Math 546 Final.

This is due on Monday, December 7 at 3:00pm. 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.

- *Put your name on the first page of the test.*
- *Since you have plenty of time for this and I have to have grades in shortly after the exam, I would just as soon not have any late papers.*
- *If you are using light pencil or pen it is good idea to scan a page or two and email to yourself to see how readable it is. (And remember my eyes are very likely not as good as yours.)*

Problem 1 (10 points). This problem is mostly to make sure you can write an induction proof. Let G be a group and let $a, b \in G$ be elements such that

$$bab^{-1} = a^k$$

for some integer k. Prove

$$b^j ab^{-j} = a^{k^j}.$$

In doing the proof carefully state both the base case and induction hypothesis. *Hint:* In the proof your are allowed to assume for any integer n that $\left(bab^{-1}\right)^n = ba^n b^{-1}$ and for all integers m and n that $(a^m)^n = a^{mn}$. $\square$

Proposition 1. *Let p be a prime number and k an integer with*

$$k^2 \equiv 1 \pmod{p}.$$

Then

$$k \equiv \pm 1 \pmod{p}.$$

Problem 2 (10 points). Prove this. *Hint:* At no point should you use the square root symbol $\sqrt{\ }$. $\square$

One of the most basic facts we have proven about groups is Lagrange's Theorem:

Theorem 2 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup of G. Then $|H| \mid |G|$. (Here $k \mid n$ is the notation for "k divides n").* $\square$

Here is generalization of something I used implicitly on the last day of class and it is something we have proven before and which uses Lagrange's Theorem.

Proposition 3. *Let m and n be positive integers with* $\gcd(m, n) = 1$. *Let G be a finite group with $|G| = mn$. Let A and B be subgroups of G with $|A| = m$ and $|B| = n$. Then*

(a) $A \cap B = \{1\}$, *and*
(b) $AB = G$ *(where, as usual* $AB = \{ab : a \in A, b \in B\}$*.*

Proof. As the intersection of two subgroups is a subgroup, we have that $A \cap B$ is a subgroup not only of G, but a subgroup of each of A and B. As $A \cap B$ is a subgroup of A Lagrange's Theorem tells us that $|A \cap B| \,\big|\, |A| = m$. Likewise $|A \cap B| \,\big|\, |B| = n$. Thus $|A \cap B|$ is a common divisor of each of m and n and as $\gcd(m, n) = 1$, this implies $|A \cap B| = 1$. Therefore $A \cap B = \{1\}$.

To see that $AB = G$ define $f : A \times B \to G$ by

$$f(a, b) = ab.$$

We now show that f is injective (i.e. one to one). Assume $f(a_1, b_1) = f(a_2, b_2)$. Then we wish to show $a_1 = a_2$ and $b_1 = b_2$. We have

$$a_1 b_1 = f(a_1, b_1) = f(a_2, b_2) = a_2 b_2$$

Multiply on the left by a_2^{-1} and on the right by b_1^{-1} to get

$$a_2^{-1} a_1 = b_2 b_1^{-1}.$$

We then do a standard proof by schizophrenia. That is the element $x = a_2^{-1} a_1 = b_2 b_1^{-1}$ has $x \in A$ as $x = a_2^{-1} a_1$. Also $x \in B$ as $x = b_2 b_1^{-1} \in B$. Therefore $x \in A \cap B = \{1\}$. Thus

$$x = a_2^{-1} a_1 = 1$$

which implies $a_1 = a_2$. Likewise $x = b_2 b_1^{-1} = 1$ implies $b_1 = b_2$. This completes the proof that f is injective.

The size of the Cartesian product $A \times B$ is $|A \times B| = mn = |G|$ and f is injective therefore the image of f fills out all of G. That is every element, g, of G is of the form $g = f(a, b) = ab$, which is precisely what we wanted to show. □

Anther basic result have shown is Cauchy's Theorem.

Theorem 4 (Cauchy's Theorem)**.** *Let* G *be a finite group and* p *a prime with* $p \,\big|\, |G|$*. Then* G *has an element of order* p*.* □

Anther fact we have used several times is

Proposition 5. *If* G *is a group and* H *is a subgroup of* G *of index* 2*, then* H *is normal in* G*.* □

Here is an application of these results.

Proposition 6. *If* G *is a nonAbelian group with* $|G| = 38$*. Then* G *is isomorphic to the dihedral group* D_{19}*.*

Proof. We have $|G| = 38 = 2 \cdot 19$. Therefore $2 \,\big|\, |G|$ and $19 \,\big|\, |G|$ and 2 and 19 are both prime. By Cauchy's Theorem this implies that G has an element b with $o(b) = 2$ and an element a with $o(a) = 19$. Let $A = \langle a \rangle$ and $B = \langle b \rangle$ be the cyclic groups generated by these elements. Then $|A| = 19$ and $|B| = 2$.

As $\gcd(2,19) = 1$ Proposition 3 gives that $G = AB$. That is every element of G is of the form $g = a^i b^j$ for some i and j.

