NAME:Key

MATH 553

Fall 2015

Midterm Exam

October 21, 2015

Instructions: Give a complete solution to each problem. You may use any result from class, the book, or homework **except** the statement you are asked to prove. Be sure to justify your statements.

1. (a) **(5 points)** Show, for any abelian group, the map $x \mapsto x^{-1}$ is an automorphism.

   (b) **(11 points)** Show, for any n, the dihedral group D_{2n} of order $2n$ satisfies $D_{2n} \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_n$.

   Solution:

   (a) Let G be an abelian group. Let $\varphi : G \to G$ be given by $\varphi(x) = x^{-1}$. Then $\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$, since G is abelian. Now $\varphi(xy) = \varphi(x)\varphi(y)$, so φ is a homomorphism. Note, $\ker \varphi = \{1\}$, so φ is injective. For any x we have $x = (x^{-1})^{-1} = \varphi(x^{-1})$ so φ is surjective. Thus $\varphi \in \operatorname{Aut}(G)$ $\square$

   (b) $G = D_{2n} = \langle r, s, | r^n = s^2 = 1, srs^{-1} = r^{-1}\rangle$. Now $K = \langle r \rangle \simeq \mathbb{Z}_n \lhd G$, since $|G : K| = 2$. Also, $H = \langle s \rangle \simeq \mathbb{Z}_2$. Note, since K is normal, HK is a group and $HK \supsetneq K$, so $HK = G$. Since $H \cap K = \{1\}$ we have $G = H \ltimes K$, and so $G \simeq \mathbb{Z}_2 \ltimes \mathbb{Z}_n$.

   Note: The solution could end here, but you could also note the following. Since $srs^{-1} = r^{-1}$, we have $sr^ks^{-1} = r^{-k}$, for all k. So if $\varphi : H \to \operatorname{Aut}(K)$ is given by $\varphi(s)(x)^{-1}$, we have $G = H \ltimes_\varphi K$. $\square$

2. **(25 points)** Show there is no simple group of order $306 = 2 \cdot 3^2 \cdot 17$.

   Solution Let $|G| = 306$. For any prime p we let $\operatorname{Syl}_p(G)$ be the collection of Sylow p–subgroups of G, and set $n_p = |\operatorname{Syl}_p(G)|$. If By Sylow's Theorems, if $n_p = 1$

and P is the unique Sylow p–subgroup, then $P \triangleleft G$. Let $P \in \mathrm{Syl}_{17}(G)$. Then, by Sylow's Theorems, $n_{17} \equiv 1 \pmod p$ and $n_{17} \mid |G : P| = 18$, so $n_{17} = 1$ or 18. Suppose $n_{17} = 18$. If $P \neq Q, \in \mathrm{Syl}_{17}(G)$, then $P \cap Q = \{1\}$, so there must me $18 \cdot 16 = 288$ elements of order 17. Now $n_3 \equiv 1 \pmod 3$ and $n_3 \mid |G : Q| = 34$, where $Q \in \mathrm{Syl}_3(G)$. If $n_{17} = 18$, and $n_3 = 34$, then we would need to create 34 subgroups of order 9 from 17 remaining non-identity elements, which is absurd, since if $Q_1, Q_2 \in \mathrm{Syl}_3(G)$ and $Q_1 \neq Q_2$,b then $|Q_1 \cap Q_2| \leq 3$. So either $n_{17} = 1$, or $n_3 = 1$, and in either case there is some nontrivial proper normal subgroup N of G, so G is not simple. □

3. **(10 points)** Suppose R is a ring with identity, and I, J, and A are (two sided) ideals of R with $A \subset I \cup J$. Prove either $A \subset I$ or $A \subset J$.

