Problem Set 4 - Thomas Boyko - 30191728

1. Let $(r, +, \cdot)$ be a ring. Recall, an element $x \in R$ is called idempotent if $x^2 = x$. Suppose every element in R is an idempotent. Such a ring is called a Boolean ring.

   (a) Show that $\mathsf{char}(R) = 2$.
   Recalling that $\mathsf{char}(R)$ is the order of the multiplicative identity with respect to addition in R, we can immediately rule out 1 from being the characteristic of R; $1^1 = 1 \neq 0$.
   And from distributive laws we can see that:

   $$1 + 1 = (1 + 1)^2 = (1 + 1)(1 + 1) = 1(1 + 1) + 1(1 + 1) = 1 + 1 + 1 + 1.$$

   And using additive inverses, $1 + 1 = 0$ and $\mathsf{char}R = 2$.

   (b) Show that R must be commutative.
   Take $a, b \in R$. (Since $\mathsf{char}R = 2$, a prime, R is an integral domain.)

   $$\begin{aligned}(a + b) &= (a + b)^2 \\ &= a^2 + ab + ba + b^2 \\ &= a + ab + ba + b \\ 0 &= ab + ba \\ ab &= -ba.\end{aligned}$$

   Well it sure would be convenient to show that each element is its own additive inverse. If this is true for 1 why wouldn't it be true for any element?
   Take $x \in R$. $x + x = 1x + 1x = x(1 + 1) = x0 = 0$. Wow! That was easy. So any element in R is its own inverse, and since $ab = -ba$, $ab = ba$ and R is commutative.

   (c) For any non-empty set X, let $P(X)$ denote its power set. Consider the ring $(P(X), \Delta, \cap)$. Show that it is Boolean ring.
   We already know from Problem Set 1 that $(P(X), \Delta)$ is a group. So we must show that $\cap$ is associative , maintains closure, has identity and that it distributes over Δ.
   Our identity for $\cap$ is X. Since any element $A \in P(X)$ must be a subset of X, every element of A is also in X. From this we can see that $X \cap A \subseteq A \subseteq X \cap A$ So, $X \cap A = A = A \cap X$ and X is identity under $\cap$.
   Now to show associativity, take $A, B, C \in P(X)$. Let $x \in A \cap (B \cap C)$. Then x must be in $A, B,$ and C. From this we can say $x \in (A \cap B) \cap C$, and the same logic works the other way. So $(A \cap B) \cap C = A \cap (B \cap C)$.
   Now we show the distributive property. Start by showing $(A \cap B)\Delta(A \cap C) \subseteq A \cap (B\Delta C)$. Let $x \in A \cap (B\Delta C)$. Then x is in A and x is in B or C, but not both. Suppose without loss of generality that $x \in B \setminus C$. then $x \in A \cap B$ but $x \notin A \cap C$. Since x is in one of these sets but not both, it is in their symmetric difference, and $x \in (A \cap B)\Delta(A \cap C)$. The other case is identical. So $A \cap (B\Delta C) \subseteq (A \cap B)\Delta(A \cap C)$.
   Now to show the other way. Suppose $x \in (A \cap B)\Delta(A \cap C)$. Then x must be in $A \cap B$ or $A \cap C$ but not both. Since both sets require $x \in A$, we know $x \in A$ either way. From this we infer that x must be in B or C but not both. So $x \in B\Delta C$. Combining these, $x \in A \cap (B\Delta C)$. So our sets are equal and $\cap$ distributes over Δ.
   Therefore $(P(X), \Delta, \cap)$ is a ring.
   To show that $P(X)$ is a boolean ring simply requires showing that $A \cap A = A$. If $a \in A$, then a is in A and A, so $a \in A \cap A$, $A \subseteq A \cap A$. And if $a \in A \cap A$, then a is in A, $A \cap A \subseteq A$.
   So $P(X)$ is a boolean ring.

2. Let R be a commutative ring and I be an ideal of R.

   (a) Define the radical of I as $\sqrt{I} = \{a \in R : a^n \in I \text{ for some integer } n > 1\}$. Show that $\sqrt{I}$ is an ideal of R, containing I.
   Subgroup: Let $x, y \in \sqrt{I}$. Then there exist $m, n \in Z_{>1}$ so that $x^m = 0$ and $y^n = 0$. Consider the following binomial expansion, since R is commutative.

   .

