Math 546 Test 3.

This is due on Friday, November 20 at midnight. You are to work alone in it. You can look up definitions and the statements of theorems we have covered in class. Needless to say (but I will say it anyway) no use of online help sites such as Stack Overflow or Chegg. Please print your name on the first page of the test as this makes my book keeping easier.

On this test all rings are commutative. If R is a ring and I is an ideal in R then we will use the notation

$$R/I = \{a + I : a \in R\}$$

for the quotient ring whose elements are the equivalence classes

$$a + I = \{x \in R : x \equiv a \pmod{I}\}$$

where, by definition,

$$a \equiv b \pmod{I} \quad \iff \quad b - a \in I.$$

The ring operations on R/I are

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I)(b + I) = ab + I.$$

Problem 1 (10 points.). Let R be a ring, $a_1, a_2, a_3 \in R$, and let

$$\langle a_1, a_2, a_3 \rangle = \{r_1a_1 + r_2a_2 + r_3a_3 : r_1, r_2, r_3 \in R\}.$$

That is $\langle a_1, a_2, a_3 \rangle$ the set of all linear combinations of a_1, a_2, and a_3 with coefficients from R. Starting wiht the definition of an ideal give a careful proof that $\langle a_1, a_2, a_3 \rangle$ is an ideal in R. □

You have proven the following in Homework 12.

Proposition 1. *Let F be a field and $f(x) \in F[x]$ with $\deg(f(x)) = 2$, or $\deg(x) = 3$. Then $f(x)$ is irreducible if and only if $f(x)$ has no roots in F.* □

For example consider the polynomial

$$f(x) = x^2 + x + 2$$

over the field $F = \mathbb{Z}_3$. The elements of $\mathbb{Z}_3$ are $[0]_3$, $[1]_3$, and $[2]_3$. Then

$$\begin{aligned} f([0]_3) &= [0^2 + 0 + 2]_3 = [2]_3 \\ f([1]_3) &= [1^2 + 1 + 2]_3 = [4]_3 = [1]_3 \qquad (\text{as } 4 \equiv 1 \pmod{3}) \\ f([2]_3) &= [2^2 + 2 + 2]_3 = [8]_3 = [2]_3 \qquad (\text{as } 8 \equiv 2 \pmod{3}). \end{aligned}$$

Therefore $f(x)$ has no roots in $F = Z_3$ and therefore $f(x)$ is irreducible. We now consider the ring

$$R = \mathbb{Z}_3/\langle f(x) \rangle$$

where, as usual, $\langle f(x)\rangle$ is the principle ideal generated by $f(x)$. Let $a \in R$ be the element

$$a = x + \langle f(x)\rangle.$$

Then by the definition of the operations in R we have

$$a^2 + a + 2 = (x^2 + x + 2) + \langle f(x)\rangle = \langle f(x)\rangle = 0 + \langle f(x)\rangle.$$

as $f(x) \in \langle f(x)\rangle$ and thus $f(x) \equiv 0 \pmod{\langle f(x)\rangle}$. As $0 + \langle f(x)\rangle$ is the zero element of R can write this as

$$a^2 + a + 2 = 0.$$

Let us rewrite this as

$$a^2 = -a - 2 = 2a + 1$$

where we are using that in the field $\mathbb{Z}_3$ we have

$$\begin{aligned} -1 &= 2 && (\text{as } -1 \equiv 2 \pmod 3) \\ -2 &= 1 && (\text{as } -2 \equiv 1 \pmod 3). \end{aligned}$$

(If we were being very precise this should be $[-1]_3 = [2]_3$ and $[-2]_3 = [1]_3$, but at some point all the brackets start to make things less readable.)

Also if $h(x) + \langle f(x)\rangle \in R$, then we use the division algorithm to write

$$h(x) = q(x)f(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or } \deg(r(x)) < \deg(f(x)) = 2.$$

The conditions on $r(x)$ imply it is of the form $r(x) = cx + d$ with $c, d \in F = Z_3$. Therefore

$$h(x) = q(x)f(x) + cx + d$$

for some $c, d \in F = \mathbb{Z}_3$. Using that $q(x)f(x) + \langle f(x)\rangle = \langle f(x)\rangle$ is the zero element of R we have

$$\begin{aligned} h(x) + \langle f(x)\rangle &= (q(x)f(x) + cx + d) + \langle f(x)\rangle \\ &= cx + d + \langle f(x)\rangle && (\text{as } q(x)f(x) \equiv 0 \pmod{f(x)}). \\ &= ca + b && (\text{as } x + \langle f(x)\rangle = a.) \end{aligned}$$

Therefore every element of R is of the form $ca + d$ with $c, d \in F = \mathbb{Z}_3$. Thus R has 9 elements:

$$R = \{0, 1, 2, a, a+1, a+2, 2a, 2a+1, 2a+2\}.$$

These are added in the usual way:

$$(2a + 2) + (a + 2) = 3a + 4 = 1$$

as in $\mathbb{Z}_3$ we have $3 = 0$ and $4 = 1$ (which is really short hand for $[3]_3 = [0]_3$ and $[4]_3 = [1]_3$). We can multiply using $a^2 = 2a + 1$. For example

$$(2a + 2)(a + 2) = 2a^2 + 6a + 4 = 2(2a + 1) + 6a + 4 = 10a + 6 = a$$

where we have used that in $\mathbb{Z}_3$ we have $6 = 0$ and $10 = 1$. Here are the complete addition and multiplication tables for $R = \mathbb{Z}_2[x]/\langle f(x)\rangle = \mathbb{Z}_1[x]/\langle x^2 + x + 1\rangle$.

