Math 661 **Fall 2013**
Homework 1 Solutions **Drew Armstrong**

1. Let $H \leq G$ be a subgroup. Call the identity element 1.

(a) State the definition of equivalence relation.

Proof. Let $R \subseteq G \times G$ be a subset and write $a \sim b$ to mean that $(a, b) \in R$. We say that $\sim$ is an equivalence relation on the set G if

- $\forall\, a \in G$, $a \sim a$ (reflexive),
- $\forall\, a, b \in G$, $a \sim b \Rightarrow b \sim a$ (symmetric),
- $\forall\, a, b, c \in G$, $a \sim b$ and $b \sim c \Rightarrow a \sim c$ (transitive). $\square$

(b) Define a relation on G by setting $a \sim_H b \Leftrightarrow a^{-1}b \in H$. Prove that this is an **equivalence** relation on G.

Proof. **Reflexive:** For all $a \in G$ we have $a^{-1}a = 1 \in H$, hence $a \sim_H a$. **Symmetric:** If $a \sim_H b$ (i.e. $a^{-1}b \in H$) then we also have $(a^{-1}b)^{-1} = b^{-1}a \in H$ (i.e. $b \sim_H a$). **Transitive:** Suppose that $a \sim_H b$ and $b \sim_H c$ (i.e. $a^{-1}b \in H$ and $b^{-1}c \in H$). Then we also have $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$ (i.e. $a \sim_H c$). $\square$

(c) Given an element $g \in G$ we define the left coset $gH := \{gh : h \in H\}$. Prove that $a \sim_H b$ **if and only if** $aH = bH$.

Proof. First suppose that $a \sim_H b$, so that $a = bk$ for some $k \in H$, and let ah (with $h \in H$) be an artibrary element of aH. Then we have $ah = bkh = b(kh) \in bH$, hence $aH \subseteq bH$. The proof of $bH \subseteq aH$ is similar.

Conversely, suppose that $aH = bH$. Since $a \in aH = bH$ we have $a = bk$ for some $k \in H$. Then $a^{-1}b = k^{-1} \in H$, hence $a \sim_H b$. $\square$

(d) Prove that the map $g \mapsto ag$ is a **bijection** from H to aH.

Proof. Consider the map $G \to G$ defined by $g \mapsto a^{-1}g$. Since an arbitrary element of aH looks like ah for some $h \in H$ we see that the map sends $aH \to H$. Since this maps also inverts the map $g \mapsto ag$ we conclude that both maps are bijective. $\square$

(e) If $|G|$ is finite, prove that $|H|$ **divides** $|G|$.

Proof. Since $\sim_H$ is an equivalence relation (by part (b)) we know that the equivalence classes (left H cosets) partition the set G. Let G/H denote the set of left H cosets. Since each coset has the same size (by part (d)) we conclude that $|G/H| \cdot |H| = |G|$. $\square$

(f) For all $a \in G$ prove that $a^{|G|} = 1$. [Hint: Use part (e).]

Proof. Let $H = \langle a \rangle \leq G$ be the cyclic subgroup generated by a, so that $a^{|H|} = 1$. Then by part (e) we have $a^{|G|} = a^{|H| \cdot |G/H|} = (a^{|H|})^{|G/H|} = 1^{|G/H|} = 1$. $\square$

(g) Finally, let $G = (\mathbb{Z}/n\mathbb{Z})^\times$ (i.e. the group of units of the ring $\mathbb{Z}/n\mathbb{Z}$). What does the result of (f) say in this case?

Proof. Let $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ (Euler's totient function). Then for all a coprime to n we have $a^{\varphi(n)} \equiv 1 \bmod n$. This is called Euler's Theorem. When n is prime, it's called Fermat's Little Theorem. $\square$

2. Let $K \leq G$ be a subgroup and let G/K denote the **set** of left cosets of K. Consider the surjective **map of sets** $\varphi : G \to G/K$ defined by $\varphi(a) := aK$.

(a) **Suppose** there exists some group operation on G/K such that φ is a group homomorphism. In this case, what is the identity element of G/K? What is $\ker \varphi$?

Proof. If φ is a homomorphism then $1_{G/K} = \varphi(1_G) = 1K = K$. Then we have $\ker \varphi = \{a \in G : aK = K\}$, which equals K by Problem 1(c). $\square$

(b) If G' is any group and $\psi : G \to G'$ is any group homomorphism, prove that $\ker \psi$ is a **normal** subgroup of G (i.e. prove that $gkg^{-1} \in \ker \psi$ for all $g \in G$ and $k \in \ker \psi$).

