MATH 113: INTRODUCTION TO ABSTRACT ALGEBRA
AUTUMN 2007
SOLUTIONS TO MIDTERM 2 PRACTICE PROBLEMS

1. Compute $3^{5,789,345}$ in $\mathbb{Z}_{70}$.

Solution: $70 = 2 \cdot 5 \cdot 7$, a product of distinct prime numbers. Hence, $\mathbb{Z}_{70}^{\times} \cong \mathbb{Z}_2^{\times} \times \mathbb{Z}_5^{\times} \times \mathbb{Z}_7^{\times}$ has $1 \cdot 4 \cdot 6 = 24$ elements. Dividing, one computes that the remainder of $5,789,345$ upon division by 24 is 17. Thus, $3^{5,789,345} = 3^{17}$ in $\mathbb{Z}_{70}$. Multiplying, we find that

n	3^n
1	3
2	9
3	29
4	11
5	33
6	29
7	17
8	51
9	13
10	39
11	47
12	1

Hence $3^{17} = 3^{12}3^5 = 33$.

2. Prove or disprove: If G is a group and $K \trianglelefteq G$ and $N \trianglelefteq G$ are two normal subgroups which are isomorphic to each other, $N \cong K$, then $G/K \cong G/N$.

Solution: The above statement is false. Consider for example, $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, $N = 2\mathbb{Z}_4 \times \{0\}$ and $K = \{0\} \times \mathbb{Z}_2$, then $N \cong K \cong \mathbb{Z}_2$, but $G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ while $G/K \cong \mathbb{Z}_4$.

3. Let $R := \{f \mid f : \mathbb{Z} \to \mathbb{Z}\}$ be the set of functions from the integers to the integers. Define $+$ on R by $(f + g)(x) := f(x) + g(x)$ and $\cdot$ on R by $(f \cdot g)(x) = (f \circ g)(x) = f(g(x))$. Prove or disprove: $(R, +, \cdot)$ is a ring.

Solution: With the multiplication defined above, R is *not* a ring as the left distributive property fails. Let f be the function $x \mapsto x^2$, g the function $x \mapsto x + 1$ and h the function $x \mapsto x - 1$. Then $f \cdot (g + h)(2) = f(g(2) + h(2)) = f(4) = 16$ while $(f \cdot g + f \cdot h)(2) = f(g(2)) + f(h(2)) = 9 + 1 = 10$.

4. Prove or disprove: if G is a group of order 32, then there is a group H of order 16 and a homomorphism $\phi : G \to H$ which is onto.

Note: This question is substantially more difficult than the questions you will find on the exam.

Solution: As $32 = 2^5$ is a power of a prime, $Z(G)$, the center of G, is nontrivial. It is easy to see that the abelian group $Z(G)$ has a subgroup K of order two. Indeed, let $g \in Z(G)$ be any nonidentity element. Then the cyclic group generated by g has order dividing the order of G and is in particular a power of two, 2^r for some $r > 0$. Let $h := g^{2^{r-1}}$. Then h^2 is the identity element but h is nontrivial. Set $K := \{e, h\}$. As K is a subgroup of the center of G, $K \trianglelefteq G$. Indeed, for any $g \in G$ and $x \in Z(G)$ we have $gx = xg$ so that $gxg^{-1} = x$. Thus, $gKg^{-1} = K$. Set $H := G/K$ and let $\phi : G \to H$ be the natural quotient map. By Lagrange's Theorem, $\#H = 32/2 = 16$.

5. Let $G = S_{\mathbb{R}}$ be the group of permutations of the real numbers. Let $H \leq G$ be the subgroup of G consisting of those permutations which fix all but finitely many points. That is, $\pi \in H \iff \{x \in \mathbb{R} \mid \pi(x) \neq x\}$ is finite. Is H a normal subgroup of G? Prove that your answer is correct.

Solution: Yes, $H \trianglelefteq G$. Let $\sigma \in G$ and $\pi \in H$. Then as π and σ are permutations, $\{x \in \mathbb{R} : \sigma\pi\sigma^{-1}(x) \neq x\} = \{x \in \mathbb{R} : \pi\sigma^{-1}(x) \neq \sigma^{-1}(x)\} = \sigma\{x \in \mathbb{R} : \pi(x) \neq x\}$ is also finite. Hence, $\sigma H \sigma^{-1} \leq H$. As σ was arbitrary, we conclude that $H \trianglelefteq G$.

6. Describe $(\mathbb{Z}_{12} \times \mathbb{Z}_3)/\langle(2, 2)\rangle$.

Solution: We compute that $\langle(2, 2)\rangle = \{(0, 0), (2, 2), (4, 1), (6, 0), (8, 2), (10, 1)\}$ has order six. Hence, by Lagrange's Theorem, the factor group has order $(12 \times 3)/6 = 6$. As the quotient of an abelian group is abelian, the quotient group must be isomorphic to $\mathbb{Z}_6$.

