WORKSHEET # 6

MATH 435 SPRING 2011

In this worksheet we will learn about subrings.

We will follow the books' (Rotman's) notation. In particular, *ALL* rings will be commutative, associative, and with multiplicative identity.

Definition 0.1. Given a ring R a subring $T \subseteq R$ is a ring T such that T's multiplication and addition operation are just those from R. We also assume that the multiplicative identity of T is equal to the multiplicative identity of R.

Notice that with our definition (at least in this worksheet), a subring is also commutative, associative, and has an identity.

1. Suppose that $\{0\} \neq T \subseteq R$ is a subring of R, an integral domain. Show that T is also an integral domain.

Solution: Choose elements $x, y \in T$ and suppose $xy = 0$. Then since $x, y \in R$ also, and R is an integral domain, either $x = 0$ or $y = 0$. But this means that T is an integral domain as well.

2. Which of the following subsets are subrings and which are not. Notice you will get different answers if you use Gallian's definition (which does not require subrings to have identity) instead of Rotman's definition (which does).

$\mathbb{Z} \subseteq \mathbb{Q}$

Solution: Subring

$3\mathbb{Z}_{\text{mod } 12} \subseteq \mathbb{Z}_{\text{mod } 12}$

Solution: Not a subring, missing the overring's multiplicative identity.

$\mathbb{Z} \oplus \mathbb{Q} \subseteq \mathbb{Q} \oplus \mathbb{Q}$

Solution: Subring

$\{0\} \oplus \mathbb{Z} \subseteq \mathbb{Z}_{\text{mod } 2} \oplus \mathbb{Z}$

Solution: Not a subring, missing the overring's multiplicative identity

$\mathbb{C}[x^2, y] \subseteq \mathbb{C}[x, y]$

Solution: Subring

3. Find an example of two rings $R \subseteq S$ such that R and S both have the same addition and multiplication operation, and both have multiplicative identities, but that $1_R \neq 1_S$.

Solution: $3\mathbb{Z}_{\text{ mod } 12} \subseteq \mathbb{Z}_{\text{ mod } 12}$. I claim that $9 \in 3\mathbb{Z}_{\text{ mod } 12}$ is a multiplicative identity. Certainly $(9)(3) = 27 \equiv 3 \mod 12$, $(9)(6) = 54 \equiv 6 \mod 12$, $(9)(9) = 81 \equiv 9 \mod 12$ and $(9)(0) = 0 \equiv 0 \mod 12$ which proves that 9 is the multiplicative identity of the first ring. Of course it's not the multiplicative identity of the second ring.

When dealing with subgroups, one of the primary things we did with them was form quotient groups. In this half of the worksheet we first explore whether we can do the same sort of construction with subrings. The answer is a resounding *NO*!

4. Suppose that R is a ring and $T \subseteq R$ is a subring. Since R is an Abelian group (under addition), T is automatically a normal subgroup of R (under addition) and so we can form the quotient Abelian group R/T. The elements are then the cosets $r + T$ for $r \in R$.

Try (and fail) to prove that the following multiplication operation is well defined.

$$(r + T)(r' + T) = (rr') + T$$

Solution: Suppose that $r+T = s+T$ and $r'+T = s'+T$. Thus we have $s = r+t$ and $s' = r'+t'$ for some $t, t' \in T$. We then would like to show that

$$(rr') + T = (ss') + T = (s + T)(s' + T) = ((r + t) + T)(r' + t') + T) = ((r + t)(r' + t')) + T$$

If we can show this, then the multiplication is well defined.

However, distributing on the right gives us $((r+t)(r'+t'))+T = (rr'+rt'+tr'+tt')+T$. This is equal to

$$(rr' + T) + (rt' + T) + (tr' + T) + (tt' + T).$$

The last term $(tt' + T) = 0 + T$, and so we need not worry about it, but the other terms we don't know are zero because r and r' are not necessarily in T.

Thus this multiplication is not well defined.

5. Find an explicit counter-example of a subring $T \subseteq R$ such that the multiplication on R/T is not well-defined.

Solution: Let's try $\mathbb{Z} \subseteq \mathbb{Q}$. Consider the two cosets $\frac{1}{2} + \mathbb{Z}$ and $\frac{1}{3} + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$. Notice that I have $\frac{1}{2} + \mathbb{Z} = \frac{3}{2} + \mathbb{Z}$. Now, notice that

$$(\frac{1}{2})(\frac{1}{3}) + \mathbb{Z} = \frac{1}{6} + \mathbb{Z}.$$

But

$$(\frac{3}{2})(\frac{1}{3}) + \mathbb{Z} = \frac{1}{2} + \mathbb{Z}.$$

Notice that $\frac{1}{2}$ is not equivalent to $\frac{1}{6}$ modulo $\mathbb{Z}$ (because their difference is not a whole number). This proves that multiplication in $\mathbb{Q}/\mathbb{Z}$ is not well defined.

6. Rings are not the right thing to form quotient groups with. Something else is, *ideals*.

Definition 0.2. If R is a ring, an ideal $I \subseteq R$ is an sub-Abelian group of R (under addition) that also satisfies the property that $rx \subseteq I$ for all $r \in R$ and $x \in I$.

Prove that the multiplication operation

$$(r + I)(r' + I) = (rr') + I$$

is well-defined. In particular, prove that R/I is a ring.

Solution: The well-definedness follows from the work we did in **4.** because now both rt' and $r't$ are in T, so the cosets $rt' + T$ and $r't + T$ are equal to $0 + T$, the additive identity.