Math 1530 Final Exam Spring 2013

Name: _____

- The exam will last 3 hours.
- There are 9 problems worth 12 points each.
- No notes or other study materials allowed.
- Please turn your phone off.
- Use the back side of the test pages for scratch work, or if you need extra space.

1	
2	
3	
4	
5	
6	
7	
8	
9	
Total	

Problem 1. Determine whether the following statements are **True** or **False**:

(a) Every subgroup of a cyclic group is cyclic.

Solution. True. □

(b) Every group is isomorphic to a subgroup of a permutation group.

Solution. True: this is Cayley's theorem. Namely G embeds faithfully into S_G when it acts on itself by left multiplication. □

(c) If a group G acts on a set A and $a \in A$, then the number of elements in the orbit of a divides $|G|$.

Solution. True. $|\mathcal{O}_a| = [G : S_G(a)]$ where $S_G(a)$ is the stabilizer of a. □

(d) If I and J are ideals of a ring R, then the set $\{ab : a \in I, b \in J\}$ is an ideal in R.

Solution. False in general. The correct replacement is IJ which consists of *finite sums* of elements of the form ab, where $a \in I$ and $b \in J$. □

Problem 2. Let R be an integral domain and complete the following statements.

(a) An ideal $I \subseteq R$ is *principal* if and only if:

Solution. $I = (a)$ is generated by a single element $a \in R$. □

(b) An element $r \in R$ is *irreducible* if and only if:

Solution. r is not a unit and $r = ab$ implies that a or b is a unit. □

(c) R is a *Euclidean Domain* if and only if:

Solution. R is an integral domain, there exists a norm $N : R \longrightarrow \mathbb{N}$ (meaning $N(0) = 0$) and for any a, b in R there exist $q, r \in R$ such that $a = q\,b + r$, and $N(r) < N(b)$ or $r = 0$. □

(d) R is a *Unique Factorization Domain* if and only if:

Solution. Every element $r \in R$ can be written as a finite product of irreducibles $r = p_1 \cdots p_n$, which are unique up to associates (multiplication by units), and the order in which they appear. □

Problem 3. Let $G = \mathbb{Z}/60\mathbb{Z}$ and $\phi : G \longrightarrow G'$ a group homomorphism to another group G'. List the possible isomorphism types for the image group $\mathrm{Im}(\phi)$.

Solution. By the first isomorphism theorem, $\mathrm{Im}(\phi) \cong R/\ker(\phi)$ where $\ker(\phi)$ may be any normal subgroup in G. Since G is abelian this may be any subgroup. The subgroups in G are those generated by divisors of 50 (if you like, by the lattice isomorphism theorem, or we proved this directly in class), so $G = \langle 1\rangle, \langle 2\rangle, \langle 5\rangle, \langle 10\rangle, \langle 25\rangle$, and $\langle 50\rangle = \{0\}$.

For any of these, $G/\langle n\rangle \cong \mathbb{Z}/n\mathbb{Z}$, say, by the third isomorphism theorem: $G/\langle n\rangle = (\mathbb{Z}/50\mathbb{Z})/(n\mathbb{Z}/50\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. (We also proved this directly in class, I believe.)

So the possible isomorphism types are

$$\{0\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/25\mathbb{Z},\ \mathbb{Z}/50\mathbb{Z}. \qquad \square$$

Problem 4. Let G be an abelian group. Show that the set $R = \mathrm{Hom}(G, G)$ of (not necessarily invertible) group homomorphisms from G to itself, equipped with the operations of pointwise addition and composition, has the structure of a ring with identity.

Solution. First observe that R is closed under these operations; if $f, h \in R$ then $f + h$ and $f \circ h$ are homomorphisms, since for $g_1, g_2 \in G$,

$$\begin{gathered}(f+h)(g_1+g_2) = f(g_1+g_2) + h(g_1+g_2) \\ = f(g_1) + h(g_1) + f(g_2) + h(g_2) = (f+h)(g_1) + (f+h)(g_2), \\ (f \circ h)(g_1+g_2) = f\big(h(g_1+g_2)\big) = f\big(h(g_1)\big) + f\big(h(g_2)\big) = (f\circ h)(g_1) + (f \circ h)(g_2)\end{gathered}$$

Next, under pointwise addition, R forms an abelian group: the additive identity is the 0 homomorphism $0(g) = 0$ for all G, the inverse of a homomorphism f is given by the homomorphism $-f$ taking $g \in G$ to $-f(g) \in G$, and that addition is associative and commutative in R follows from associativity and commutativity of addition in G.

