Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 16, 2020

Problems in Section 3.7.

1. In a commutative ring with unit element prove that the relation a is an associate of b is an equivalence relation.

Proof. (Reflexive) For $a \in R$, $a = 1 \cdot a$ so that $a \sim a$.
(Symmetry) For $a, b \in R$, if $a \sim b \iff b = ua$ for some unit u, $uk = 1$ for some unit $k \in R$ and consequently, $kb = kua = (uk)a = a$. Hence, $b \sim a$. So from now on, we can make use of the term u^{-1} for the inverse of unit u in R.
(Transitive) For $a, b, c \in R$, if $a \sim b$ and $b \in c$ then $b = ua$, $c = kb$ for some units u, k in R. Consequently, $c = kb = k(ua) = (ku)a$. Note that product of unit is still an unit, so that $a \sim c$. $\square$

2. In a Euclidean ring prove that any two greatest common divisors of a and b are associates.

Proof. Apply Lemma 3.7.2. Then the result is straightforward. $\square$

3. Prove that a necessary and sufficient condition that the element a in the Euclidean ring be a unit is that $d(a) = d(1)$.

Proof. Suppose a is an unit in R. Then $ab = 1$ for some $b \in R$. Hence, $d(a) \leq d(ab) = d(1)$. Since $d(1) \leq d(1 \cdot a) = d(a)$, $d(1) = d(a)$. Conversely, if $d(a) = d(1)$. Suppose a is not an unit. Then by Lemma 3.7.3, $d(1) < d(1 \cdot a) = d(a)$, which is a contradiction. Hence, a must be an unit. $\square$

4. Prove that in a Euclidean ring (a, b) can be found as follows:

$$\begin{aligned}
b &= q_0 a + r_1, \quad \text{where} \quad d(r_1) < d(a) \\
a &= q_1 r_1 + r_2, \quad \text{where} \quad d(r_2) < d(r_1) \\
r_1 &= q_2 r_2 + r_3, \quad \text{where} \quad d(r_3) < d(r_3) \\
&\vdots \qquad\qquad\qquad\qquad\qquad \vdots \\
r_{n-1} &= q_n r_n
\end{aligned}$$

and $r_n = (a, b)$.

Proof. We claim that (a, b) equals (r_1, a)(upto associates). Note that $r_1 = b - q_0 a$ and $(a, b) \mid b - q_0 a$ so that $(a, b) \mid r_1$. It is also trivial that $(a, b) \mid a$, and hence $(a, b) \mid (r_1, a)$. Conversely, $(r_1, a) \mid r_1, a$ and hence $(r_1, a) \mid (q_0 a + r) = b$ so that $(r_1, a) \mid (a, b)$. Hence $(a, b) = (r_1, a)$ upto associates. We repeat this process until one of the elements in the tuple (r_k, r_{k-1}) terminates with 0(this is always the case since $d(a)$ is finite). So we obtain

$$(a, b) = (r_1, a) = (r_2, r_1) = \cdots = (r_{n-1}, r_{n-2}) = (r_n, r_{n-1}) = (0, r_n) = r_n$$

so that $r_n = (a, b)$. □

5. Prove that if an ideal U of a ring R contains a unit of R, then $U = R$.

Proof. If a is an unit of R and $a \in U$, then $a^{-1} a = 1 \in U$ so that $U = R$. □

6. Prove that the units in a commutative ring with a unit element form an abelian group.

Proof. Let U be the set of all units in commutative ring R. Then clearly U is closed under associative product. The unit element 1 is the multiplicative identity of U. Let $u \in U$ and consider its multiplicative inverse u^{-1}. Since $u^{-1} u = 1$, u^{-1} is also an unit so that $u^{-1} \in R$. Thus, U is a commutative multiplicative group in R. □

7. Given two elements a, b in the Euclidean ring R their least common multiple $c \in R$ is an element in R such that $a \mid c$ and $b \mid c$ and such that whenever $a \mid x$ and $b \mid x$ for $x \in R$ then $c \mid x$. Prove that any two elements in the Euclidean ring R have a least common multiple of R.

Proof. Let us define a set $I = \{c \in R : a \mid c,\ b \mid c\}$. We claim that I is an ideal in R. For any $x, y \in I$, $a \mid (x + y)$ and $b \mid (x + y)$ clearly. Also, for any $r \in R$, $a \mid xr, rx$ so that I is now an ideal in R. Since R being an Euclidean ring and hence a Principal Ideal Domain, $I = (c)$ for some $c \in R$. We now claim that c is the required least common multiple of a and b. By the definition, $a \mid c$ and $b \mid c$ clearly. Suppose $a \mid x$ and $b \mid x$ for some $x \in R$. Then $x \in I$. Hence, x is represented as a multiple of c, that is, $c \mid x$. Hence, c is the least common multiple of a and b. □

8. In Problem 7, if the least common multiple of a and b is denoted by $[a, b]$, prove that $[a, b] = ab/(a, b)$.

Proof. Let $d = (a, b)$. Thus $a = dk_1$, $b = dk_2$ for some $k_1, k_2 \in R$. Note that k_1 and k_2 are relatively prime, otherwise d is no more a greatest common divisor of a and b. We claim $[a, b] = dk_1 k_2$. Let $c = dk_1 k_2$. Then clearly $a \mid ak_2 = c$, $b \mid bk_1 = c$. Suppose $a \mid x$ and $b \mid x$ for some $x \in R$. Then $au_1 = x$, $bu_2 = x$ for some $u_1, u_2 \in R$. From $au_1 = bu_2$, $dk_1 u_1 = dk_2 u_2 \iff k_1 u_1 = k_2 u_2$. Hence, $k_1 \mid k_2 u_2$. We know that $(k_1, k_2) = 1$

so that $k_1 \mid u_2$. Consequently, $c = dk_2k_1 = bk_1 \mid bu_2 = x$ so that c is the required least common multiple of a and b. Recall that $c = dk_1k_2$ and $dk_1k_2 = ab/(a, b)$. Therefore, $[a, b] = ab/(a, b)$. □