.....

Summaries, March 3 and 5

Rings.

A ring R is a set with two laws of composition called addition and multiplication. The axioms are:
• with the operation of addition, R is an abelian group. Its identity element is denoted by 0.
• multiplication is associative and commutative, and there is an identity element that is denoted by 1.
• *distributive law* For all a, b, c in R, $(a + b)c = ac + bc$.

The axioms can be weakened. If multiplication isn't commutative, the structure is called a *noncommutative ring*. For example, the set of $n \times n$ matrices forms a noncommutative ring. One might also drop the requirement that multiplication has an identity element. But for us a ring will be a structure having the properties listed above.

Examples.
• The set of integers forms a ring denoted by $\mathbb{Z}$.
• The set $\mathbb{Z}[i]$ of *Gauss integers*, complex numbers of the form $a + bi$ with a, b in $\mathbb{Z}$ forms a ring.
• Let R be any ring. The set $R[x]$ of polynomials with coefficients in R forms a ring, with the usual rules for adding and multiplying polynomials. For instance, the set $\mathbb{Z}[x]$ of polynomials with integer coefficients is a ring.
• If A and B are rings, the product set $AtimesB$ is a ring. Addition is vector addition and mulltipication is component-wise: $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$.

(Sometimes, we put a $\cdot$ in to denote multiplication, for clarity.)

Ring Homomorphisms.

Let R and R' be rings. A *homomorphism* $R \xrightarrow{\varphi} R'$ is a map that is compatible with addition and multipication, and sends the identity element 1 of R to the identity element $1'$ of R':

$\varphi(a + b) = \varphi(a) + \varphi(b)$
$\varphi(ab) = \varphi(a)\varphi(b)$
$\varphi(1) = 1'$

The assumption that 1 is sent to $1'$ means, for example, that the map $A \to A \times B$ from a ring A to a product $A \times B$ that sends an element a to $(a, 0)$ is not called a homomorphism, though it is compatible with addition andd multiplication.

Examples of homomorphisms.

• There is a unique homomorphism $\mathbb{Z} \to R$ from the ring of integers to any ring R. It sends the integer 1 to the identity element 1_R of R, 2 to $1_R + 1_R$, etc., and it sends -1 to -1_R, etc.

• The projection $A \times B \to A$ from a product ring to the first factor that sends (a, b) to a is a homomorphism.

• Let $\mathbb{C}[x]$ be the ring of polynomials with complex coefficients, and let α be a complex number. The map $\mathbb{C}[x] \to \mathbb{C}$ that substitutes α for x is a homomorphism:

This is an example of a general principle, called the *substitution principle*, that describes maps from a polynomial ring $R[x]$ to another ring R'.

Substitution Principle This is important.

Let $A \xrightarrow{\varphi} B$ be a ring homomorphism, and let α be an element of B. There is a unique homomorphism $A[x] \xrightarrow{\Phi} B$ such that $\Phi(a) = \varphi(a)$ if a is in A, and $\Phi(x) = \alpha$.

If $f(x) = na_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is a polynomial in $A[x]$ and $b_i = \varphi(a_i)$, the homomorphism Φ sends $f(x)$ to the element $b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$ of B, applying φ to the coefficients and substituting α for x.

For example, we can map the ring $\mathbb{Z}[x]$ of integer polynomials to the ring of complex numbers $\mathbb{C}$, defining φ to be the unique homomorphism $\mathbb{Z} \to \mathbb{C}$, and substituting $\sqrt{2}$ for x. This homomorphism sends the polynomial $x^2 + 3x + 5$ to the complex number $2 + 3\sqrt{2} + 5 = 7 + 3\sqrt{2}$.

Or, let $F = \mathbb{F}_p$ be the field of integers modulo p, and let' s denote the residue of an integer n in F by $\overline{n}$. The unique homomorphism $\mathbb{Z} \to F$ sends n to $\overline{n}$. We can map $\mathbb{Z}[x]$ to F by substituting any element of F, such as $\overline{2}$ for x. The polynomial $3x + 5$ will be mapped to $\overline{3}\overline{2} + \overline{5} = \overline{11}$.

