Math 403 Chapter 14: Ideals and Quotient (Factor) Rings

1. **Introduction:** In group theory we introduced the concept of a normal subgroup and we showed that if $N \triangleleft G$ then we can create the quotient (factor) group G/N. This idea has an analogy in the theory of rings.

2. **Ideals:**

   (a) **Definition:** A subring $A \leq R$ is called an *ideal of* R if $\forall r \in R$ and $\forall a \in A$ we have $ar, ra \in A$.

   Definition: A is a *proper ideal* if it is an ideal which is not the entire ring.

   Example: For any ring R both $\{0\}$ and R are ideals of R.

   Example: $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

   Example: The set of polynomials with real coefficients and constant term 0 is an ideal of $\mathbb{R}[x]$.

   (b) **Theorem (Ideal Test):** If $A \subseteq R$ with $A \neq \emptyset$ then A is an ideal of F if:

      i. $\forall a, b \in A$ we have $a - b \in A$. Note that $a - b$ means $a + (-b)$.

      ii. $\forall a \in A$ and $\forall r \in R$ we have $ar, ra \in A$.

   Proof: This is a straightforward mash-up of the subring test and the definition of an ideal. $\mathcal{QED}$

   (c) **Definition:** If R is a commutative ring with unity and $a \in R$ then the *principal ideal generated by* a is the set:

   $$\langle a \rangle = \{ra \,|\, r \in R\}$$

   Note: The fact that its an ideal follows from the definition.

   Warning: We use the notation $\langle g \rangle$ in group theory but the definitions are different!

   Example: In $\mathbb{R}[x]$ the ideal $\langle x \rangle$ consists of all polynomials with constant term 0.

   Definition: We can expand the above for $a_1, ..., a_n \in R$ commutative with unity to have the ideal generated by all of the a_i:

   $$\langle a_1, ..., a_n \rangle = \{r_1 a_1 + ... + r_n a_n \,|\, r_1, ..., r_n \in R\}$$

   Example: In $\mathbb{Z}[x]$ the ideal $\langle x, 2 \rangle$ consists of all polynomials with even constant term. This is because an element in this ideal has the form $p(x)(x)+q(x)(2)$ for $p(x), q(x) \in \mathbb{Z}[x]$.

3. **Quotient (Factor) Rings:**

   (a) **Definition:** Let R be a ring and A be a subring of A. Then the set of cosets (defined the same way as for groups with addition):

   $$R/A = \{r + A \,|\, r \in R\}$$

   is a ring under the operations $(r+A)+(s+A) = (r+s)+A$ and $(r+A)(s+A) = rs+A$ iff A is an ideal of R.

   Proof: Suppose A is an ideal of R. Since R is an Abelian group under addition we know A is a normal subgroup and so the set of cosets forms a group under addition. Next we need to show that our multiplication is well-defined. Suppose we have $s + A = s' + A$ and

$t+A=t'+A$, then $s'+0 \in s+A$ so $s'=s+a$ and likewise $t'=t+b$ for $a,b \in A$. Then observe that:

$$s't'+A=(s+a)(t+b)+A=st+at+sb+ab+A=st+A$$

The final equality holds because $at, sb \in A$ because A is an ideal and $ab \in A$ because A is a subring of R. Showing that multiplication is associative and distributes over addition follows immediately.

Note that if A is not an ideal of R then choose $a \in A$ and $r \in R$ with (WLOG) $ar \notin A$. Then $(a+A)(r+A)=ar+A$ but $(a+A)(r+A)=(0+A)(r+A)=0+A$ which contradicts the fact that $ar \notin A$. $\mathcal{QED}$

Example: The quotient ring $\mathbb{Z}/4\mathbb{Z}$ consists of the elements $\{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$ with obvious operations, for example $(2+4\mathbb{Z})+(3+4\mathbb{Z})=5+4\mathbb{Z}=1+4\mathbb{Z}$ and $(2+4\mathbb{Z})(3+4\mathbb{Z})=6+4\mathbb{Z}=2+4\mathbb{Z}$.