Proof. Given $a, b \in \ker \psi$ we have $\psi(a^{-1}b) = \psi(a)^{-1}\psi(b) = 1^{-1}1 = 1$, hence $a^{-1}b \in \ker \psi$ and we conclude that $\ker \psi$ is a subgroup of G (you didn't need to show this). Now consider any $g \in G$ and $k \in \ker \psi$. Then we have $\psi(gkg^{-1}) = \psi(g)\psi(k)\psi(g)^{-1} = \psi(g)1\psi(g)^{-1} = \psi(g)\psi(g)^{-1} = 1$, hence $gkg^{-1} \in \ker \psi$ and we conclude that $\ker \psi \trianglelefteq G$. $\square$

(c) Now suppose that $K \trianglelefteq G$ is normal (i.e. suppose that $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$). In this case, prove that the operation $(G/K) \times (G/K) \to G/K$ given by $(aK, bK) \mapsto (ab)K$ is **well-defined**.

Proof. Suppose that $(aK, bK) = (a'K, b'K)$, so by Problem 1(c) we have $a = a'k_1 \in K$ and $b = b'k_2 \in K$. In this case we wish to show that $(ab)K = (a'b')K$. So consider an arbitrary element $abk \in (ab)K$ with $k \in K$. Then we have $abk = a'k_1b'k_2k = a'b'((b')^{-1}k_1b')k_2k$, and since $(b')^{-1}k_1b' \in K$ by normality, we conclude that $abk \in (a'b')K$, hence $(ab)K \subseteq (a'b')K$. The proof of $(a'b')K \subseteq (ab)K$ is similar. $\square$

(d) Moreover, prove that this operation makes G/K into a **group**. (And hence the original φ is a group homomorphism.)

Proof. Let's call the operation $aK \cdot bK = (ab)K$. We must show that this operation is **associative**, with an **identity element**, and that **inverses exist**. **Associative:** For all $a, b, c \in G$ we have $aK \cdot (bK \cdot cK) = aK \cdot (bc)K = (a(bc))K = ((ab)c)K = (ab)K \cdot cK = (aK \cdot bK) \cdot cK$, since G is a group. **Identity:** Note that for all $a \in G$ we have $aK \cdot 1K = (a1)K = aK = (1a)K = 1K \cdot aK$, hence $1K$ is an identity element for G/K. **Inverses:** For all $a \in G$ we have $aK \cdot a^{-1}K = (aa^{-1})K = 1K = (a^{-1}a)K = a^{-1}K \cdot aK$, hence $a^{-1}K$ is an inverse for aK. $\square$

(e) Finally, let $H \leq G$ be any subgroup. Prove that H is **normal if and only if** there exists a group G' and a group homomorphism $\mu : G \to G'$ such that $\ker \mu = H$.

Proof. First suppose that $\mu : G \to G'$ is a group homomorphism with $\ker \mu = H$. Then by part (b) we see that $H \trianglelefteq G$.

Conversely, suppose that $H \trianglelefteq G$. Then by parts (a), (b) and (d) we can define a group G/H such that the map $\mu : G \to G/H$ defined by $g \mapsto gH$ is a group homomorphism with $\ker \mu = H$. $\square$

3. Let R be a commutative ring with 1 and let $I \leq R$ be an ideal.

(a) Finish the sentence: We say that R is an integral domain if ...

Proof. for all $a, b \in R$ with $ab = 0$ we have $a = 0$ or $b = 0$. $\square$

(b) Finish the sentence: We say that I is a prime ideal if ...

Proof. for all $a, b \in R$ with $ab \in I$ we have $a \in I$ or $b \in I$. $\square$

(c) If R/I is an integral domain, prove that I must be prime.

Proof. Let R/I be an integral domain and suppose that $ab \in I$ for some $a, b \in R$. Then we have $(a + I)(b + I) = ab + I = I$. Since R/I is an integral domain this implies $a + I = I$ (i.e. $a \in I$) or $b + I = I$ (i.e. $b \in I$). $\square$

(d) If I is prime, prove that R/I must be an integral domain.

Proof. Let I be prime and suppose that $(a+I)(b+I) = I$ for some $a, b \in R$. Then we have $ab + I = (a + I)(b + I) = I$, hence $ab \in I$. Since I is prime this implies $a \in I$ (i.e. $a + I = I$) or $b \in I$ (i.e. $b + I = I$). $\square$

(e) Finish the sentence: We say that R is a field if ...

Proof. every nonzero element $0 \neq a \in R$ has a multiplicative inverse $a^{-1} \in R$. $\square$

(f) Finish the sentence: We say that I is a maximal ideal if ...

Proof. for all ideals $I < J$ we have $J = R$. $\square$

(g) If R/I is a field, prove that I must be maximal.

Proof. Let R/I be a field. The correspondence theorem says there is a 1-1 correspondence between nontrivial ideals of R/I and ideals of R strictly between I and R. Suppose that $J < R/I$ is a nonzero ideal with $a+I \in J$. Since R/I is a field we have $b+I \in R/I$ with $(a+I)(b+I) = 1+I \in J$. But then $(r+I)(1+I) = r+I \in J$ for all $r \in R$, hence $J = R/I$. We conclude that R/I has no nontrivial ideals, and hence there are no ideals between I and R. $\square$

(h) If I is maximal, prove that R/I must be a field.

