# Abstract Algebra Homework 7

Michael Nelson

## Problem 1

**Proposition 0.1.** *Let $K \subseteq L$ be an extension of fields and let $\alpha \in L$ be algebraic over $K$ of odd degree. Then $K(\alpha^2) = K(\alpha)$.*

*Proof.* It suffices to show that $K(\alpha) \subseteq K(\alpha^2)$ since the other direction is clear. The extension of fields

$$K \subseteq K(\alpha^2) \subseteq K(\alpha)$$

gives us the relation

$$[K(\alpha) : K] = [K(\alpha) : K(\alpha^2)][K(\alpha^2) : K] \tag{1}$$

We claim that $[K(\alpha) : K(\alpha^2)] \leq 2$. Indeed, let denote $n = [K(\alpha) : K]$. Then a $K$-basis of $K(\alpha)$ is given by

$$\{\alpha^i \mid 0 \leq i \leq n-1\}.$$

It follows that

$$\{\alpha^{2i} \mid 0 \leq 2i \leq n-1\}$$

is a linearly independent set in $K(\alpha^2)$. Therefore $[K(\alpha^2) : K] \geq n/2$, which implies

$$\begin{aligned} [K(\alpha) : K(\alpha^2)] &= \frac{[K(\alpha) : K]}{[K(\alpha^2) : K]} \\ &= \frac{n}{[K(\alpha^2) : K]} \\ &\leq \frac{n}{n/2} \\ &= 2. \end{aligned}$$

and hence $[K(\alpha) : K(\alpha^2)] \leq 2$ by (1).

Now combining (1) with the fact that $2 \nmid [K(\alpha) : K]$, we see that $2 \nmid [K(\alpha) : K(\alpha^2)]$. Therefore $[K(\alpha) : K(\alpha^2)] = 1$, which implies $K(\alpha) = K(\alpha^2)$. $\square$

*Remark.* Note that if $\alpha$ was transcendental, then all we say can is $K(\alpha^2)$ is *strictly* contained in $K(\alpha)$. Indeed, assume for a contradiction that $K(\alpha^2) = K(\alpha)$. Then $\alpha \in K(\alpha^2)$ implies

$$\alpha = a_0 + a_2\alpha^2 + a_4\alpha^4 \cdots + a_{2N}\alpha^{2N}$$

for some $N \in \mathbb{N}$ and $a_0, a_2, a_4, \ldots, a_{2N} \in K$. However this would imply $\alpha$ is algebraic over $K$, which is a contradiction.

## Problem 2

### Problem 2.a

**Lemma 0.1.** *Let $A$ be a finite abelian group. Then the order of every element must divide the maximal order.*

*Proof.* From the fundamental theorem of finite abelian groups, we have an isomorphism

$$A \cong \mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_n}$$

where $k_1 \mid \cdots \mid k_n$. Let $e_1, \ldots, e_n$ denote the standard $\mathbb{Z}$-basis for $\mathbb{Z}^n$, and let $\overline{e}_i$ denote the corresponding coset in $\mathbb{Z}_{k_i}$ for each $1 \leq i \leq n$. Since $k_i \mid k_n$ we see that $k_n$ kills each $\mathbb{Z}_{k_i}$ for all $1 \leq i \leq n$. Therefore $k_n$ kills all of $A$. In particular, the order of every element must divide $k_n$, which is in fact the maximal order as $k_n = \operatorname{ord}(\overline{e}_{i_n})$. $\square$

**Lemma 0.2.** *The number of roots of a polynomial over a field is at most the degree of the polynomial.*

*Proof.* Let $K$ be a field and let $f(T)$ be a polynomial coefficients in $K$. By replacing $K$ with a splitting field of $f(T)$ if necessary, we may assume that $f(T)$ splits into linear factors over $K$, say

$$f(T) = (T - \alpha_1) \cdots (T - \alpha_n).$$

where $\alpha_1, \ldots \alpha_n \in K$ and $n = \deg f(T)$. Let $\alpha \in K$. Then we have

$$\begin{aligned} f(\alpha) = 0 &\iff (\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0 \\ &\iff \alpha - \alpha_i = 0 \text{ for some } i \\ &\iff \alpha = \alpha_i \text{ for some } i, \end{aligned}$$

where we obtained the second line from the first line from the fact that $K$ is an integral domain. Therefore $f(T)$ has *at most* $n$ roots. □