And either $mn - k > m$ or n, otherwise $k > m$ or $k > n$, and so one of our two coefficients will become zero in each term of the expansion. So $(\sqrt{I}, +)$ is a subgroup of $(R, +)$.
Now we show that $I \subseteq \sqrt{I}$. Let $i \in I$. Then $i^1 = i$ must be in $\sqrt{I}$.
Let $a \in \sqrt{I}$ and $r \in R$. Then by definition of $\sqrt{I}$, we know there exists some $n \in \mathbb{Z}_{>1}$ so that $a^n \in I$. Then consider $(ar)^n = a^n r^n$ since R is commutative. Since a^n is in I, an ideal, $(ar)^n \in I$, and by definition of $\sqrt{I}$, $ar \in \sqrt{I}$. So $\sqrt{I}$ is an ideal of R containing I.

(b) Show that if I is a maximal ideal, then $\sqrt{I} = I$.
Let I be maximal. Then since $I \subseteq \sqrt{I} \subseteq R$, either $\sqrt{I} = R$ or $\sqrt{I} = I$. If $\sqrt{I} = R$, then $1 \in \sqrt{1}$ which would mean for some $n \in \mathbb{Z}_{>1}$, $1^n \in I$, which would have $I = R$, a contradiction by the definition of ideal.

(c) The set of all prime ideals of R is denoted by Spec(R). Show that

$$\sqrt{\{0\}} \subseteq \bigcap_{P \in \mathrm{Spec}(R)} P.$$

Let $a \in \sqrt{\{0\}}$. Then $a^n = 0$ for some $n \in \mathbb{Z}_{>1}$. To show the above, we must show that a is any prime ideal of R. Let P be a prime ideal in R. Then $0 \in P$ since P is a subgroup of $(R, +)$ and must contain additive identity. And $a^{n-1}a = 0$, so since P is a prime ideal, a^{n-1} or a must be in P.
If $a^{n-1} \in P$, then we split off another a, writing $aa^{n-2} \in P$. Again, one of these must be in P, and we can continue until this happens, or untill we obtain $n - k = 1$, since $n > 1$.

3. Let R be a commutative ring and R[x] denote the ring of polynomials with coefficients in R.

(a) For $\alpha \in R$, define the evaluation map, $ev_\alpha : R[x] \to R$ by $ev_\alpha(f(x)) = f(\alpha)$. Show that it is a ring homomorphism.
Let $f(x), g(x) \in R[x]$, so that $f(x) = a_0 + a_1 x + \ldots$, $g(x) = b_0 + b_1 x + \ldots$. Then:

$$\begin{aligned} ev_0(f(x) + g(x)) &= ev_0(a_0 + b_0 + (a_1 + b_1)x + \ldots) \\ &= a_0 + b_0 + (a_1 + b_1)\alpha + \ldots \\ &= a_0 + a_1\alpha + \ldots + b_0 + b_1\alpha + \ldots \\ &= ev_\alpha(f(x)) + ev_\alpha(g(x)). \end{aligned}$$

So ev_α preserves addition.

$$\begin{aligned} ev_\alpha(f(x)g(x)) &= ev_0(\sum_{k=1}^{\max\{m,n\}} \sum_{i+j=k} x^k a_i b_j \\ &= ev_\alpha(\sum_{k=0}^{\max\{m,n\}} \sum_{i+j=k} x^k a_i b_j) \\ &= ev_\alpha(\sum_{k=0}^{\max\{m,n\}} x^k \sum_{i+j=k} a_i b_j) \\ &= \sum_{k=0}^{\max\{m,n\}} \alpha^k \sum_{i+j=k} a_i b_j \qquad = \sum_{k=0}^{\max\{m,n\}} \sum_{i+j=k} \alpha^k a_i b_j = f(\alpha)g(\alpha) \\ &= ev_\alpha(f)ev_\alpha(g) \end{aligned}$$
.

So ev_α is a ring homomorphism.

(b) For $\alpha = 0$, what is the $\ker(ev_0)$?
Claim: $\ker(ev_0) = \{a_1 x + a_2 x^2 + \ldots \in R[x]\}$, or the set of all polynomaials with a zero constant coefficient.
Let $f(x) \in \{a_1 x + a_2 x^2 + \ldots \in R[x]\}$. Then $f(x) = a_1 x + a_2 x^2 + \ldots$ where $a_i \in R$. Then $f(0) = a_1 0 + a_2 0^2 + \ldots = 0$ and $f \in \ker(ev_0)$.

(c) Is $\ker(ev_0)$ a prime ideal? Is it maximal? What extra condition do you need to impose on R, for this ideal to be prime or, maximal?

