phi(1) = 1$ is the only possible case. □