   Solution: Suppose $A \not\subset I$ and $A \not\subset J$. Then we have $x, y \in A$, with $x \in I \setminus J$ and $y \in J \setminus I$. Now $x + y \in A$, so $x + y \in I$ or $x + y \in J$. Now, if $x + y \in I$, then $y = (x + y) - x \in I$ which contradicts our choice of y. Similarly, if $x + y \in J$, then $x \in J$, which is a contradiction. Thus, either $A \subset I$ or $A \subset J$. □

4. Let R and S be rings and suppose $\varphi : R \to S$ is a ring homomorphism. Let I be an ideal of R and J an ideal of S.

   a) **(10 points)** Show that $\varphi^{-1}(J) = \{r \in R | \varphi(r) \in J\}$ is an ideal in R.

   b) **(10 points)** Show that if φ is surjective, then $\varphi(I) = \{\varphi(r) | r \in I\}$ is an ideal in S.

   c) **(5 points)** Give an example where φ is not surjective and $\varphi(I)$ is not an ideal in S.

   Solution:

   (a) Since φ is a homomorphism of the additive groups, we have $\varphi^{-1}(J)$ is an additive subgroup of R. Now, if $r \in R$ and $x \in \varphi^{-1}(J)$, then $\varphi(x) \in J$, and since J is an ideal $\varphi(r)\varphi(x) = \varphi(rx) \in J$. Thus, $rx \in \varphi^{-1}(J)$. Similarly, $xr \in \varphi^{-1}(J)$ so$\varphi^{-1}(J)$ is an ideal of R.

(b) Again, since φ is a homomorphism of additive groups, we have $\varphi(I)$ is an additive subgroup of S. If $x \in \varphi(I)$ and $s \in S$, then, since φ is surjective, we can find $y \in I$ and $r \in R$ with $\varphi(y) = x$ and $\varphi(r) = s$. Now $sx = \varphi(r)\varphi(y) = \varphi(ry)$. Since I is an ideal of R we have $ry \in I$, so $sx \in \varphi(I)$. Similarly, $xs \in \varphi(I)$, so $\varphi(I)$ is an ideal.

(c) There are several examples, but a simple one if to let $\varphi : \mathbb{Z} \to \mathbb{Z}[x]$ be the inclusion. Then $I = 2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but not of $\mathbb{Z}[x]$, since $2 \cdot x \notin 2\mathbb{Z}$. $\square$

5. **(12 points each)**

(a) Let R be a commutative ring with identity $1 \neq 0$. Suppose that, for every $r \in R$, there is some $n = n_r \geq 2$ so that $r^n = r$. Prove that every prime ideal of R is maximal.

(b) Suppose R is a unique factorization domain, $p \in R$ is irreducible, and P is a prime ideal with $0 \subsetneq P \subset (p)$. Show $P = (p)$. (Hint: Prove P can be generated by irreducible elements.)

Solution:

(a) Let P be a prime ideal of R. Consider R/P and let $r + P = \bar{r} \neq \bar{0} = P \in R/P$. So, $r \notin P$. Now, for some $n \geq 2$, we have $r^n = r$, so $\bar{r}^n = \bar{r}$. So in the integral domain R/P (since P is prime) we have $\bar{r} \cdot \bar{r}^{n-1} = \bar{r} \cdot \bar{1}$. Thus, by cancellation (again, R/P is an integral domain) we have $\bar{r}^{n-1} = \bar{1}$, with $n - 1 \geq 1$. Thus $\bar{r}^{n-1}$ is a unit, so R/P is a field. Therefore, P is a maximal ideal.

(b) First suppose X is a generating set for P, i.e., $(X) = P$. Let $x \in X$. Then $x = p_1 p_2 \cdots p_r$, with p_i irreducible in R. Since P is a prime ideal, we have $p_x = p_i \in P$ for at least one i. Now $x \in (p_x)$. So let $Y = \{p_x | x \in X\}$. Then $X \subset (Y) \subset P = (X)$, so $P = (Y)$, i.e. P can be generated by irreducible elements. Now let $q \in P$ be irreducible. Then $q \in (p)$, so $q = pu$ for some $u \in R$. Since p and q are irreducible, we must have u is a unit and p and q are associates. Thus $(p) = (q) \subset P \subset (p)$, so $P = (p)$. $\square$