**Proposition 0.2.** *Let $K$ be a field and let $G$ be a finite subgroup of $K^\times$. Then $G$ is cyclic.*

*Proof.* Let $n = |G|$ and let $m$ be the maximal order among all elements in $G$. We will show $m = n$. By Lagrange's Theorem, we have $m \mid n$, and hence $m \leq n$. It follows from Lemma (0.1) that every order of every element must divide the maximal order. In particular, we have $x^m = 1$ for all $x \in G$. Therefore all numbers in $G$ are roots of the polynomial $T^m - 1$. By Lemma (0.2), the number of roots of a polynomial over a field is at most the degree of the polynomial, so $n \leq m$. Combining both inequalities gives us $m = n$. □

## Problem 2.b

**Proposition 0.3.** *Let $K$ be a finite field. Then the product of two nonsquares in $K$ is a square in $K$.*

*Proof.* By problem 2.a, $K^\times$is cyclic. Choose $\gamma \in K^\times$ such that $K^\times = \langle \gamma \rangle$.

**Step 1:** Assume that $\operatorname{char} K = 2$. Thus $|K| = 2^k$ for some $n \geq 1$. We claim that every number is a square. Indeed, clearly $0$ is a square of itself. Also, for any $\gamma^i \in K^\times$, we have

$$\begin{aligned} \gamma^i &= (\gamma^i)^{2^k} \\ &= (\gamma^i)^{2 \cdot 2^{k-1}} \\ &= (\gamma^{i(2^{k-1})})^2. \end{aligned}$$

Thus every number is a square.

**Step 2:** Now assume that $\operatorname{char} K \neq 2$ and denote $n = |K^\times|$. We claim that the set of all nonsquares in $K$ is given by

$$\{\gamma^{2i+1} \in K^\times \mid 1 \leq 2i + 1 \leq n - 2\}. \tag{2}$$

Indeed, assume for a contradiction that $\gamma^{2i+1} = (\gamma^j)^2 = \gamma^{2j}$ for some $\gamma^j \in K^\times$. If $2i + 1 \geq 2j$, then this implies

$$\gamma^{2(i-j)+1} = 1. \tag{3}$$

Then (3) implies $2(i - j) + 1 \mid n - 1$, which is a contradiction since $2(i - j) + 1$ is odd and $n - 1$ is even. Similarly, if $2j \geq 2i + 1$, then

$$\gamma^{2(j-i)-1} = 1,$$

which implies $2(j - i) - 1 \mid n - 1$. Again this is a contradiction since $2(j - i) - 1$ is odd and $n - 1$ is even. Therefore every number in (2) is a nonsquare. In fact it contains *all* nonsquares, since as a set, we can partition $K$ as

$$K = \{0\} \cup \{\gamma^{2i} \in K^\times \mid 0 \leq 2i \leq n - 3\} \cup \{\gamma^{2i+1} \in K^\times \mid 1 \leq 2i + 1 \leq n - 2\}.$$

Clearly $\{\gamma^{2i} \in K^\times \mid 0 \leq 2i \leq n - 3\}$ and $\{0\}$ consists of square elements.

**Step 3:** Let $\gamma^{2i+1}$ and $\gamma^{2j+1}$ be nonsquares in $K$ for some $1 \leq 2i + 1, 2j + 1 \leq n - 2$. Then their product is a square:

$$\begin{aligned} \gamma^{2i+1}\gamma^{2j+1} &= \gamma^{2i+2j+2} \\ &= (\gamma^{i+j+1})^2. \end{aligned}$$

Thus the product of two nonsquares is a square. □

## Problem 2.c

**Proposition 0.4.** *Let $K$ be a finite field. Then each number in $K$ is the sum of two squares.*

*Proof.* If $\operatorname{char} K = 2$, then every element is a square (by step 1 in problem 2.b), and hence is a sum of two squares. Therefore we may assume that $\operatorname{char} K \neq 2$. Let $a \in K$ and denote $n = |K|$. Consider the following sets

$$S = \{x \in K \mid x \text{ is a square}\} \quad \text{and} \quad a - S = \{a - x \in K \mid x \text{ is a square}\}.$$