Multiplication is given by composition, which is associative. It distributes over addition on the left by the homomorphism property:

$$\big(f \circ (h+l)\big)(g) = f\big(h(g) + l(g)\big) = f\big(h(g)\big) + f\big(l(g)\big) = (f\circ h)(g) + (f \circ l)(g),$$

and on the right directly:

$$\big((f+h)\circ l\big)(g) = (f+h)(l(g)) = f\big(l(g)\big) + h\big(l(g)\big) = (f\circ l)(g) + (h\circ l)(g).$$

The multiplicative identity is given by the identity homomorphism $1(g) = g$ for all $g \in G$. $\square$

Problem 5. Suppose $\phi : R \longrightarrow F$ is a ring homomorphism from a ring R to a field F. Prove that $\ker(\phi)$ is a prime ideal.

Solution. By the first isomorphism theorem,

$$R/\ker(\phi) \cong \mathrm{Im}(\phi) \subseteq F.$$

F is a field, and therefore also an integral domain, so $\mathrm{Im}(\phi)$ has no zerodivisors. This is equivalent to $\ker(\phi)$ being prime.

Alternatively, this may be proved directly. Suppose $ab \in \ker(\phi)$. Then

$$0 = \phi(ab) = \phi(a)\phi(b) \implies \phi(a) = 0 \text{ or } \phi(b) = 0$$

since F has no zerodivisors. Thus $a \in \ker(\phi)$ or $b \in \ker(\phi)$, so $\ker(\phi)$ is prime. $\square$

Problem 6. Let $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

(a) Show that $p(x)$ is irreducible, and deduce that $K = \mathbb{F}_2[x]/\big(p(x)\big)$ is a field in which $p(x)$ has a root. What is the order of K (i.e. how many elements does it have)?

Solution. By direct inspection, $p(0) = 1 \neq 0$ and $p(1) = 1 \neq 0$, so $p(x)$ has no roots. Since $\deg\big(p(x)\big) = 3$, this shows $p(x)$ is irreducible. It follows that $p(x)$ is prime, hence $\big(p(x)\big)$ is prime and therefore maximal (since $\mathbb{F}_2[x]$ is a PID), so K is a field. Letting $\theta = x \mod \big(p(x)\big)$ be the image of x in K, it follows that $p(\theta) = 0 \in K$. Since p has degree 3, $[K : F] = 3$ so K has $2^3 = 8$ elements. □

(b) Let θ be a root of $p(x)$ in K, and compute $\dfrac{1+\theta+\theta^2}{1+\theta} \in K$. Your answer should be of the form $a + b\theta + c\theta^2$, where $a, b, c \in \mathbb{F}_2$.

Solution. Using division with remainder,

$$x^3 + x + 1 = (x^2 + x)(x + 1) + 1 \implies 1 = (x^2 + x)(x + 1) + (x^3 + x + 1)$$

so that $(1 + \theta)^{-1} = \theta + \theta^2 \in K$. Next,

$$(x^2 + x + 1)(x^2 + x) = x^4 + x = x(x^3 + x + 1) + x^2$$

so that

$$\frac{1+\theta+\theta^2}{1+\theta} = (1 + \theta + \theta^2)(\theta + \theta^2) = \theta^2 \in K.$$

□

Problem 7. Let R be a ring with elements $a, b \in R$. We say $m \in R$ is a *least common multiple* if both a and b divide m, and if m' is any other element divisible by both a and b then m divides m'. If R is a PID, prove that a least common multiple always exists.

Solution. There are (at least) three ways to prove this. First, translating the LCM property into the language of ideals, it follows that m is a least common multiple of a and b if $(m) \subseteq (a) \cap (b)$ and if $(m') \subseteq (a) \cap (b)$, then $(m') \subseteq (m)$.

Since R is a PID, the ideal $(a) \cap (b)$ is principal, so $(a) \cap (b) = (m)$ for some m, which is therefore a least common multiple.

