# HOMEWORK 5

JASON MEDCOFF

**97iii.** We want to show that if $f : (H \times K) \to H$ is an homomorphism, $K^*$ is the kernel of $f$ and therefore a normal subgroup of $(H \times K)$ by the first isomorphism theorem. In addition, we must show that the image of $f$ is $H$; then it follows from the first isomorphism theorem that $(H \times K)/K^*$ is isomorphic to $H$. Namely, we take $f$ that maps $(h, k) \mapsto h$ for $h \in H$ and $k \in K$.

First, $f$ is a homomorphism since

$$f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2 = f(h_1, k_1)f(h_2, k_2).$$

We know that we can write

$$\begin{aligned}\ker f &= \{(h, k) \in (H \times K) : f(h, k) = 1_H\} \\ &= \{(1_H, k) \in (H \times K)\} \\ &= K^*\end{aligned}$$

and therefore $K*$ is a normal subgroup of $(H \times K)$. Next, we want to show that the image of $f$ is the entirety of $H$. In particular,

$$\begin{aligned}\text{im } f &= \{h \in H : \exists (h, k) \in (H \times K), f(h, k) = h\} \\ &= \{h \in H\} \\ &= H\end{aligned}$$

since the first element in $(h, k)$ can be chosen from $H$ arbitrarily. Thus, $H$ is the image of $f$, and so is isomorphic to the quotient group $(H \times K)/K^*$.

**98.** Suppose $G/Z(G)$ is cyclic with generator $g$. Then the cosets of $Z(G)$ are of the form $g^iZ(G)$. Since these cosets partition $G$, every element of $G$ belongs to one coset. Take $a = g^iz_1$ and $b = g^jz_2$ for some $z_1$, $z_2 \in Z(G)$. Then we can write

$$ab = g^iz_1g^jz_2 = g^ig^jz_1z_2 = g^{i+j}z_1z_2 = g^{j+i}z_2z_1 = g^jg^iz_2z_1 = g^jz_2g^iz_1 = ba$$

since $z_1$ and $z_2$ belong to the center and thus commute with every element in $G$. Thus $G$ is abelian. The conclusion is exactly the contrapositive of this.

**99.** Since every element in $G$ appears in one coset of $H$, it follows from Lagrange's theorem that

$$|G| = |G/H||H|.$$

Write $|G/H| = p^x$ and $|H| = p^y$. Then

$$|G| = |G/H||H| = p^xp^y = p^{x+y}$$

and so the order of $G$ is a power of $p$.

**105.** Let $H$ be any other subgroup of $G$ with order $|K|$. Define $f : G \to G/K$. Then $f(H)$ is a quotient group of $H$ and thus $|f(H)|$ divides $|H| = |K|$. By the first isomorphism theorem, $f(H)$ is a subgroup of $G/K$ so $|f(H)|$ also divides $[G : K]$. Then it must be that $|f(H)| = 1$. Then $H \subseteq K$, but since they have the same cardinality, $H = K$.

**106.** First, suppose $HK$ is a subgroup of $G$, with $h \in H$ and $g \in G$. Then $h = h1 \in HK$ and $k = 1k \in HK$, therefore $kh \in HK$. So $KH \subseteq HK$. We must also have $(hk)^{-1} \in HK$, so it must follow that $(hk)^{-1} = h'k'$ for $h' \in H$, $k' \in K$. Then $hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH$ since $k'^{-1} \in K$, $h'^{-1} \in H$. Thus $HK \subseteq KH$, so if $HK$ is a subgroup in $G$, $HK = KH$.

Conversely, suppose that $HK = KH$. Then let $a$, $b \in HK$. Then $a = h_a k_a$ and $b = h_b k_b$ for $h_a$, $h_b \in H$ and $k_a$, $k_b \in K$. Then $k_a h_b \in KH = HK$, so $k_a h_b = hk$ for some $h \in H$ and $k \in K$. Therefore

$$ab = h_a k_a h_b k_b = h_a h k k_b \in HK$$

as $h_a h \in H$ and $kk_b \in K$. Then

$$a^{-1} = (h_a k_a)^{-1} = k_a^{-1} h_a^{-1} \in KH = HK$$

so $HK$ is closed under multiplication and inverses. Thus, $HK$ is a subgroup of $G$.

