Algebra 1 Assignment 9 Solutions

Problem 1 In the ring $\mathbb{Z}$, we have the prime ideals (2) and (3), but their intersection is the principal ideal (6) which is not prime.

The following theorem is extremely useful:

Theorem 1 *Let R and let $P \subset R$ be an ideal, then R/P is an integral domain if and only if P is a prime ideal.*

Proof: Let $\pi : R \longrightarrow R/P$ be the natural surjection and denote $\pi(r) = \bar{r}$.
($\Rightarrow$) Suppose towards a contradiction that R/P is an integral domain, but that P is not a prime ideal. P not prime $\Rightarrow$ there exist $, r, s \in R$ such that $r, s \notin P$ but that $rs \in P$. $r, s \notin P \Rightarrow \bar{r} \neq \bar{0} \neq \bar{s}$, bur $rs \in P \Rightarrow \bar{0}\overline{rs} = \bar{r}\bar{s}$ contradicting our assumption that R/P was an integral domain.
($\Leftarrow$) Suppose now that P is a prime ideal. Suppose $\bar{r}, \bar{s} \neq 0(\star)$. Then there exist $r, s \in R$ such that $\pi(r) = \bar{r}, \pi(s) = \bar{s}$. By $(\star)$ we get $r, s \notin P$. P is a prime ideal so $rs \notin P \Rightarrow \overline{rs} = \bar{r}\bar{s} \neq \bar{0}$. So R/P is an integral domain. $\square$

Here are two more useful results that one should automatically pop up in one's head when one see the appropriate buzzwords...

Theorem 2 *Let $M \subset R$ be an ideal then R/M is a field $\Leftrightarrow$ M is a maximal ideal.*

Theorem 3 *If R is a principal ideal domain, i.e. all its ideals are principal, and $I \subset R$ is an ideal, then I prime $\Leftrightarrow$ I maximal.*

Problem 2 Note that $R \approx R/\{0\}$ (I write $\approx$ for "isomorphic") so by the theorem that was just proven, it follows immediately that R is an integral domain $\Leftrightarrow$ $\{ 0 \}$ is a prime ideal.

Problem 3 Let R be a ring and let $P \subset R$ be a nonzero proper prime ideal. Let $x \notin P$. Then the elements $(x, 0), (0, x)$ are clearly not in

$$I = P \times P = \{(p, q) \in R \times R | p, q \in P\}$$

However it is important to recal that *every ideal* contains zero so $(x, 0)(0, x) = (0, 0) \in I$ so I is not a prime ideal.

Problem 4 Let $\varphi : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ be the surjective homomorphism given by the rule $\varphi((a, b)) = a$. Let $I = \ker(\varphi)$, then we have by the first isomorphism theorem that $(\mathbb{Z} \times \mathbb{Z})/I \approx \mathbb{Z}$. Now $\mathbb{Z}$ is an integral domain but not a field, so I is prime but non maximal.

Problem 5 Let R be a commutative ring and let $F[x]$ be the ring of polynomial over the *field* F. Let $f : R \longrightarrow F[x]$ be a ring homomorphism. Then the image (or range) of f, $f(R) \subset F[x]$ is a subring of $F[x]$ and the map $f : R \longrightarrow f(R)$

is surjective. By the first isomorphism theorem, $f(R) \approx R/\ker(f)$ $(\star)$. On the other hand, $F[x]$ is an integral domain so the same must be true of its subrings. (Suppose not then for some subring $S \subset F[x]$ there are nonzero elements $r, s \in S$ such that... contradiction.) So $f(R)$ is an integral domain so by $(\star), \ker(f)$ must be a prime ideal.

Problem 6 Let F be a field, we check the group axioms for $G = F - \{1\}$ equipped with the binary operation $*$.

1. For any $a \in G$ we have:

$$0 * a = 0 + a - 0 \times a = 0$$

   G has an identity element, 0.