Example: Consider the quotient ring $\mathbb{Z}[x]/\left\langle x^2-2\right\rangle$. What do the distinct cosets look like? Well we have $x^2-2+\left\langle x^2-2\right\rangle=0+\left\langle x^2-2\right\rangle$ so we can think of this as $x^2+\left\langle x^2-2\right\rangle=2+\left\langle x^2-2\right\rangle$. This allows drastic simplification of the cosets, for example:

$$\begin{aligned}7x^6+x^5-3x^2+4x-1+\left\langle x^2-2\right\rangle &= 7(x^2)^3+(x^2)^2x-3(x^2)+4x-1+\left\langle x^2-2\right\rangle \\ &= 7(2)^3+(2)^2x-3(2)+4x-1+\left\langle x^2-2\right\rangle \\ &= 8x-49+\left\langle x^2-2\right\rangle\end{aligned}$$

and similarly every $p(x)+\left\langle x^2-2\right\rangle$ is equivalent to $ax+b+\left\langle x^2-2\right\rangle$ with $a,b \in \mathbb{Z}$.

Could we reduce further? In other words could two of these be the same? Well suppose $ax+b+\left\langle x^2-2\right\rangle=cx+d+\left\langle x^2-2\right\rangle$. Then we have $(a-c)x+(b-d)+\langle x-2\rangle=0+\left\langle x^2-2\right\rangle$ and so $(a-c)x+(b-d) \in \left\langle x^2-2\right\rangle$.

However elements in $\left\langle x^2-2\right\rangle$ have the form $q(x)(x^2-2)$ for $q(x) \in \mathbb{Z}[x]$ and therefore have degree at least 2 except for the zero polynomial. Since $(a-c)x+(b-d)$ has degree at most 1 it must be the zero polynomial and so $a=c$ and $b=d$. Thus these elements are all distinct.

How does multiplication work in this ring? In general:

$$\begin{aligned}\left(ax+b+\left\langle x^2-2\right\rangle\right)\left(cx+d+\left\langle x^2-2\right\rangle\right) &= acx^2+(ad+bc)x+bd+\left\langle x^2-2\right\rangle \\ &= ac(2)+(ad+bc)x+bd+\left\langle x^2-2\right\rangle \\ &= (ad+bc)x+(bd+2ac)+\left\langle x^2-2\right\rangle\end{aligned}$$

Example: Consider the quotient ring $\mathbb{Z}[i]/\langle 3+i\rangle$. What do the distinct cosets look like? Well we have $3+i+\langle 3+i\rangle=0+\langle 3+i\rangle$ so we can think of this as $i+\langle 3+i\rangle=-3+\langle 3+i\rangle$. However since $i^2=-1$ we can square both sides to get $-1+\langle 3+i\rangle=9+\langle 3+i\rangle$ and so $10+\langle 3+i\rangle=0+\langle 3+i\rangle$.

Since every coset has the form $a+bi+\langle 3+i\rangle$ such a coset can be rewritten by replacing i with -3 and 10 with 0, therefore every coset has the form $c+\langle 3+i\rangle$ for $c \in \mathbb{Z}_{10}$.

Could two of these coset be identical? Suppose $a+\langle 3+i\rangle=b+\langle 3+i\rangle$ so that $a-b \in \langle 3+i\rangle$ and so $a-b=(c+di)(3+i)=(3c-d)+(c+3d)i$ for some $c,d \in \mathbb{Z}$. But then $3c-d=a-b$ and $c+3d=0$. Solving these yields $a-b=-10d$ but since $a,b \in \mathbb{Z}_{10}$ we have $d=0$ and $a=b$.

Thus they are unique. In fact this is essentially the ring $\mathbb{Z}_{10}$ written differently.

4. **Maximal and Prime Ideals:**

(a) **Definition:** A proper ideal A of a commutative ring R is a *maximal ideal of* R if whenever B is another ideal with $A \subseteq B \subseteq R$ then $B = A$ or $B = R$.

Basically this means that an ideal which is larger must be the entire ring. Typically proving that an ideal is maximal involves taking another ideal B with $A \subsetneq B$ and showing $B = R$. Typically to show $B = R$ we show $1 \in B$ because then $r = r(1) \in B$ for any $r \in R$.