We claim that $|a - S| = |S|$. Indeed, let $\varphi \colon K \to K$ be the negation map given by

$$\varphi(x) = -x$$

for all $x \in K$ and let $\psi \colon K \to K$ be the addition by $a$ map given by

$$\psi(x) = a + x$$

for all $x \in A$. Then $\varphi$ is a bijection since $-1$ is a unit and $\psi$ is a bijection since $K$ is a group under addition, and thus their composite $\psi\varphi$ is a bijection. In particular, it restricts to a bijection $S \to a - S$ since

$$\psi\varphi(S) = a - S.$$

Finally, by step 2 in problem 2.b, we know that more than half of the numbers in $K$ are squares. Therefore since $|S| > n/2$, $|a - S| > n/2$, and

$$\begin{aligned} |S \cup (a - S)| &\leq |K| \\ &= n, \end{aligned}$$

it follows from the pigeonhole principle that $S \cap (a - S) \neq \emptyset$. Thus we may choose $a - x \in S \cap (a - S)$ where both $x$ and $a - x$ are squares. Therefore

$$a = x + (a - x)$$

is a sum of two squares. □

# Problem 3

**Lemma 0.3.** *Let $A \subset B$ be an integral extension and suppose $B$ is an integral domain. Then $B$ is a field if and only if $A$ is a field.*

*Proof.* Suppose that $B$ is a field and let $a$ be a nonzero element in $A$. We will show that $a$ is a unit in $A$. Since $a$ belongs to $B$, we know that it is a unit in $B$, say $ab = 1$ for some $b$ in $B$. Since $B$ is integral over $A$, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0. \tag{4}$$

Multiplying $a^{n-1}$ on both sides of (4) gives us

$$b + a_{n-1} + \cdots + a^{n-1}a_0 = 0.$$

In particular, $b \in A$. Thus $a$ is a unit in $A$.

Conversely, suppose $A$ is a field and let $b$ be a nonzero element in $B$. Since $b$ is integral over $A$, there exists $n \in \mathbb{N}$ and $a_0, \dots, a_{n-1} \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0,$$

where we may assume that $n$ is minimal. Then since $n$ is minimal and $B$ is an integral domain, we must have $a_0 \neq 0$. Thus

$$\begin{aligned} 1 &= (-a_0)^{-1}(b^n + a_{n-1}b^{n-1} + \cdots + a_1 b) \\ &= (-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)b \end{aligned}$$

implies

$$(-a_0)^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1)$$

is the inverse of $b$. □

**Proposition 0.5.** *Let $L/K$ be an algebraic extension of fields and let $R$ be an integral domain such that*

$$K \subseteq R \subseteq L.$$

*Then $R$ is a field.*

*Proof.* First note that $K \subseteq R$ is an integral extension since $L/K$ is an algebraic extension. Indeed, let $x \in R$. Then $x \in L$, and since $L/K$ is algebraic, there exists $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n \in K$ such that

$$a_n x^n + \cdots + a_1 x + a_0 = 0. \tag{5}$$

where $a_n \neq 0$. Since $K$ is a field, we can multiply both sides of (5) by $a_n^{-1}$ and obtain

$$x^n + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0 = 0. \tag{6}$$

Then (6) implies $x$ is integral over $K$. Since $x$ was arbitrary, we see that $K \subseteq R$ is an integral extension. Now it follows from Lemma (0.3) that since $K$ is a field, $R$ must be a field too. □

# Problem 4

**Proposition 0.6.** *Let $K$ be a field and let $\alpha$ and $\beta$ be algebraic numbers in some field extension of $K$. Denote $[K(\alpha) : K] = m$ and $[K(\beta) : K] = n$. Then*

$$[K(\alpha, \beta) : K] \leq mn$$

*with equality holding if* $\gcd(m, n) = 1$.