Alternatively, we can use the fact that a PID is a UFD and suppose that $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = vp_1^{\beta_1} \cdots p_n^{\beta_n}$ be factorizations of a and b into irreducibles p_i (here u and v are units). Then a least common multiple is given by

$$m = p_1^{\max(\alpha_1, \beta_1)} \cdots p_n^{\max(\alpha_n, \beta_n)}.$$

Finally a method which did not occur to me before writing this problem but which was used by a few students is to construct a least common multiple from a greatest common divisor. Let $(d) = (a, b)$ so d is a GCD of a and b (using the PID property). Then since $ab \in (a, b) = (d)$ it follows that

$$ab = md, \quad \text{for some } m \in R,$$

and m can be shown to be a least common multiple. Indeed, since d divides a, $a = a'd$ for some a', so

$$ab = a'bd = md \implies a'b = m \iff b \mid m.$$

Similarly $a \mid m$. If $a \mid m'$ and $b \mid m'$ for some other m', then

$$m' = c_1 a = c_2 b.$$

Multiplying by b and a respectively, one gets

$$\begin{aligned} bm' &= c_1 ab, \quad & am' &= c_2 ab, \\ bm' &= c_1 md, \quad & am' &= c_2 md, \end{aligned}$$

Now $d = xa + yb$ for some $x, y \in R$ (this is one of the properties of a GCD and can be seen from the fact that $d \in (a, b) \equiv (a) + (b)$.) so,

$$\begin{aligned} dm' = xam' + ybm' = xc_2 md + yc_1 md = md(xc_2 + yc_1), \\ \implies m' = m(xc_2 + yc_1), \end{aligned}$$

so m divides m'. (Hat tip to Ittai Baum for this proof). $\square$

Problem 8. Let G be a finite group of order $56 = 7 \cdot 2^3$. Prove that G must have a normal subgroup. (Hint: Use the Sylow theorem and then count the elements of various orders.)

Solution. By the Sylow theorem the number $n_7(G)$ of Sylow 7-subgroups satisfies

$$n_7(G) \equiv 1 \mod 7, \quad n_7(G) \mid |G| = 56,$$

from which it follows that $n_7(G)$ is either 1 or 8. In the first case G has a unique, and hence normal, subgroup of order 7.

In the case that $n_7(G) = 8$, the eight Sylow 7-subgroups must intersect trivially (since they have the same prime order the intersection of two of them is a subgroup, hence must be trivial or else they would be the same). Thus there are $8 \cdot 6 = 48$ elements of order 7 in G, which leaves room for only $56 - 48 = 8$ other elements including the identity. None of the elements of order 7 can be in a Sylow 2-subgroup, which must have order $2^3 = 8$, so there must be exactly one Sylow 2-subgroup, which is therefore normal. $\square$

Problem 9. Let $f(x) = x^2 - (\alpha+\beta)x + \alpha\beta = (x-\alpha)(x-\beta) \in \mathbb{C}[x]$, where $\alpha \neq \beta \in \mathbb{C}$. Describe all the ideals in the ring $R = \mathbb{C}[x]/\big(f(x)\big)$.

Solution. By the lattice isomorphism theorem, the ideals in R are in bijection with the ideals I in $\mathbb{C}[x]$ containing $\big(f(x)\big)$. Since $\mathbb{C}[x]$ is a PID, such an $I = \big(p(x)\big)$ for some $p(x)$ and then the fact that $\big(f(x)\big) \subseteq I = \big(p(x)\big)$ is equivalent to

$$p(x) \;\big|\; f(x) = (x-\alpha)(x-\beta).$$

Since $(x-\alpha)$ and $(x-\beta)$ are irreducible and $\mathbb{C}[x]$ is a UFD, the only possibilities are

$$p(x) = u, \quad p(x) = v(x-\alpha), \quad p(x) = w(x-\beta), \text{ or } \quad p(x) = z(x-\alpha)(x-\beta)$$

where $u, v, w, z \neq 0$ are units, corresponding to ideals

$$I = \mathbb{C}[x], \quad I = (x-\alpha), \quad I = (x-\beta), \text{ or } \quad I = \big(f(x)\big).$$

In R these descend to the ideals

$$R, \quad (\overline{x}-\alpha), \quad (\overline{x}-\beta), \text{ or} (0),$$

where $\overline{x}$ denotes the image of x in R. $\square$