Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 16, 2020

Problems in Section 3.6.

1. Prove that if $[a,b]=[a',b']$ and $[c,d]=[c',d']$ then $[a,b][c,d]=[a',b'][c',d']$.

Proof. Note that

$$[a,b]=[a',b'] \iff a'b=b'a, \quad [c,d]=[c',d'] \iff c'd=d'c$$

so that

$$a'c'(bd)-(b'd')(ac)=(a'b)(c'd)-(ab')(cd')=0 \iff [a,b][c,d]=[a',b'][c',d'].$$

□

2. Prove the distributive law in F.

Proof. Suppose $[a,b]$, $[c,d]$ and $[e,f]$ are given. Then

$$\begin{aligned}[a,b]([c,d]+[e,f]) &= [a,b]([cf+ed,df]) = [acf+aed,bdf]\\ ([a,b][c,d])+([a,b][e,f]) &= [ac,bd]+[ae,bf] = [acbf+aebd,b^2df] = [acf+aed,bdf]\end{aligned}$$

so that $[a,b]([c,d]+[e,f])=([a,b][c,d])+([a,b][e,f])$. Similarly,

$$\begin{aligned}([a,b]+[c,d])[e,f] &= [ad+bc,bd][e,f] = [ade+bce,bdf]\\ ([a,b][e,f])+([c,d][e,f]) &= [ae,bf]+[ce,df] = [aedf+bfce,bdf^2] = [ade+bce,bdf]\end{aligned}$$

so that $([a,b]+[c,d])[e,f]=([a,b][e,f])+([c,d][e,f])$. Hence the distribution laws are verified. □

3. Prove that the mapping $\phi: D\to F$ defined by $\phi(a)=[a,1]$ is an isomorphism of D to F.

Proof. It is clearly a homomorphism since

$$\phi(a+b) = [a+b,1] = [a,1]+[b,1], \quad \phi(ab) = [ab,1] = [ab, 1\cdot 1] = [a,1][b,1].$$

Now we investigate the kernel of ϕ. Suppose $\phi(a) = [a,1] = [0,1]$. Then it follows that $a = 0$, hence ϕ is an injection(isomorphism). $\square$

4. Prove that if K is any field which contains D then K contains a subfield isomorphic to F.

Proof. Define a mapping $\phi : F \to K$ by $\phi(a/b) = a/b$ (Be cautious with the meaning of slash in the left and right. They are different). We check if ϕ is a homomorphism. Note that

$$\phi(a/b + c/d) = \phi\left(\frac{ad+bc}{bd}\right) = (ad+bc)/bd = a/b + c/d,$$
$$\phi(a/b \cdot c/d) = \phi(ac/bd) = ac/bd = a/c \cdot b/d,$$

and hence ϕ is a homomorphism. We check if ϕ is injective. Suppose $\phi(a) = \phi(a/1) = 0$, then it is must that $a = 0$. Thus, ϕ is an imbedding of F into K. Therefore, K contains a subfield isomorphic to F. $\square$

5. Let R be a commutative ring with unit element. A nonempty subset S of R is called a multiplicative system if
1. $0 \in S$. 2. $s_1, s_2 \in S$ implies that $s_1, s_2 \in S$.
Let M be the set of all ordered pairs (r,s) where $r \in R, s \in S$. In M define $(r,s) \sim (r', s')$ if there exists an element $s" \in S$ such that

$$s"(rs' - sr') = 0$$

a) Prove that this defines an equivalence relation on M.

Proof. (Symmetry) For any $r \in R$, $s \in S$, $(rs - sr) = 0$ so that $(r,s) \sim (r,s)$.
(Reflexive) For any $r, r' \in R$, $s, s' \in S$, if $(r,s) \sim (r', s')$,

$$s''(rs' - sr') = 0 \iff s''rs' = s''sr' \iff s''(r's - s'r) = 0$$

for some $s'' \in S$ so that $(r', s') \sim (r,s)$.
(Transitive) For any $r, r', r'' \in R$, $s, s', s'' \in S$, if $(r,s) \sim (r', s')$ and $(r', s') \sim (r'', s'')$, then

$$u(rs' - sr') = 0, \quad v(r's'' - s'r'') = 0$$

for some $u, v \in S$. Then

$$(uvs')(rs'' - sr'') = (urs')(vs'') - (vs'r'')(us) = (rsr')(vs'') - (vr's'')(us) = 0$$

so that $(r,s) \sim (r'', s'')$. $\square$

Let the equivalence class of (r, s) be denoted by $[r, s]$ and let R_S be the set of all the equivalence classes. In R_S define $[r_1, s_1] + [r_2, s_2] = [r_1 s_2 + r_2 s_1, s_1 s_2]$ and $[r_1, s_1][r_2, s_2] = [r_1 r_2, s_1 s_2]$.

b) Prove that the addition and multiplication described above are well defined and that R_S forms a ring under these operations.