Kernels.

Let $A \xrightarrow{\varphi} B$ be a ring homomorphism. The *kernel* K of φ is the set of elements of A that map to zero in B:

$$K = \{a \in A \,|\, \varphi(a) = 0\}$$

The kernel has these properties:

K is an additive subgroup of A. If u and v are in K, so are $-u$ and $u + v$.

If u is in K and a is any element of A, the product au is in K.

The proof of is as follows: $\varphi(au) = \varphi(a)\varphi(u) = \varphi(a) \cdot 0 = 0$.

(In a ring B, it is true that $b \cdot 0 = 0$ for all b in B. Since $0 = 0 + 0$, $\;b \cdot 0 = b(0 + 0) = b \cdot 0 + b \cdot 0$. Because B is a goupwithrepsectto addition, we can cancel $b \cdot 0$ from both sides: $0 = b \cdot 0$.)

A subset I of a ring R that is closed under addition and under multiplication by any element of R is called an *ideal*. The kernel of a homomorphism is an ideal.

If a is an element of a ring R, the set $Ra = \{ra \,|\, r \in R\}$ of multiples of a is an ideal. Such an ideal is called a *principal ideal*, and the element a is called a *generator* of that ideal.

A ring in which all ideals are principal ideals is a *prinipal ideal ring*. Principal ideal rings are very rare. However, there are three interesting ones:

Proposition. The following are principal ideal rings:

the ring $\mathbb{Z}$ of integers,

the ring $F[x]$ of polynomials with coefficients in a field F,

the ring $\mathbb{Z}[i]$ of Gauss integers.

The proofs of all parts of this proposition are analogous. They are based on division with remainder. It isn't the case that all principal ideal rings have division with remainder, but the three listed above do.

I hope that you learned in 18.701 that every subgroup of the additive group of integers is cyclic, but let's review the proof. Let a and b be integers, with a positive. Then $b = aq + r$ where q, r are integers and r is in the range $0 \le r \le a - 1$. Now let H be an additive subgroup of $\mathbb{Z}$. If $H = \{0\}$, then H is cyclic, generated by 0. Otherwise, H contains a nonzero integer n and its negative $-n$, one of the two of which is positive. So H contains a positive integer. Let a be the smallest positive integer in H. We show that H is the cyclic group $\mathbb{Z}a$ of integer multiples of a: If b is any element of H, and if we write $b = aq + r$ as above, then b and aq are in H, and therefore $r = b - aq$ is in H. But since a is the smallest positive integer in H, the only integer in the range $[0, a - 1]$ that is in H is 0. Therefore $r = 0$, and $b = aq$ is in $\mathbb{Z}a$. □

By the way, the cyclic group of multiples of a consists of the integer multiples of a. It is the same as the principal ideal generated by a.

Next, for a ring of the form $F[x]$, $\;F$ a field, one can also use division with remainder.

We state division with remainder for the ring $R[x]$ of polynomials with coefficients in any ring R.

A monic polynomial is one whose highest coefficent is 1.

division with remainder in $R[x]$. Let $f(x)$ and $g(x)$ be polynomials in $R[x]$, with f monic, and of degree d. There are polynomials $q(x)$ and $r(x)$ in $R[x]$, with r of degree less than d, such that

$$g(x) = f(x)q(x) + r(x)$$

The proof of this is an easy induction argument. Say that $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Then $g(x) - b_n x^{n-d} f(x)$ has lower degree than n ...

Now let I be an ideal of $F[x]$. If $I = \{0\}$, then I is a principal ideal. Suppose that $I \neq 0$. Let $f(x)$ be a nonzero polynomial of minimal degree d in I. Since F is a field, we can divide by the leading coefficient to make f monic. Then if g is any polynomial in I, we write $g = fq + r$ where r has degree $< d$. Then $r = g - fq$ is in I, and since d is the minimal degree of a nonzero polynomial in I, $r = 0$, and $q = fq$ is in the principal ideal generated by f.

