Math 343K (Rusin) Exam 2, Lucky Friday Apr 13, 2012. **ANSWERS**

1. Suppose G is a group containing two subgroups H and K.

(a) Give the definition: what does it mean to say K is normal in G?

(b) Show that if K is normal in G, then

$$HK = \{hk \,|\, h \in H, k \in K\}$$

is a subgroup of G.

(Remark: this statement can be false when K is not normal in G, for example if $G = Sym(3)$, $H = \{e, (12)\}$, and $K = \{e, (13)\}$.)

ANSWER: Normality means that for every $k \in K$ and every $g \in G$ it must be true that $g^{-1}kg$ also lies in K. Replacing g by g^{-1}, it is equivalent to insist that $gkg^{-1} \in K$ for every $g \in G$.

HK is not empty, since it contains $e = ee \in HK$. We must show HK is closed under products and inverses. So suppose h_1k_1 and h_2k_2 are two elements of HK. Their product is $h_1(k_1h_2)k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2$; but $h_1h_2 \in H$ and also $(h_2^{-1}k_1h_2)k_2 \in K$ since K is normal in G. Similarly $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$.

2. Recall that in any group G, the *center* of G is

$$Z(G) = \{g \in G | \text{ for all } h \in G, gh = hg\}$$

For every group G, $Z(G)$ is a normal subgroup of G (you do NOT have to prove this) and so we may form the quotient group $G/Z(G)$.

Show that if $G/Z(G)$ is cyclic, then G is abelian.

ANSWER: (I will abbreviate $Z(G)$ as just Z.) Suppose G/Z is cyclic; then there is a generator a, meaning every element of G/Z is a power of this a. But the elements of G/Z are all cosets, so in particular we may write $a = gZ$ for some $g \in G$. Thus all the cosets of $G/Z(G)$ may be written as $a^n = (gZ)^n = g^nZ$ for some n.

But every element of G lies in one of these cosets; that means every element of G may be written as g^nz for some integer n and some $z \in Z$. So now we can see that G is abelian:

$$(g^{n_1}z_1)(g^{n_2}z_2) = g^{n_1}g^{n_2}z_1z_2 = g^{n_2}g^{n_1}z_2z_1 = (g^{n_1}z_1)(g^{n_2}z_2)$$

because z_1 commutes with g^{n_1} and with z_2, and because the two powers of g commute with each other.

Note that since G is abelian, $Z(G)$ is all of G, and thus all of G is in one single coset: $G/Z(G)$ is the trivial (i.e. one-element) group!

3. An element r of a ring R is called *idempotent* if $r^2 = r$.

(a) List the idempotents of $\mathbf{Z}/10$.

(b) Show that if r is an idempotent, so is $1 - r$.

(c) Show that the ideals $I = rR$ and $J = (1-r)R$ have no elements in common except 0. (Hint: Find a way to get an equation into your proof, and then multiply that equation by r.)

ANSWER: (a) is essentially asking for the digits whose square ends with that same digit; the answers are $0, 1, 5, 6$. It is significant that these are precisely the elements of $\mathbf{Z}/10$ that are congruent to 0 or 1 modulo 2 and also congruent to 0 or 1 modulo 5. I invite you to explain why that is relevant, to form a conjecture, and to prove your conjecture!

(b) $(1-r)^2 = 1 - 2r + r^2 = 1 - 2r + r = 1 - r$

(c) An element a in the intersection can be written both as $a = rx$ and $a = (1-r)y$ for some x and y in R. Thus we have $rx = (1-r)y$. Multiply by r to get $a = rx = r^2x = r(1-r)y = (r-r^2)y = (r-r)y = 0y = 0$.

4. (a) Show that if $\phi : R \longrightarrow S$ is a homomorphism of rings, then $\ker(\phi)$ is an ideal in R.

(b) Use this to prove that whenever R is a field, every homomorphism from R to any (nonzero) ring is one-to-one. (Hint: first decide what $\ker(\phi)$ would have to be.)

ANSWER: Let $I = \ker(\phi)$. This I is closed under sums because if $a, b \in I$ then $\phi(a+b) = \phi(a) + \phi(b) = 0 + 0 = 0$, showing that $a + b \in I$ too. Similarly if $a \in I$ and $r \in R$ then $\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0$, showing that $ra \in I$ as well.