Proof. Suppose $[r_1, s_1] = [r_1', s_1']$ and $[r_2, s_2] = [r_2' s_2']$. Thus, there exits $u_1, u_2 \in S$ such that

$$u_1(r_1 s_1' - s_1 r_1') = 0, \quad u_2(r_2 s_2' - s_2 r_2') = 0$$

Observe that

$$\begin{aligned}
(u_1 u_2)\cdot &\left[(r_1 s_2 + r_2 s_1)(s_1' s_2') - (s_1 s_2)(r_1' s_2' + r_2' s_1')\right] \\
&= (u_1 r_1 s_1')(u_2 s_2 s_2') + (u_1 s_1 s_1')(u_2 r_2 s_2') - (u_1 r_1' s_1)(u_2 s_2 s_2') - (u_1 s_1 s_1')(u_2 r_2' s_2') \\
&= (u_1 r_1' s_1)(u_2 s_2 s_2') + (u_1 s_1 s_1')(u_2 r_2' s_2') - (u_1 r_1' s_1)(u_2 s_2 s_2') - (u_1 s_1 s_1')(u_2 r_2' s_2') = 0
\end{aligned}$$

so that $[r_1 s_2 + r_2 s_1, s_1 s_2] = [r_1' s_2' + r_2' s_1', s_1' s_2']$. Hence, addition is well defined. Now for the multiplication,

$$\begin{aligned}
(u_1 u_2)\cdot &\left[(r_1 r_2)(s_1' s_2') - (s_1 s_2)(r_1' r_2')\right] \\
&= (u_1 r_1 s_1')(u_2 r_2 s_2') - (u_1 s_1 r_1')(u_2 r_2' s_2) \\
&= (u_1 s_1 r_1')(u_2 r_2' s_2) - (u_1 s_1 r_1')(u_2 r_2' s_2) = 0
\end{aligned}$$

so that $[r_1 r_2, s_1 s_2] = [r_1' r_2', s_1' s_2']$. Thus, multiplication is also well defined. ☐

c) Can R be imbedded in R_S?

Solution. It depends on the choice of S. Look at the next problem. ☐

d) Prove that the mapping $\phi : R \to R_S$ defined by $\phi(a) = [as, s]$ is a homomorphism of R into R_S and find the kernel of ϕ.

Proof. Choose $a, b \in R$. Then

$$\begin{aligned}
\phi(a + b) &= [(a + b)s, s] = [as + bs, s] = [as, s] + [bs, s], \\
\phi(ab) &= [(ab)s, s] = [abss, ss] = [as, s][bs, s]
\end{aligned}$$

so that ϕ is a homomorphism. Let K be the kernel of ϕ. Then

$$K = \{x \in R : [xs, s] = [0, s'] \iff uxss' = 0 \text{ for some } u \in S\}.$$

Note that K may or may not be trivial, depending on the choice of S. Let $R = \mathbb{Z}_6$, $S = U_6$ and $S' = U_6 \cup 3$. Both the S and S' are multiplicative system of R. If we choose S, we get the trivial kernel $K = (0)$ so that R can be imbedded to R_S, but if we choose S', setting $s, s' = 1$, then for the equation $3x = 0$ we have $x = 0, 2 \in K$, so that $K \supsetneq (0)$. Hence, appropriate choice of S is required for the imbedding of R into R_S ☐

e) Prove that this kernel has no element of S in it.

Proof. If there is some $t \in S$ such that $t \in K$, then it must satisfy the equation $utss' = 0$ for some $u, \in S$ and each $s, s' \in S$. But the product of elements in S cannot be 0, so it is a contradiction. $\square$

f) Prove that every element of the form $[s_1, s_2]$(where $s_1, s_2 \in S$) in R_S has an inverse in R_S.

Proof. Note that for each $s_1, s_2 \in S$, $[s_1, s_2] \cdot [s_2, s_1] = [s, s]$ where $s = s_1 s_2 \in S$. Since every unit element in R_S is of the form $[s, s]$, $[s_2, s_1]$ is the inverse element for every $[s_1, s_2]$. $\square$

6. Let D be an integral domain, $a, b \in D$. Suppose that $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n. Prove that $a = b$.

Proof. Since m and n are relatively prime positive integers, without loss of generality, there exists two integers $\lambda > 0$, $\mu < 0$ such that $m\lambda + n\mu = 1$. Thus,

$$a \cdot a^{(-\mu)n} = a^{m\lambda} = b^{m\lambda} = b \cdot b^{(-\mu)n} = b \cdot (b^n)^{(-\mu)} = b \cdot (a^n)^{(-\mu)} = b \cdot a^{(-\mu)n},$$
$$a \cdot a^{(-\mu)n} = b \cdot a^{(-\mu)n} \iff (a-b)a^{(-\mu)n} = 0.$$

Recall that D is an integral domain. If $a^{(-\mu)n} = 0$, then it forces us that $a = 0$. Hence, $a = b = 0$. If $a^n \neq 0$, it forces us that $a - b = 0$ so that $a = b$. Hence, in either cases, $a = b$. $\square$

7. Let R be a ring, possibly noncommutative, in which $xy = 0$ implies $x = 0$ or $y = 0$. If $a, b \in R$ and $a^n = b^n$ and $a^m = b^m$ for two relatively prime positive integers m and n, prove that $a = b$.

Proof. Exact same proof for the Problem 6 can be applied here; Hence proved. $\square$