**113.** i) Suppose $x$, $y \in G$. Then their commutator is $xyx^{-1}y^{-1}$. Take $g \in G$, then

$$g(xyx^{-1}y^{-1})g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}$$

and thus the conjugate of the commutator of $x$ and $y$ is the commutator of $gxg^{-1}$ and $gyg^{-1}$. Then for $x_i$ and $y_i$ in $G$ for $1 \le i \le n$ we have

$$g\bigg(\prod_1^n x_i y_i x_i^{-1} y_i^{-1}\bigg)g^{-1} = g(x_1 y_1 x_1^{-1} y_1^{-1})\bigg(\prod_2^n x_i y_i x_i^{-1} y_i^{-1}\bigg)g^{-1} = \cdots = \prod_1^n g x_i y_i x_i^{-1} y_i^{-1} g^{-1}$$

and since the conjugate of a commutator is a commutator, and the conjugate of a product of commutators is a product of commutators, and is therefore in $G'$. So $G'$ is normal in $G$.

ii) Let $aG'$ and $bG' \in G/G'$. Then $aG'bG' = (ab)G' = ba(a^{-1}b^{-1}ab)G' = (ba)G'$ since the commutator is in $G'$. Thus $G/G'$ is abelian.

iii) We want to show that every commutator maps to the identity.

$$\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}$$

and since these elements commute and cancel to the identity, $G' \le \ker\varphi$.

iv) Since $G/G'$ is abelian, every subgroup of it is normal. Subgroups of $G/G'$ correspond to subgroups of $G$ that contain $G'$, and normal subgroups of $G/G'$ correspond to normal subgroups of $G$ containing $G'$. Thus, any subgroup containing $G'$ is also normal.

**30.** Take $x \in R[x]$. If it had an inverse, say $f(x)$, then $xf(x) = 1$. But then if $f(x)$ is of degree $n$, $1 = xf(x)$ has degree $n+1$. But $\deg(xf(x)) = \deg(1) = 0$, a contradiction. So $x$ does not have an inverse, and therefore $R[x]$ is not a field.

**31.** i) Addition associativity is inherited from ordinary matrix addition. Commutativity of addition exists from the same reason. The additive identity is the zero matrix, taking $c_i = 0\ \forall i$. Inverses exist, since every entry is in $k$, and everything in $k$ has an inverse; let each entry $a_{ij}$ in a matrix in $k[A]$ be $-a_{ij}$ in the matrix's inverse. Multiplicative associativity is inherited from matrix multiplication; so is distributivity over addition. The multiplicative identity is inherited as the identity matrix, which is in $k[A]$ as $f(A)$ with $c_0 = 1$, all other $c_i = 0$. To demonstrate commutativity of multiplication, take $f(A) = a_0 I + a_1 A + \cdots + a_m A^m$ and $g(A) = b_0 I + b_1 A + \cdots + b_m A^m$. Then

$$\begin{aligned} f(A)g(A) &= a_0 b_0 + (a_1 b_0 + a_0 b_1)A + \ldots \\ &= b_0 a_0 + (b_1 a_0 + b_0 a_1)A + \ldots \\ &= g(A)f(A). \end{aligned}$$

ii) Part i) showed that $k[A]$ is a ring, for any choice in $A$ over $k$. Then if $f(x)$ factors into $p(x)q(x)$ over $k$, $f(A)$ factors into $p(A)q(A)$ over $k$ since they have the same underlying field.

iii) Let $A = I$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. $k[A]$ is a domain since every element will be of the form $\begin{bmatrix} k & 0 \\ 0 & k \end{bmatrix} = kI$, and so no two elements $kI$ and $jI$ can multiply to zero since $kIjI = kjI^2 = kjI \neq 0$. $k[B]$ is not a domain since $B^2 = 0$ yet $B \neq 0$.

**32.** i) If $R$ is a domain, so is $R[x]$. Then the degree of a product of two polynomials is the sum of the degree of each. Thus, $f(x)$ can only be a unit if its degree is zero, and its inverse is thus of degree zero. But an invertible constant is a unit in $R$.

ii) $(2x+1)(2x+1) = 4x^2 + 4x + 1$. Modulo 4, the first two terms are zero, so this is always 1.

**33.** We know from Fermat's little theorem that for prime $p$ and any $x$,

$$x^p \equiv x \mod p.$$

In other words,

$$x^p - x \equiv 0 \mod p$$

for all $x$, so letting $f(x) = x^p - x$, we have that $f^b$ will always evaluate to zero.