2. Let $a \in G$ be arbitrary, then we can solve for b such that $a * b = 0$ indeed,

$$\begin{aligned} a * b = 0 &\Leftrightarrow \\ a + b - ab = 0 &\Leftrightarrow \\ b - ab = -a &\Leftrightarrow \\ b = \tfrac{-a}{1-a} &\text{ which is well defined because } a \neq 1 \end{aligned}$$

   So it follows that every element has an inverse.

3. We finally verify $(a * b) * c = a * (b * c)$.

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

So $(G, *)$ is a group.

The next two problems are counting problems, the next three facts are key:

1. Any $\sigma \in S_n$ can be essentially uniquely written as a product of disjoint cycles.
2. A k-cycle, i.e. some $\sigma = (123\ldots k) \in S_n$, has order k, i.e. $\sigma^k = 1$.
3. Disjoint cycles commute

From this we get that the order of an element $\sigma \in S_n$ is determined by the "shape" of its cycle decomposition. e.g.

$$\sigma = \underbrace{(123)}_{=x}\underbrace{(45678)}_{=y}$$

Then since x and y are disjoint we have that they commute so $\sigma^n = (xy)^n = x^n y^n$. It follows that the order of σ is $\operatorname{lcm}(3, 5) = 15$.

Problem 7 It is fairly clear that that the only elements of order 3 in S_3 are three cycles, first we count how many "different looking" three cycles there are

$$\begin{array}{ccccccc} (& * & & * & & * &) \\ & \uparrow & & \uparrow & & \uparrow & \\ & \text{3 choices} & & \text{2 choices} & & \text{1 choice} & \end{array}$$

and since every 3-cycle has 3 different presentations e.g.$(123) = (231) = (312)$ then we divide through our result by three (to avoid counting a cycle more than once) we find that there are $3!/3 = 2$ elements of order 3 in S_3.

Problem 8 An element of order six is either a 6-cycle or a product disjoint of 2-cycles and 3-cycles, adopting the convention of writing shorter cycles on the left (to avoid counting things more than once) we have that elements of order 6 in S_5 look like

$$(**)(***)$$

We immediately see that there are $5\times4\times3\times2\times1 = 5!$ different looking products of this form. Now each 2-cycle has 2 presentations and every 3-cycle has three presentations, so there are $5!/(2 \times 3) = 20$ distinct elements of order 6 in S_5.

For the record, counting problems are notoriously tricky, it's easy to forget to divide by something or add things instead of multiplying, but it sure beats checking all 120 elements of S_5.

Problem 9 First notice that any ring is a group under the binary operation $+$. Indeed, zero is our identity element, each element has an inverse (i.e. its additive inverse) and associativity holds. So for any $n \in N$ $(\mathbb{Z}_n, +)$ is a group with n elements.

Now if G and H are groups finite then $G \times H$ the cartesian product is a group with $\text{order}(G) * \text{order}(H)$ elements (count the possibilities). Also the subset $S = \{(g, 1_H) \in G \times H | g \in G\}$ is in fact a subgroup of $G \times H$ that is isomorphic to G (these two claims should be checked).

If a group G is abelian, i.e. for all $x, y \in G, xy = yx$, then all its subgroups must also be abelian.

Now S_3 is a nonabelian group, $(12)(23) = (123) \neq (132) = (23)(12)$, with 6 elements (in fact it is the smallest possible nonabelian group). And the groups $S_3 \times \mathbb{Z}_2$ and $S_3 \times \mathbb{Z}_5$ are groups with orders 12 and 30 respectively and since they have nonabelian subgroups they themselves are nonabelian.

Other examples (with completely different structures) are the groups of symmetries (i.e. reflections and rotations) of a hexagon, D_{12} (though some will write D_6 instead), and a regular polygon with 15 edges, D_{30}. One may check that they have the right number of elements and verify that rotation and reflection do not commute by making the polygons out of construction paper, numbering the vertices and applying the said symmetries.