7. Let R be an integral domain and $a, b, c \in R$ elements of R. Show that there are at most three elements x of R satisfying $x^3 + ax^2 + bx + c = 0$.

Remark: This problem takes too much work given what we know at this point. Next week, after we have studied factorization of polynomials, it will be an easy exercise.

8. Prove or disprove: If G is a group and $H \leq G$ is any subgroup, then there is a one-to-one and onto function $f : G/H \to H\backslash G$. [Note: G is not assumed to be finite.]

Solution: Define a function $f : G/H \to H\backslash G$ by $aH \mapsto Ha^{-1}$. Let us check that this function is well-defined. If $aH = a'H$, then there is some $h \in H$ for which $a' = ah$. So $H(a')^{-1} = H(ah)^{-1} = Hh^{-1}a^{-1} = Ha^{-1}$ as $h^{-1} \in H$. Thus, f is well-defined. Define $g : H\backslash G \to G/H$ by $Ha \mapsto a^{-1}H$. A similar calculation shows that g is well-defined and clearly $f \circ g = \mathrm{id}_{H\backslash G}$ and $g \circ f = \mathrm{id}_{G/H}$. Hence, f is one-to-one and onto.

9. Prove or disprove: If G is a group, $H \leq G$ is a subgroup and $\#G/H = 2$, then $H \lhd G$.

Solution: This statement is true. By problem 8, we know $\#(H\backslash G) = 2$. Hence, for any $g \in G \setminus H$ we have $G \setminus H = gH = Hg$ while clearly for any $g \in H$ we have $gH = H = Hg$. Thus, $H \lhd G$.

10. What is the exponent of S_8?

Solution: 840.

11. Is there a subgroup of $S_5 \times \mathbb{R}$ which is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_5$? If so, exhibit such a group. If not, prove that it cannot exist.

Remark: As stated, this question is too hard.

Solution: Such a group cannot exists. Suppose that $G \leq S_5 \times \mathbb{R}$ is a subgroup isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_5$. Let $\pi : S_5 \times \mathbb{R} \to S_5$ be the projection onto the first coördinate and $\rho : S_5 \times \mathbb{R} \to \mathbb{R}$ the projection onto the second coördinate. Both of these maps are homomorphisms. The image $\rho[G] \leq \mathbb{R}$ is a finite subgroup of $\mathbb{R}$ and as such must be trivial as every nonzero real number has infinite order. Thus, $G \leq S_5 \times \{0\}$. So $G \cong \pi[G] \leq S_5$. However, $\#G = \#(\mathbb{Z}_5 \times \mathbb{Z}_5) = 25$ while $\#S_5 = 120$ which is not divisible by 25 contrary to Lagrange's Theorem.

12. Let $F := \mathcal{C}([0,1])$ be the set of continuous real-valued functions of the interval $[0,1]$. F is a ring when we define $(f+g)(x) := f(x)+g(x)$ and $(f \cdot g)(x) := f(x)g(x)$. Let $I : F \to \mathbb{R}$ be defined by $I(f) := \int_0^1 f(x)x^2 dx$. Is I is a homomorphism of *rings*? Is it a homomorphism of additive *groups*?

Solution: I is *not* a homomorphism of rings as, for example, $I(1) = \int_0^1 x^2 dx = \frac{1}{3}x^3|_{x=0}^{x=1} = \frac{1}{3} \neq 1$. It is, however, a homomorphism of groups: $I(f+g) = \int_0^1 (f+g)(x)x^2 dx = \int_0^1 (f(x)x^2 + g(x)x^2)dx = \int_0^1 f(x)x^2 dx + \int_0^1 g(x)x^2 dx = I(f) + I(g)$.

13. Prove or disprove: If G is an abelian group and $n \in \mathbb{Z}_+$ is any positive integer, then $nG := \{g \in G \mid (\exists h \in G) g = nh := \overbrace{h + \cdots + h}^{n \text{ times}}\}$ is a normal subgroup and $G/nG \cong \mathbb{Z}_n$.

Solution: It is true that $nG \trianglelefteq G$, but it is not true that G/nG is necessarily isomorphic to $\mathbb{Z}_n$. For example, if $G = \mathbb{R}$, then $nG = G$ so that G/nG is trivial.

14. What is the multiplicative inverse of 13 in $\mathbb{Z}_{19}$?

Solution: $13^{-1} = 3$ in $\mathbb{Z}_{19}$ as $3 \times 13 = 39 = 1 + 38 = 1 + 2 \times 19$.

15. Prove or disprove: For every positive integer $a < 223$, there is an integer x for which the remainder of $129x$ upon division by 223 is a.

Solution: Dividing 223 by 3 and 43, one checks that 129 and 223 are relatively prime. [In fact, 223 is prime.] Hence, 129 is invertible in $\mathbb{Z}_{223}$. Let $b \in \mathbb{Z}_{223}$ be the inverse of 129. Then set $x := ba$ so that $129x = 129ba = (129b)a = a$ in $\mathbb{Z}_{223}$. That is, the remainder of $129ba$ upon division by 223 is a.