Proof. Suppose that the ideal $I < R$ is maximal and consider a nonzero element $a + I \in R/I$ (i.e. $a \notin I$). Then the inclusion of ideals $I < (a) + I$ implies that $(a) + I = R$. Since $1 \in R = (a) + I$ there exists $b \in R$ and $u \in I$ such that $1 = ab + u$. Finally we have $(a + I)(b + I) = ab + I = 1 - u + I = 1 + I$, hence $(a + I)$ is invertible. $\square$

(i) Finally, explain why every maximal ideal is prime.

Proof. If I is maximal then R/I is a field by part (h). But then R/I is also an integral domain, hence I is prime by part (c). $\square$

4. Let $F \subseteq K$ be a field extension with $\alpha \in K$, and consider the ring of polynomials $F[x]$. Let $\varphi_\alpha : F[x] \to K$ be the ring homomorphism defined by $\varphi_\alpha(x) := \alpha$ and $\varphi_\alpha(a) := a$ for all $a \in F$. We use the notation $\varphi_\alpha(f(x)) = f(\alpha)$.

(a) Prove that $I := \ker \varphi_\alpha$ is an **ideal** of $F[x]$.

Proof. Given any two elements $f(x), g(x) \in I$ we have $\varphi_\alpha(f(x) + g(x)) = f(\alpha) + g(\alpha) = 0 + 0 = 0$, hence $f(x) + g(x) \in I$. Furthermore, for any $f(x) \in I$ and $h(x) \in F[x]$ we have $\varphi_\alpha(f(x)h(x)) = f(\alpha)h(\alpha) = 0 \cdot h(\alpha) = 0$, hence $f(x)h(x) \in I$. $\square$

(b) Prove that this ideal $I \leq F[x]$ is **principal**. [Hint: If $I \neq (0)$ then choose $0 \neq f(x) \in I$ with minimal degree. Show that $I \subseteq (f(x))$.]

Proof. If $I = (0)$ there is nothing to show. So suppose that $I \neq (0)$ and choose nonzero $f(x) \in I$ with minimal degree (this is possible by the well-ordering principle). Since $f(x) \in I$ we have $(f(x)) \subseteq I$. We wish to show that $I \subseteq (f(x))$.

To do this, choose any $g(x) \in I$ and divide by $f(x)$ to get $g(x) = q(x)f(x) + r(x)$ where either: (1) $\deg(r) < \deg(f)$ or (2) r is the zero polynomial. We note that (1) is impossible since $r(x) = g(x) - q(x)f(x) \in I$ and $f(x)$ was assumed to have minimal degree. Hence $r(x) = 0$ and we conclude that $g(x) \in (f(x))$. This shows that $I \subseteq (f(x))$ as desired. $\square$

(c) By part (b) we can write $I = (m_\alpha(x))$ for some monic $m_\alpha(x) \in F[x]$. Prove that this $m_\alpha(x)$ is **irreducible** over F.

Proof. Suppose that $m_\alpha(x) = f(x)g(x)$ for some $f(x), g(x) \in F[x]$. Applying the evaluation map φ_α gives $f(\alpha)g(\alpha) = m_\alpha(\alpha) = 0$, and without loss of generality we suppose that $f(\alpha) = 0$ (i.e. $f(x) \in (m_\alpha(x))$). We now know that $m_\alpha(x) = f(x)g(x)$ and $f(x) = m_\alpha(x)h(x)$ for some $h(x) \in F[x]$, hence $f(x) = f(x)g(x)h(x)$ or $f(x)(1 - g(x)h(x)) = 0$. Since $F[x]$ is a domain this implies $g(x)h(x) = 1$ hence $g(x), h(x)$ are units and $f(x), m_\alpha(x)$ are associates. We conclude that $m_\alpha(x)$ has no proper factor. $\square$

(d) Use the first isomorphism theorem to prove that $F \subseteq \operatorname{im} \varphi_\alpha \subseteq K$ is a **field**.

Proof. Clearly we have $F \subseteq \operatorname{im} \varphi_\alpha \subseteq K$. Then by the first isomorphism theorem we have $\operatorname{im} \varphi_\alpha \approx F[x]/\ker \varphi_\alpha = F[x]/(m_\alpha(x))$. Since $F[x]$ is a PID, any strictly larger ideal $(m_\alpha(x)) < (p(x))$ would imply a proper factor. But $m_\alpha(x)$ is irreducible by part (c), hence the ideal $(m_\alpha(x))$ is maximal. By Problem 2(h) we conclude that $\operatorname{im} \varphi_\alpha$ is a field. $\square$

(e) If L is any intermediate field $F \subseteq L \subseteq K$ such that $\alpha \in L$, prove that $\operatorname{im} \varphi_\alpha \subseteq L$. (Hence $\operatorname{im} \varphi_\alpha$ is the **smallest** subfield of K containing F and α.)

Proof. Let $f(x) = \sum_k a_k x^k$ be any element of $F[x]$. Then by definition we have $\varphi_\alpha(f(x)) = f(\alpha) = \sum_k a_k \alpha^k$. Since L is a field containing a_i and α^i for all i, we have $f(\alpha) \in L$. $\square$