Example: The ideal $6\mathbb{Z}$ is not maximal in $\mathbb{Z}$ because $6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Example: The ideal $7\mathbb{Z}$ is maximal in $\mathbb{Z}$. To see this suppose $7\mathbb{Z} \subsetneq B \subseteq R$, then there is some $b \in B$ with $b \notin 7\mathbb{Z}$ and so $\gcd(7, b) = 1$ and so there exist $x, y \in \mathbb{Z}$ with $7x + by = 1$. Then since $b \in B$ and $7 \in 7\mathbb{Z} \subsetneq B$ we have $1 \in B$ and then $r = r(1) \in B$ for all r and so $R = B$.

Example: The ideal $\langle x \rangle$ is not maximal in $\mathbb{Z}[x]$ since $\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}[x]$.

(b) **Definition:** A proper ideal A of a commutative ring R is a *prime ideal of* R if for all $a, b \in R$ if $ab \in A$ then $a \in A$ or $b \in A$.

Example: The ideal $6\mathbb{Z}$ is not prime in $\mathbb{Z}$ because $(2)(3) \in 6\mathbb{Z}$ but $2 \notin 6\mathbb{Z}$ and $3 \notin 6\mathbb{Z}$.

Example: The ideal $7\mathbb{Z}$ is prime in $\mathbb{Z}$. To see this suppose $ab \in 7\mathbb{Z}$. Then $7 \mid ab$ and so $7 \mid a$ or $7 \mid b$ and so $a \in 7\mathbb{Z}$ or $b \in 7\mathbb{Z}$.

Example: The ideal $\langle x \rangle$ is prime in $\mathbb{Z}[x]$. To see this suppose $p(x)q(x) \in \langle x \rangle$. The ideal $\langle x \rangle$ consists of all polynomials with constant term zero and hence one of $p(x)$ or $q(x)$ must have constant term 0 since the constant term of $p(x)q(x)$ is the product of the constant terms of $p(x)$ and of $q(x)$. Thus either $p(x)$ or $q(x)$ is in $\langle x \rangle$.

(c) **Theorem:** Let R be a commutative ring with unity and let A be an ideal. Then R/A is an integral domain iff A is a prime ideal.

Proof:

$\Longrightarrow$: Suppose R/A is an integral domain and suppose $ab \in A$. Then $(a + A)(b + A) = ab + A = 0 + A$ so either $a + A = 0 + A$ or $b + A = 0 + A$ and so either $a \in A$ or $b \in A$.

$\Longleftarrow$: Suppose A is a prime ideal and suppose $(a + A)(b + A) = 0 + A$. Then $ab + A = 0 + A$ and so $ab \in A$ and so either $a \in A$ or $b \in A$ and so either $a + A = 0 + A$ or $b + A = 0 + A$.

$\mathcal{QED}$

(d) **Theorem:** Let R be a commutative ring with unity and let A be an ideal. Then R/A is a field iff A is maximal.

Proof:

$\Longrightarrow$: Suppose R/A is a field and $A \subsetneq B \subseteq R$. Let $b \in B$ with $b \notin A$. Then $b + A \neq 0 + A$ and so $b + A$ is a unit in R/A and so there is some $c + A$ with $(b + A)(c + A) = 1 + A$. Thus $bc + A = 1 + A$ and so $1 - bc \in A \subseteq B$. Since $b \in B$ we then have $bc \in B$ (because B is an ideal) and hence $1 \in B$ and so $B = R$.

$\Longleftarrow$: Suppose A is maximal and let $x + A \neq 0 + A$. Consider the set $B = \{rx + a \mid r \in R, a \in A\}$. A short proof (omitted) shows that B is an ideal of R which contains but is larger than A. Thus $B = R$ and so $1 = r'x + a'$ for some $r' \in R$ and $a' \in A$ and so $(r' + A)(x + A) = r'x + A = 1 - a' + A = 1 + A$. $\mathcal{QED}$

Corollary: If R is commutative then if an ideal A is maximal then it is prime.

Proof: If A is maximal then R/A is a field and hence R/A is an integral domain and hence A is prime. $\mathcal{QED}$

The reverse is of course not true as we have seen: The ideal $\langle x \rangle$ is prime but not maximal in $\mathbb{Z}[x]$.