As above, $\ker(\phi)$ is an ideal of R, but fields have only two ideals, R itself and $\{0\}$. The kernel of ϕ cannot be all of R because it doesn't contain 1_R: homomorphisms have to send 1_R to 1_S, not to 0_S. So $\ker(\phi) = \{0\}$.

Now, if $\phi(x) = \phi(y)$ then $\phi(x-y) = \phi(x) - \phi(y) = 0$, meaning $(x-y) \in I$. But then $x - y = 0$, i.e. $x = y$. So ϕ is one-to-one.

5. An element r of a ring R is called a *square* if there is another element $s \in R$ with $r = s^2$. (This s is then called a *square root* of r, naturally.)

(a) Find all the square roots of 1 in $\mathbf{Z}/8$.

(b) Show that $1-4X$ is not a square in $\mathbf{R}[X]$. (Here $\mathbf{R}$ is the ring of all real numbers.)

(Extra Credit) Show that $1-4X$ is a square in $\mathbf{R}[[X]]$

ANSWER: (a) Squaring all eight candidates, we find that only $1^2 = 3^2 = 5^2 = 7^2 = 1$. But that's cool, eh? An element with FOUR different square roots!

(b) Since $\mathbf{R}$ is a field, the degree of the product of two polynomials is the sum of their degrees; in particular, squares have even degree, while $1-4X$ has odd degree.

(c) You don't have to "find" the square root; it suffices to demonstrate how it could be found. Here's the idea. Let $P_1 = 1 - 2X \in \mathbf{R}[[X]]$. Then $P_1^2 = 1 - 4X + 4X^2$ agrees with $Q = 1 - 4X$ through the linear term, i.e. $Q - P_1^2$ is a multiple of X^2. Now we will show that if we are given a polynomial P_{n-1} of degree $n-1$ for which $Q - P_{n-1}^2$ is a multiple of X^n, then for some constant $c \in \mathbf{R}$ it will be true that $P_n := P_{n-1} + cX^n$ makes $Q - P_n^2$ be a multiple of X^n. Indeed, for any c, we will have $Q - P_n^2 = (Q - P_{n-1}^2) - 2cX^nP_{n-1} + c^2X^{2n}$ which is a multiple of X^n. Since the constant term of P_{n-1} is 1, we see that the coefficient of X^n in the whole expression will vanish if c is chosen to equal half the coefficient in in $Q - P_{n-1}^2$. Continuing in this way, we can compute each of the coefficients of P to have $Q - P^2 = 0$, namely $P = 1 - 2X - 2X^2 - 4X^3 - 10X^4 - 28X^5 \ldots$. (The coefficients may also be obtained from the binomial theorem: the coefficient of X^i is $-(2^i)(2i-3)(2i-5)(\ldots)(3)(1)/i!$, which is also -2 times the central number of in the $(2i-1)$th row of Pascal's Triangle.)

NB — I just gave a formula for the coefficient of X^i in P that can be computed on a calculator with around $2i$ ring operations in $\mathbf{Z}$. Obviously you can compute the coefficient modulo N with the same number of ring operations in $\mathbf{Z}_N$. What's the fastest way you can compute these coefficients mod N if, say, $i = 2^{100}$? There's no way you can ever carry out 2^{100} iterations of anything. If you can find a way to compute that coefficient mod N (for, say, a 100-digit N) with let's say a mere billion ring operations, I can promise you much fame and fortune as a mathematician and cryptographer! See me for details ...

6. Show that if R and S are isomorphic rings, then the groups of units $U(R)$ and $U(S)$ are isomorphic groups.

ANSWER: If $\phi : R \longrightarrow S$ is an isomorphism, then ϕ also provides an isomorphism between the two groups of units. Indeed, $xy = 1$ implies $\phi(x)\phi(y) = 1$, so that if x is a unit in R, then $\phi(x)$ is a unit in S. Similarly if z is a unit in S then $\phi^{-1}(z)$ is a unit in R. So ϕ establishes a one-to-one correspondence between the two sets of units, and has the homomorphism property (for groups) because ϕ preserves multiplication (of rings).