For the ring $\mathbb{Z}[i]$ of Gauss integers, we need to define division with remainder. It is as follows: Let α and β be complex numbers, $\alpha \neq 0$. There are complex numbers q and r, with q a Gauss integer and $|r| < |\alpha|$, such that $\beta = \alpha q + r$. I verified this by a picture in class. You will be able to make an algebraic proof.

With this division algorithm, the proof carries over. □

But, note that q and r aren't unique Division with remainder isn't a unique process.

Quotient Rings.

Recall that, if H is a normal subgroup of a group G, there is a quotient group $\overline{G} = G/H$. Its elements are equivalence classes $\overline{a}$ of elements a of G, the equivalence relation being that $\overline{b} = \overline{a}$, i.e., $b \sim a$, if $b = ah$ for some h in H. Or, one can think of the elements of $\overline{G}$ as the cosets aH of H. Multiplication in $\overline{G}$ is defined by multiplication in G: $\overline{a}\overline{b} = \overline{ab}$.

Let I be an ideal of a ring R. Then I is a subgroup of the additive group of R, and one can form the quotient $\overline{R}$ as an additive group. Since the law of composition is addition, the cosets of I are sets of the form $a + I$. Then $b \sim a$ means that b is in the coset $a + I$.

Similarly, if I is an ideal of $\longrightarrow ringR$, there is a quotient ring $\overline{R}$ whose elements are equvalence classes of elements of R, the relation being that $\overline{b} = \overline{a}$, i.e., $b \sim a$, if $b = a + x$ for some x in the ideal I. Or, one can think of $\overline{R}$ as the set of cosets $a + I$. Multilplication is defined as follows: Let $\overline{a} = a + I$ and $\overline{b} = b + I$. The product $\overline{a}\overline{b}$ is the coset $ab + I$. This is the unique coset that contains the products $(a + x)(b + y)$ for all x, y in I. In symbolic terms, the verification that those products lie in a coset is $(a + I)(b + I) = ab + aI + Ib + II$. The three terms aI, Ib, II are all contained in I, so $(a + I)(b + I) \subset ab + I$. The cosets $ab + I$ that contains the products is unique because the cosets partition the ring.

When aN and bN are cosets of a normal subgroup N of a group G, the product $aNbN$ is actually equal to abN. However, for ideals it needn't be true that $(a + I)(b + I) = ab + I$. For example, if $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$, then $(2 + 6\mathbb{Z})(2 + 6\mathbb{Z}) \subset 4 + 12\mathbb{Z} < 4 + 6\mathbb{Z}$.

mapping property of the quotient ring

Let $R \xrightarrow{\varphi} R'$ be a ring homomorphism, and let I be an ideal of R. Let $R \xrightarrow{\pi} oR$ be the canonical map to the quotient ring $\overline{R} = R/I$ There is a homomorphism $\overline{R} \xrightarrow{\overline{\varphi}} R'$ such that φ is the composition $\overline{\varphi}\pi$ if and only if I is contained in the kernel of φ. If so, then $\overline{\varphi}$ is uniqely determined. So if $I \subset \ker \varphi$, there is a diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ {\scriptstyle\pi}\downarrow & & \downarrow{=} \\ \overline{R} & \xrightarrow{\overline{\varphi}} & R' \end{array}$$

If φ is surjective and $I = \ker \varphi$, then $\overline{\varphi}$ is an isomorphism.

For example, let I be the ideal $n\mathbb{Z}$ in the ring of integers $\mathbb{Z}$ for some integer n, and let π be the canonical homomorphism $\mathbb{Z} \to \mathbb{Z}/I$ $(= \mathbb{Z}/n\mathbb{Z})$. Also, let $\mathbb{F}_p$ be the field $\mathbb{F}_p$ of integers modulo p, and let φ be the homomorphism $\mathbb{Z} \to \mathbb{F}_p$. There is a unique homomorphism $\overline{\varphi}$ from the quotient ring $\mathbb{Z}/I$ to $\mathbb{F}_p$ if and only if p divides n. This is fairly obvious.