ASSIGNMENT 5 – ELEMENTARY NUMBER THEORY MATH 392

Eyal Goren, November 11, 1998

1. Let $\phi : G_1 \longrightarrow G_2$ be a homomorphism of groups.

(a) Prove that if H is a subgroup of G_1 then $\phi(H)$ is a subgroup of G_2.

(a) Prove that if H is a subgroup of G_2 then $\phi^{-1}(H)$ is a subgroup of G_1, where $\phi^{-1}(H) = \{g \in G_1 : \phi(g) \in H\}$.

2. Let G be a group. Prove that

$$\sum_{g \in G} g = \sum_{g \in G;\ \mathrm{ord}(g)=2} g.$$

Conclude Wilson's theorem: Let p be a prime number then

$$(p-1)! \equiv -1 \pmod{p}.$$

3. Let R be a ring.

(A) Given elements $a_1, \cdots, a_r$ of R. Consider the set

$$Ra_1 + Ra_2 + \cdots + Ra_r$$

and denote it by $(a_1, \cdots, a_r)$. Prove it's an ideal.

(B) Let I and J be two ideals of R and let IJ denote the set of all finite sums $d_1 + \cdots + d_t$ in which each d_ℓ is a product of an element from I and an element from J. That is,

$$IJ = \{d_1 + \cdots + d_t : \forall \ell, \exists (i_\ell \in I, j_\ell \in J), d_\ell = i_\ell j_\ell\}.$$

Prove that IJ is an ideal of R.

(C) Prove that if $I = (a_1, \cdots, a_\alpha)$ and $J = (b_1, \cdots, b_\beta)$, then $IJ = (c_{11}, \cdots, c_{ij}, \cdots, c_{\alpha\beta})$, where $c_{ij} = a_i b_j$.

4 Write the proof of Lagrange's theorem on sum of squares in *complete* detail.

5 (A) Let p be a prime and $f(x)$ be a polynomial of degree d and coefficients in $\mathbb{Z}/p\mathbb{Z}$. Prove that f has atmost d roots.

(B) Show by an example that if p is not a prime, the assertion needs no longer be true.

6 Write a fully detailed proof of the Quadratic Reciprocity Law, following Baker's book. In particular, check that the transformation

$$x = \frac{1}{2}(q+1) - x'; \;\; y = \frac{1}{2}(p+1) - y',$$

appearing there, does give a bijection between the integer points in the regions appearing in the proof.

7 Find the number of solutions for the following equations in $\mathbb{Z}/65537\mathbb{Z}$ (65537 is a prime number...):

(A) $x^2 + y^2 = -1$.

(B) $x^2 + y^2 = 3$.

(C) $2x^2 + y^2 = 1$.