$\ker(ev_0)$ is a prime ideal when R is a domain. To show this, let $f(x)g(x) \in \ker(ev_0)$. Then we know that the constant term of fg must be zero. We know the constant term of fg to be $\sum_{i+j=0} a_i b_j$, assuming that coefficients of f are given by a_i and g given by b_j. Then $a_0 b_0$ must be zero, which is true for all f and g only in a domain.

$\ker(ev_0)$ is maximal when $\operatorname{Im}(ev_0)$ is a field. From the first isomorphism theorem, and since ev_0 is a homomorphism, we know that $R[x]/\ker(ev_0) \cong \operatorname{Im}(ev_0)$. And when $\operatorname{Im}(ev_0)$ is a field, we know that $\ker(ev_0)$ must be maximal.

4. (a) Let $\varphi : R \to S$ be a ring homomorphism. Show that for any ideal $J \subseteq S$, the preimage $\varphi^{-1}(J) = r \in R : \varphi(r) \in J$ is an ideal of R. (That is, the preimage of an ideal under a ring homomorphism is an ideal.)

First we show that $\varphi^{-1}(J)$ is a subgroup of R. Clearly $0 \in \varphi^{-1}(J)$ since $\phi(0) = 0$.

Let $a, b \in \varphi^{-1}(J)$. Then $\varphi(a - b) = \varphi(a) - \varphi(b)$ since φ is a homomorphism. And since $\varphi(a), \varphi(b)$ are in J, $\varphi(a - b) \in J$. So $\varphi^{-1}(J)$ is a group w.r.t +.

Let $\varphi : R \to S$ be a ring homomorphism and $J \subseteq S$. Then let $i \in \varphi^{-1}(J)$. Then for some $j \in J$, $\varphi(i) = j$. Let $r \in R$, and suppose $\varphi(r) = s$. Since J is an ideal of S, $\varphi(ri) = \varphi(r)\varphi(i) = js \in J$. So $ri \in \varphi^{-1}(J)$, and φ^{-1} is an ideal of J.

(b) Show that the image of an ideal under an onto ring homomorphism is an ideal. (That is, if $\varphi : R \to S$ is an onto ring homomorphism, then for any ideal I of R the image $\varphi(I) = \varphi(r) : r \in I$ is an ideal of A.)

Begin by showing that $\varphi(I)$ is a subgroup of $(S, +)$. Clearly since $0 \in I$ (since I is a subgroup of $(R, +)$. So $\varphi(0) = 0 \in \varphi(I)$.

Now let $a, b \in \varphi(I)$. Then there exists $c, d \in I$ so that $\varphi(c) = a$ and $\varphi(d) = b$. And since φ is a homomorphism $a - b = \varphi(c) - \varphi(d) = \varphi(c - d) \in \varphi(I)$, and $\varphi(I)$ is a subgroup of $(S, +)$.

Let $i \in I$ so that $\phi(i) = j \in S$. Then let $s \in S$. We know since φ is onto that there exists $r \in R$ so that $\varphi(r) = s$. Then $js = \varphi(i)\varphi(r) = \varphi(ir)$ since φ is a homomorphism. And $ir \in I$ since i is in the ideal I. And since js is the image of ir under φ, $js \in \varphi(I)$ and $\varphi(I)$ is an ideal of S.

(c) Give an example which shows that the image of an ideal under a ring homomorphism need not be an ideal if the map is not onto.

Consider the given mapping $f : \mathbb{Z} \to \mathbb{Q}, f(x) = x$, where $\operatorname{Im} f = \mathbb{Z}$, which is not an ideal for $\mathbb{Q}$ since given $\frac{1}{2} \in \mathbb{Q}$, and $3 \in \mathbb{Z}$, $\frac{3}{2} \notin \mathbb{Q}$. So the image of $\mathbb{Z}$, which is an ideal for $\mathbb{Z}$, is not an ideal of $\mathbb{Q}$.

(d) Prove that if I is an ideal of a ring R, there is an inclusion preserving bijection between the ideals of R/I and the ideals of R which contain I.

Proof. Let I be an ideal of R. Consider $\pi : R \to R/I\ \pi(r) = r + I$, and $\Gamma : \{idealsJofRsuchthatI \subseteq J\} \to \{idealsofR/I\}$

$\square$

my statistics group will be more mad at me if i dont finish that assignment than i will be at myself not finishing this one so i think im done here :p