The subgroup $A = \langle a \rangle$ has index two in G (as $|G| = 2|A|$) and therefore A is normal. This means that for every $g \in G$ we have $gAg^{-1} = A$ and therefore (letting $g = b$) we have $bab^{-1} \in A = \langle a \rangle$. As elements of $\langle a \rangle$ are just the powers of a this implies

$$bab^{-1} = a^k$$

for some integer k. Then by the result of Problem 1 and that $b^2 = 1$ this implies

$$a = 1a1^{-1} = b^2ab^{-2} = a^{k^2}.$$

This implies

$$a^{k^2-1} = 1.$$

Therefore $19 = o(a) \,\big|\, (k^2 - 1)$. That is

$$k^2 \equiv 1 \pmod{19}.$$

By Proposition 1 this implies $k \equiv \pm 1 \pmod{19}$. If $k \equiv 1 \pmod{19}$, then

$$bab^{-1} = a^1 = a$$

which implies $ba = ab$. As elements of G are of the form $g = a^i b^j$ this implies G is Abelian and we are assuming G is nonAbelian. Therefore $k \equiv -1 \pmod{19}$. This gives that

$$bab^{-1} = a^{-1}$$

which can be rewritten as $ba = a^{-1}b$. Thus G is generated by two elements a and b with

$$a^{19} = 1, \qquad b^2 = 1, \qquad ba = a^{-1}b.$$

This is our standard representation of the dihedral group and so G is isomorphic to D_{19}. $\square$

The previous proposition generalizes:

Theorem 7. *Let p be an odd prime. Then every nonAbelian group G with $|G| = 2p$ is isomorphic to D_p.*

Problem 3 (25 points). Prove this. $\square$

Problem 4 (15 points). In the symmetric group S_6 let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 2 & 6 & 5 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 4 & 6 & 2 \end{pmatrix}$$

(a) Write σ and τ, σ^{-1} and $\sigma\tau$ in cycle notation.
(b) If $\alpha, \beta \in S_6$ have are

$$\alpha = (123)(46), \qquad \beta = (2345)$$

compute $\alpha\beta$ and β^{-1} and write the result in cycle notation. $\square$

Problem 5 (15 points). In the symmetric group S_7

(a) Given an example of an element of order 7.
(b) Give an example of an element of order 10.

Problem 6 (30 points). Let $F = \mathbb{Z}_2$ be the field with two elements and let $f(x) = x^2 + 1$. Note that in $F = \mathbb{Z}_2$ that $2 = 0$ and $-1 = 1$. Therefore the polynomial $f(x)$ can be factored as

$$f(x) = x^2 + 1 = x^2 - 1 = (x - 1)(x + 1) = (x + 1)^2.$$

Therefore $f(x)$ is *not* irreducible. Let $I = \langle f(x) \rangle$ be the principle ideal in $F[x]$ generated by $f(x)$ and let R be the quotient ring

$$R = F[x]/I$$

and let a be the element of R given by

$$a = x + I$$

(a) Explain why every element of R is of the form $u + va$ with $u, v \in \mathbb{Z}_2$ and therefore that R has four elements

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

(b) Show that $a^2 = 1$ in R.
(c) Give the addition and multiplication tables for R.
(d) Show that R is not a field.
(e) Find all solutions to $y^2 = 0$ with $y \in R$. □

One of the main results we have shown about polynomial rings is

Theorem 8. *If F us a field, then every ideal in the ring $F[x]$ is principal. That is if I is an ideal then $I = \langle h(x) \rangle$ for some polynomial $h(x)$. (Where $\langle h(x) \rangle$ is the set of multiples of $h(x)$ in $F[x]$. The element $h(x)$ is called a **generator** of I.)* □

Problem 7 (10 points). Let $\mathbb{Q}$ be the field of rational numbers and let α be a real number (which does not have to be rational). Show that

$$I = \{f(x) \in \mathbb{Q}[x] : f(\alpha) = 0\}$$

is an ideal in $\mathbb{Q}[x]$. □

Problem 8 (15 points). Let m be a positive integer such that $\sqrt{m}$ is irrational and let I be the ideal of $\mathbb{Q}[x]$ defined by

$$I = \{f(x) \in \mathbb{Q}[x] : f(\sqrt{m}) = 0\}.$$

Show that $h(x) = x^2 - m$ is a generator of I. *Hint:* You may use the fact, which was used in our proof of Theorem 8, that a polynomial in an ideal of smallest degree is a generator of the ideal. Note that $h(x) = x^2 - m \in I$. Show that I does not have any elements of degree 1 (this is where you use that $\sqrt{m}$ is irrational) and therefore $x^2 - m$ has the smallest degree of any element of I. □

About the last result we covered in class was

Theorem 9. *Let $\phi \colon R \to S$ be a surjective ring homomorphism where R and S are rings. Then*

$$S \cong R/\ker(\phi).$$

(Here $R_1 \cong R_2$ means the rings are isomorphic.)

We saw on the last test that the set

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

is a sub-field of the field of real numbers when $\sqrt{m}$ is irrational.

Problem 9 (15 points). With S as just defined define a map $\phi \colon \mathbb{Q}[x] \to S$ by

$$\phi(f(x)) = f(\sqrt{m}).$$

It is not hard to show this is a ring homomorphism and you can assume that it is. Use this fact, Problem 8 and Theorem 9 to show

$$\mathbb{Q}[x]/\langle x^2 - m\rangle \cong S. \qquad \square$$

Problem 10 (5 points). Put your name on the first page and have this in on time. $\square$