$+$	0	1	2	a	$a+1$	$a+2$	$2a$	$2a+1$	$2a+2$
0	0	1	2	a	$a+1$	$a+2$	$2a$	$2a+1$	$2a+2$
1	1	2	0	$a+1$	$a+2$	a	$2a+1$	$2a+2$	$2a$
2	2	0	1	$a+2$	a	$a+1$	$2a+2$	$2a$	$2a+1$
a	a	$a+1$	$a+2$	$2a$	$2a+1$	$2a+2$	0	1	2
$a+1$	$a+1$	$a+2$	a	$2a+1$	$2a+2$	$2a$	1	2	0
$a+2$	$a+2$	a	$a+1$	$2a+2$	$2a$	$2a+1$	2	0	1
$2a$	$2a$	$2a+1$	$2a+2$	0	1	2	a	$a+1$	$a+2$
$2a+1$	$2a+1$	$2a+2$	$2a$	1	2	0	$a+1$	$a+2$	a
$2a+2$	$2a+2$	$2a$	$2a+1$	2	0	1	$a+2$	a	$a+1$

$*$	0	1	2	a	$a+1$	$a+2$	$2a$	$2a+1$	$2a+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	a	$a+1$	$a+2$	$2a$	$2a+1$	$2a+2$
2	0	2	1	$2a$	$2a+2$	$2a+1$	a	$a+2$	$a+1$
a	0	a	$2a$	$2a+1$	1	$a+1$	$a+2$	$2a+2$	2
a+1	0	$a+1$	$2a+2$	1	$a+2$	$2a$	2	a	$2a+1$
a+2	0	$a+2$	$2a+1$	$a+1$	$2a$	2	$2a+2$	1	a
2a	0	$2a$	a	$a+2$	2	$2a+2$	$2a+1$	$a+1$	1
2a+1	0	$2a+1$	$a+2$	$2a+2$	a	1	$a+1$	2	$2a$
2a+2	0	$2a+2$	$a+1$	2	$2a+1$	a	1	$2a$	$a+2$

Problem 2 (10 points.). Use these tables or otherwise and give an explication of what you did to

(a) find $\dfrac{1}{1+a}$,
(b) solve $(1+a)y - 2a + 1 = 0$ for y, and
(c) solve $y^2 = 2a + 1$ for y.

Problem 3 (30 points.). In this problem $F = \mathbb{Z}_2$ is the two element field. Let $f(x) \in F[x]$ be the polynomial

$$f(x) = x^3 + x + 1.$$

(a) Use Proposition 1 to show $f(x)$ is irreducible.

We now let

$$R = F[x]/\langle f(x)\rangle.$$

and let $b \in R$ be the element

$$b = x + \langle f(x)\rangle.$$

(b) Show

$$b^3 = b + 1.$$

Hint: In Z_2 we have $[1]_2 = [-1]_2$, that is in $\mathbb{Z}_2$ we have $-1 = 1$ (and also $2 = 0$).

(c) Use this to show

$$b^4 = b^2 + b.$$

(d) Use the division algorithm as we did above to show every element of R can be written in the form $\alpha b^2 + \beta b + \gamma$ where $\alpha, \beta, \gamma \in F = \mathbb{Z}_2$ and therefore R has 8 elements:

$$R = \{0, 1, b, b+1, b^2, b^2+1, b^2+b, b^2+b+1\}$$

(e) Make the addition and multiplication tables for R. □

Problem 4 (10 points.). Let m be a positive integer such that $\sqrt{m}$ is irrational. (For example $m = 2$.)

$$R = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}.$$

That is R is the set of real numbers of the form $a + b\sqrt{m}$ where both a and b are rational numbers.

(a) Show that R is a subring of $\mathbb{R}$ (where $\mathbb{R}$ is the set of real numbers). *Hint:* You do not have to verify all the ring axioms, you just have to show that $1 \in R$ and that R is closed under addition, subtraction, and products.

(b) Show that R is a field, that is show that all nonzero elements of R have a multiplicative inverse in R. □

Definition. Let R and S be rings. A function $\phi\colon R \to S$ is a ***ring homomorphism*** if and only if

(i) $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in R$,
(ii) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$,
(iii) $\phi(1) = 1$.

Definition. Let $\phi\colon R \to S$ be a ring homomorphism between rings. Then the ***kernel*** of ϕ is

$$\ker(\phi) = \{r \in R : \phi(r) = 0\}.$$

Proposition 2. *If $\theta\colon R \to S$ is a homomorphism of rings, then $\ker(\theta)$ is an ideal in R and $1 \notin \ker(\theta)$.*

Problem 5 (10 points.). Prove this. *Hint:* The proof of this standard and can be found in many places, including our text. But do not just copy a proof, rewrite it in your own words and also use the notation here (that is θ). □

Problem 6 (20 points.). Let $\theta\colon R \to S$ be a surjective (that is onto) ring homomorphism and let $K = \ker(\theta)$. Since this is an ideal we can form the quotient ring R/K. Define $\widehat{\theta}\colon R/K \to S$ by

$$\widehat{\theta}(r + K) = \theta(r).$$

(a) State precisely what it means for the map $\widehat{\theta}$ to be ***well defined***.
(b) Prove $\widehat{\theta}$ is well defined.
(c) Prove $\widehat{\theta}$ is a homomorphism of rings.
(d) Prove $\widehat{\theta}$ is surjective.
(e) Prove $\widehat{\theta}$ is injective. □

Problem 7 (10 points.). Let m be an integer and let $\alpha = \sqrt[3]{m}$ and let

$$S = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Z}\}.$$

Prove R is a subring of the real numbers. $\square$