Problems and Comments for Section 17, 18, and 21

~

Problems: 17.6, 17.7, 18.1 (a), (b), (c), 21.11, 21.12

Comments (**and synopsis for these sections**): You should read 17 and 18 simultaneously. You may stop reading section 18 after the examples for Theorem 18.5.

Add in the definition of a ring homomorphism the condition

iii) $\varphi(1_R) = 1_S$

because all rings should have a unit.

The kernel of a ring homomorphism $\varphi : R \to S$ is the set of all elements of R which are mapped to the zero of S. By what we have learned about group homomorphisms, $\ker(\varphi)$ must be a subgroup I of $(R,+,-,0)$. Moreover, if $\varphi(a) = 0$ and if b is any element in R then $\varphi(ba) = \varphi(ab) = 0$. That is, if $a \in I$ and if $b \in R$ then $ab \in I$ and $ba \in I$. This is how ideals are defined. If I is an ideal then the group $(R/I,+,-,0 = I)$ is also a ring under "representative wise" multiplications (see Theorem 17.3). The multiplicative unit is the class of 1, that is $1 + I$. If I is the ideal (that is the kernel) for a homomorphism φ then the ring $R/I \cong im(\varphi)$. That is the homomorphism theorem for rings, Theorem 18.5

If an ideal I contains an element a which has an inverse a^{-1} then $a^{-1}a = 1 \in I$, hence $I = R$

If $\mathbf{F}$ is a field and $I \neq 0$ an ideal of $\mathbf{F}$ then $I = \mathbf{F}$.

Assume that R is commutative and R/I is a domain. That is, whenever $(a+I)(b+I) = ab + I = I$, one has that $(a+I) = I$ or $(b+I) = I$. Thus $ab \in I$ iff $a \in I$ or $b \in I$. Such ideals are called *prime* ideals. The converse is also easy to see, that is R/I is a domain if I is prime.

Let I be any ideal of the commutative ring R. Let $a \in R$. Then $J = I + (a) = \{i + ab | i \in I, b \in R\}$ is an ideal, actually the smallest ideal that contains I and a.

An ideal M is called *maximal* if $M \neq R$ and if for any ideal $I \supseteq M$ one has that $I = M$ or $I = R$.

If M is maximal and $a \notin M$ then $M + (a) = R$. Hence $m + ab = 1$ for some $m \in M$ and $b \in R$.

Now, $(a+M)$ is not the zero in R/M is equivalent to $a \notin M$. By what we just said, one has some b and m such that $m + ab = 1$. But this is: $(a+M)(b+M) = (ab+M) = 1 + M$. Hence every element $(a+M) \neq 0$ of R/M has an inverse $(b+M)$. We proved:

If M is a maximal ideal of the commutative ring R then R/M is a field.

Now, if R/I is a field then every class $(a+I) \neq I$ has an inverse $(b+I)$. Thus $(a+I)(b+I) = 1 + I$. This is $ab - 1 = i$ for some $i \in I$. We conclude that $I + (a)$ contains 1 if $a \notin I$. Hence I has to be maximal.

A (commutative) domain D is called a principal ideal domain (PID) if every ideal is principal. $\mathbb{Z}$ and polynomial rings, like $\mathbb{R}[x]$ are PId's.

For domains the divisibility relation is all important:

$$a|b \text{ iff } a \cdot q = b \text{ for some } q \in D \text{ iff } (a) \supseteq (b)$$

Every element $a \in D$ has trivial divisors: a and 1.

We have that $a|b$ and $b|a$ iff $b = ea$ and $a = fb$. Hence $a = fea$ This is $fe = 1$ because D is a domain. Hence a and b differ only by an invertible element. In this case we say that a and b are associates and write $a \sim b.$ For example, in $\mathbb{Z}$ one has that $a \sim \pm a$ because 1 and -1 are the only elements which have an inverse.

One always has $a|0$, that is with respect to divisibility, 0 is the largest element and because $1|a$, 1 is the smallest element.

An element $q \in D$ is called *irreducible* if q has only tivial divisors. Trivial divisors of an element a are all $e \sim 1,$ that is the invertible elements, and $a' \sim a$.

An element $p \in D$ is called *prime* if whenever $p|ab$ one has that $p|a$ or $p|b$.

Remark *A prime element is irreducible.*

Proof Assume that $p = a \cdot b$. Because $p \cdot 1 = a \cdot b$ we have that $p|a \cdot b.$ Hence $p|a$ or $p|b.$ On the other hand, $p = a \cdot b$ tells us that $a|p$ and $b|p.$ Thus $a \sim p$ or $b \sim p$.

Theorem *In a PID, every irreducible element is prime.*

Proof That q is irreducible means that (q) is a maximal ideal. Hence $D/(q)$ is a field, thus a domain. So (q) is a prime ideal and (easy to see), q has to be prime.

Theorem *In a PID, every ascending chain $I_1 \subseteq I_2 \subseteq \ldots$ of ideals is finite. That is for some k one has that $I_k = I_{k+1} = \ldots$*

Proof It is quite obvious that the union of an ascending chain of ideals is an ideal. Thus $\bigcup I_n = I = (d).$ If $d \in I_k$ then all ideals are equal from k on.

Theorem *Let a be a non invertible element of the PID D. Then there is some irreducble p which divides a.*

Theorem *If a is not irreducible then it has a proper divisor a_1. Thus $(a) \subset (a_1)$. If $a_1$is irreducible, we are done. Otherwise, a_1 has a proper divisor a_2 and we have $(a_1) \subset (a_2)$. If If a_2 is irreducible, we are done. Otherwise, a_2 has a proper divisor a_3 and we have $(a_2) \subset (a_3)$. By the previous theorem, this has to stop at some point. Thus a has an irreducible divisor $q = a_k$.*

Theorem *In a PID, any non invertible element a different from zero is a product of irreducible elements. The factorization is essentially unique.*

Proof The element $a \neq 0$ has an irreducible divisor p_1. If $q_1 = a/p_1$ is invertible, we are done. Otherwise q_1 has an irreducible divisor p_2. If $q_2 = q_1/p_2 = a/p_1p_2$ is invertible, we are done. Otherwise q_2 has an irreducible divisor p_3. If $q_3 = q_2/p_3 = a/p_1p_2p_3$ is invertible, we are done.....Notice that $\ldots q_3|q_2|q_1$or $(q_1) \subset (q_2) \subset (q_3) \subset \ldots$ Hence for some k we must have that $q_k = a/p_1p_2p_3\ldots p_k = \epsilon$ is an invertible element, hence $a = (\epsilon p_1)p_2p_3\ldots p_k$ where ϵp_1 as an associate of p_1 is also irreducible.

Assume that

$$a = p_1p_2p_3\ldots p_k = q_1q_2q_3\ldots q_l$$

then $k = l$ and after some re-enumeration one has that $p_i \sim q_i$.

This follows from the fact that irreducible elements are prime. Thus, because $p_1|q_1(q_2q_3\ldots q_l)$ we have that $p_1|q_1$ or $p_1|q_2(q_3\ldots q_l)$. If$p_1|q_1$ then becasue q_1 is irreducible one has that $p_1 \sim q_1$. Otherwise $p_1|q_2$ which leads to $p_1 \sim q_2$ or $p_1|q_3(\ldots q_l)$. If $p_1|q_3$ then because q_3 is irreducible one has that $p_1 \sim q_3$. hence, we must get $p_1 \sim q_j$ for some $j \leq l$. After some re-arrangement of the $q's$ we can assume that $j = 1$. We cancel on both sides p_1 and continue or finish by induction.