*Proof.* Since $\beta$ is algebraic over $K$, it is also algebraic over $K(\alpha)$. Let

$$f(T) = T^k + \alpha_{k-1} T^{k-1} + \cdots + \alpha_0$$

be the minimal polynomial of $\beta$ in $K(\alpha)[T]$, where $\alpha_0, \ldots, \alpha_{n-1} \in K(\alpha)$, and let

$$g(T) = T^n + a_{n-1} T^{n-1} + \cdots + a_0$$

be the minimal polynomial of $\beta$ in $K[T]$. Since $g(T)$ is a monic polynomial with coefficients in $K(\alpha)$ which kills $\beta$, we must have $k \leq n$, by minimality of $k$. Therefore

$$\begin{aligned}
[K(\alpha, \beta) : K] &= [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] \\
&= [K(\alpha)(\beta) : K(\alpha)][K(\alpha) : K] \\
&= km \\
&\leq nm.
\end{aligned}$$

This gives us the bound we are looking for.

Now assume that $\gcd(m, n) = 1$. Denote $k' = [K(\alpha, \beta) : K(\beta)]$. By the same argument as above, we have

$$km = [K(\alpha, \beta) : K] = k'n.$$

Therefore $[K(\alpha, \beta) : K]$ is a common multiple of $m$ and $n$. Then since $\gcd(m, n) = 1$, we have

$$\begin{aligned}
mn &= \operatorname{lcm}(m, n) \\
&\leq [K(\alpha, \beta) : K] \\
&\leq mn.
\end{aligned}$$

It follows that $[K(\alpha, \beta) : K] = mn$. □

# Problem 5

**Proposition 0.7.** *The only automorphism of* $\mathbb{R}$ *which fixes* $\mathbb{Q}$ *is the identity map.*

*Proof.* Let $\sigma\colon \mathbb{R} \to \mathbb{R}$ be an automorphism of $\mathbb{R}$ which fixes $\mathbb{Q}$. We will show that $\sigma$ is the identity map as follows:

**Step 1:** We first show that $\sigma$ sends positive numbers to positive numbers. Let $x$ be a positive real number. Then $x = a^2$ for some $a \in \mathbb{R}\backslash\{0\}$. Then

$$\begin{aligned}
\sigma(x) &= \sigma(a^2) \\
&= \sigma(a)^2 \\
&> 0.
\end{aligned}$$

It follows that $\sigma$ sends positive numbers to positive numbers.

**Step 2:** Next we show $\sigma$ is strictly increasing. Let $x$ and $y$ be real numbers such that $x > y$. Then $x - y > 0$. This implies

$$\begin{aligned}
\sigma(x) - \sigma(y) &= \sigma(x - y) \\
&> 0.
\end{aligned}$$

It follows that $\sigma$ is strictly increasing.

**Step 3:** We show that $\sigma$ is continuous with respect to the usual topology on $\mathbb{R}$. Let $(x_n)$ be a sequence of real numbers which converges to some real number $x$. Let $\varepsilon > 0$ and choose $M \in \mathbb{N}$ such that $1/M < \varepsilon$. Also, choose $N \in \mathbb{N}$ such that $n \geq N$ implies

$$-\frac{1}{M} < x_n - x < \frac{1}{M}.$$

Then $n \geq N$ implies

$$\begin{aligned}
-\varepsilon &< -\frac{1}{M} \\
&= \sigma\left(-\frac{1}{M}\right) \\
&< \sigma(x_n) - \sigma(x) \\
&< \sigma\left(\frac{1}{M}\right) \\
&= \frac{1}{M} \\
&< \varepsilon.
\end{aligned}$$

It follows that the sequence $(\sigma(x_n))$ converges to $\sigma(x)$. This implies $\sigma$ is continuous.

**Step 4:** Finally we show that $\sigma$ is the identity map. Let $x$ be a real number. As $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists a sequence of rational numbers $(x_n)$ which converges to $x$. Choose such a sequence $(x_n)$. It follows from continuity of $\sigma$ and the fact that $\sigma(x_n) = x_n$ for all $n \in \mathbb{N}$ that we must have $\sigma(x) = x$. Thus $\sigma$ is the identity map. $\square$