

# Math 225 Modern Algebra

## Final Exam

Prof. D. Joyce

December, 2003

On this take-home exam you may consult your notes for the course, the text book, and any other books you like. Do all your own work; don't consult with anyone but me.

Start your answer to each problem on a separate page. Staple the pages together before you hand them in.

Points are in square brackets.

**Problem 1. On ideals, quotient rings, and fields.** [24; 8 points each part]

Consider the polynomial ring  $\mathbf{Q}[x]$ . Let  $f$  be the polynomial  $x^2 - x - 1$ . Consider the principal ideal  $(f)$  generated by  $f$ .

**1a.** Show that the polynomial  $x^4 - x^3 + x^2 - 2x - 2$  is an element of  $(f)$ .

Now let  $S$  be the quotient ring  $\mathbf{Q}[x]/(f)$ . The elements of  $S$  are named by polynomials. Two polynomials name the same element of  $S$  if their difference lies in  $(f)$ . Thus,  $x^2$  and  $x + 1$  name the same element of  $S$  since their difference,  $x^2 - (x + 1)$  is  $f$  itself. In this situation, the standard congruence notation is often used, and we write  $x^2 \equiv x + 1 \pmod{f}$ . The polynomial  $f$  is quadratic, so every element of  $S$  can be named by a linear polynomial. (In general, if  $f$  is of degree  $n$ , then elements of the quotient can be named by polynomials of degree less than  $n$ .)

**1b.** For each of  $x^3, x^4, x^5$ , and  $x^6$ , find congruent linear polynomials. That is, find rational numbers  $a$  and  $b$  so that  $x^n \equiv ax + b \pmod{f}$ . In general, what can you say about  $x^n$ ? (Look at the pattern you've got so far for  $x^3, x^4, x^5$ , and  $x^6$ .)

In fact,  $S$  is a field, so every nonzero element will have an inverse.

**1c.** Find an inverse for  $x$ . It will be a polynomial  $g(x)$  (which you can assume is a linear polynomial) such that  $xg(x) \equiv 1 \pmod{f}$ . (If you were to generalize what you do in 1c for  $x$  to any linear polynomial, then you would have a proof that  $S$  is a field.)

**Problem 2. On transformation groups of the plane.** [16 points; 8 points each part]

The group  $G$  of isometries of the plane has many subgroups. In this problem, you'll investigate one of these subgroups and its associated quotient group.

**2a.** The translations of the plane form a subgroup  $T$  of  $G$ . Show that  $T$  is a normal subgroup of  $G$ .

**2b.** Since  $T$  is a normal subgroup of  $G$ , there is a quotient group  $G/T$ . Another subgroup of  $G$  is the orthogonal group  $O$  which consists of isometries of the the plane that fix the origin  $(0,0)$ . Show that the group  $G/T$  is isomorphic to the group  $O$ . (One way to do that is to show that the composition of the inclusion homomorphism  $O \rightarrow G$  with the canonical quotient homomorphism  $G \rightarrow G/T$  is an isomorphism. Another way is to apply one of the theorems in the text about subgroups and quotient groups.)

**Problem 3. On ring isomorphisms.** [24 points; 8 points each part]

In this problem, you'll show that the ring  $\mathbf{Z}_5 \times \mathbf{Z}_8$  is isomorphic to the ring  $\mathbf{Z}_{40}$  as rings with a multiplicative identity. The isomorphism depends on 5 and 8 being relatively prime.

**3a.** First, what is the multiplicative identity of the ring  $\mathbf{Z}_5 \times \mathbf{Z}_8$ ?

Now, suppose  $f$  is an isomorphism  $f : \mathbf{Z}_{40} \rightarrow \mathbf{Z}_5 \times \mathbf{Z}_8$  preserving 1. Since every element of  $\mathbf{Z}_{40}$  is a multiple of 1, therefore  $f(n) = nf(1)$ . Also,  $f$  must send 1 in  $\mathbf{Z}_{40}$  to the identity of  $\mathbf{Z}_5 \times \mathbf{Z}_8$ , which you identified in 3a. Therefore, there can be only one such isomorphism.

**3b.** If you try to define a ring homomorphism  $f : \mathbf{Z}_{39} \rightarrow \mathbf{Z}_5 \times \mathbf{Z}_8$  in the same way, it doesn't work, and you don't get a ring homomorphism. In your own words, explain what goes wrong. (Here are some possibilities of what can go wrong:  $f$  is not well-defined,  $f$  doesn't preserve addition,  $f$  doesn't preserve

multiplication. Note that it has something to do with 5 and 8 dividing 40, but not 39.)

**3c.** If  $f$  is an isomorphism, then it has an inverse,  $f^{-1} : \mathbf{Z}_5 \times \mathbf{Z}_8 \rightarrow \mathbf{Z}_{40}$ . What is  $f^{-1}$ ? (Note that it's enough to specify  $f^{-1}(1, 0)$  and  $f^{-1}(0, 1)$  since all the other elements of  $\mathbf{Z}_5 \times \mathbf{Z}_8$  are linear combinations of  $(1, 0)$  and  $(0, 1)$ .)

**Problem 4. On groups and their presentations.** [21; 7 points each part]

A certain group  $G$  can be described as having two elements  $a$  and  $b$  with the following relations:  $a^2 = 1$ ,  $b^3 = 1$ , and  $(ab)^3 = 1$ .

**4a.** Show that  $b^2a = abab$  follows from the relations.

**4b.** Find two elements  $a$  and  $b$  of the symmetric group  $S_4$  that satisfy the stated relations.

**4c.** What do you think the order of  $G$  might be? (Full credit on this part if you're right, none if you're wrong. You don't have to justify your answer.)

**Problem 5. On field automorphisms.** [16; 8 points each part]

Consider the field  $\mathbf{Q}[\sqrt{5}]$ . Every element in this field can be written as  $x + y\sqrt{5}$  where  $x$  and  $y$  are rational numbers. Also consider the function  $f : \mathbf{Q}[\sqrt{5}] \rightarrow \mathbf{Q}[\sqrt{5}]$ , where  $f(x + y\sqrt{5}) = x - y\sqrt{5}$ .

**5a.** Carefully show that  $f$  is a ring homomorphism.

**5b.** Show that  $f$  is an isomorphism.

(Comment. This  $f$  along with the identity form a two-element group, the group of automorphisms of  $\mathbf{Q}[\sqrt{5}]$  over  $\mathbf{Q}$ . In general, for any field extension  $K$  over  $F$ , there is a group of automorphisms of  $K$  that fix  $F$ , called the Galois group of  $K/F$ . Galois groups are used to study field extensions and solutions of polynomial equations.)