
For this exam, you may use your class notes, results established in homework, and your textbook. You cannot consult with any other individuals, be they KU students, KU professors, family members, friends, etc. You may not use the internet. If you have any questions you may ask me directly or via email.

1. Prove the following statement, known as the Rational Root Test. Let \( p(x) = a_nx^n + \cdots + a_1x + a_0 \) be a polynomial with integer coefficients. If the rational number \( r \) is a root of \( p(x) \), then \( r = \pm \frac{c}{d} \), where \( c \) is a factor of \( a_0 \) and \( d \) is a factor of \( a_n \). Hint: The proof of this statement is very similar to the proof of Homework 16(i).

   (i) Use the rational root test to show that \( p(x) = x^3 + 725x^2 + 2019x - 1 \) is irreducible over \( \mathbb{Q} \).
   (ii) Use the rational root test to find all rational roots to \( q(x) = 3x^3 - 4x^2 - 17x + 6 \).

Solution. Suppose \( p(r) = 0 \), where \( r = \frac{u}{v} \), with \( u, v \in \mathbb{Z} \) and relatively prime. Then:

\[
an_n \left( \frac{u}{v} \right)^n + a_{n-1} \left( \frac{u}{v} \right)^{n-1} + \cdots + a_1 \frac{u}{v} + a_0 = 0,
\]

and thus,

\[
a_nu^n = -(a_{n-1}u^{n-1}v + \cdots + a_1uv^{n-1} + a_0v^n) = -(a_{n-1}u^{n-1} + \cdots + a_1uv^{n-2} + a_0v^{n-1})v.
\]

Thus \( v \) divides \( a_nu^n \). Since \( u \) and \( v \) are relatively prime, this means \( v \) divides \( a_n \). Similarly, we may write

\[
u(a_nu^{n-1} + a_{n-1}u^{n-2}v + \cdots + a_1v^{n-1}) = -a_0v^n.
\]

Thus, \( u \) divides \( a_0v^n \). Since \( u \) and \( v \) are relatively prime, \( u \) must divide \( a_0 \), which gives what we want.

For the polynomial \( p(x) \) given in (i), by the Rational Root Test, we must only check the fractions \( \pm \frac{1}{1} = \pm 1 \). Clearly, \( p(1) \neq 0 \) and \( p(-1) \neq 0 \), so \( p(x) \) has no roots in \( \mathbb{Q} \). Since \( p(x) \) has degree three, it must be irreducible over \( \mathbb{Q} \).

For the polynomial \( q(x) \) given in (ii), the possible rational roots are: \( \pm 6, \pm 3, \pm 2, \pm 1, \pm \frac{1}{3}, \pm \frac{2}{3} \). Substitution yields the roots \( \frac{1}{3}, -2, 3 \).

2. Prove that \( \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5}) \).

Solution. \( \mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) \), since the latter contains \( \sqrt{3}, \sqrt{5} \) and is closed under addition. To see the reverse containment, we just have to see that \( \mathbb{Q}(\sqrt{3}, \sqrt{5}) \) is contained in any subfield of \( \mathbb{R} \) containing \( \mathbb{Q}(\sqrt{3} + \sqrt{5}) \) and for this it suffices to show that both \( \sqrt{3} \) and \( \sqrt{5} \) are in any such field. Let \( F \) a subfield of \( \mathbb{R} \) containing \( \mathbb{Q}(\sqrt{3} + \sqrt{5}) \).

Then \( F \) contains \( (\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15} \), and so \( \sqrt{15} \in F \). Therefore \( \sqrt{15} \cdot (\sqrt{3} + \sqrt{5}) = 3\sqrt{5} + 5\sqrt{3} \), belongs to \( F \). Therefore \( 3\sqrt{5} + 5\sqrt{3} - 3(\sqrt{3} + \sqrt{5}) = 2\sqrt{3} \) belongs to \( F \), so \( \sqrt{3} \) belongs to \( F \). And thus \( \sqrt{3} + \sqrt{5} - \sqrt{3} = \sqrt{5} \) belongs to \( F \). Hence \( \mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq F \), which is what we want.

Another approach would be to first show that \( \left| \mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q} \right| = 4 \) and then show that \( \sqrt{3} + \sqrt{5} \) does not satisfy a polynomial of degree two over \( \mathbb{Q} \). Thus, \( \left| \mathbb{Q}(\sqrt{3} + \sqrt{5}) : \mathbb{Q} \right| \neq 2 \). Since this latter degree must divide 4, it has to be 4, which forces \( \mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5}) \).

3. Let \( F \) denote the field \( \mathbb{Q}[x] \) modulo \( x^3 + x + 1 \). Write the following expressions in the form \( a + bx + cx^2 \) as elements of \( F \).

   (i) \( \frac{1}{1} + 2x + 3x^2 \cdot \frac{3}{2} + 2x + x^2 \).
   (ii) \( \frac{1}{x + x^2} \).
Note: that $x^3 + x + 1$ is easily seen to have no rational roots, by the rational root test, so that it is irreducible over $\mathbb{Q}$. Thus, $F$ is, in fact, a field.

**Solution.** Using the division algorithm we get: (i) \( \frac{1 + 2x + 3x^2}{3 + 2x + x^2} = -\frac{5}{3} - 3x + 11x^2 \). Via the Euclidean algorithm we get \( 3 = (x^2 - 2x + 2) \cdot (x^2 + x + 1) + (1 - x) \cdot (x^3 + x + 1) \), and thus \( (1 + x + x^2)^{-1} = \frac{2}{3} - \frac{2}{3}x + \frac{1}{3}x^2 \).

4. Let $K \subseteq F$ be fields, such that $[F : K] = p$, a prime number. Prove that $F = K(\alpha)$ for any $\alpha$ in $F$, that is not in $K$.

**Solution.** For any $\alpha \in F \setminus K$, we have $K \subseteq K(\alpha) \subseteq F$, and thus $p = [F : K] = [F : K(\alpha)] \cdot [K(\alpha) : K]$, with $[K(\alpha) : K] \neq 1$. Since $p$ is prime, we must have $p = [K(\alpha) : K]$, which forces $F = K(\alpha)$, since a $p$-dimensional subspace of a $p$-dimensional vector space must be the vector space itself.

5. Let $\sqrt[3]{2}$ be the real cube root of two. Set $\epsilon := -1 + \sqrt[3]{3}i$.

(i) Show that $\sqrt[3]{2}, \sqrt[3]{2}i, \sqrt[3]{2}i^2$ are the distinct roots of $x^3 - 2$.

(ii) Conclude that the field $Q(\sqrt[3]{2}, \epsilon)$ contains all of the roots of $x^3 - 2$.

(iii) Find $[Q(\sqrt[3]{2}, \epsilon) : Q]$.

**Solution.** Note that $\epsilon$ is a root of $x^2 + x + 1$. Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, this shows $x^3 = 1$. Thus, $(\epsilon^2)^3 = 1$. Since $\epsilon^2$ is not equal to 1 or $\epsilon, 1, \epsilon^2$ are distinct. Therefore, $\sqrt[3]{2}, \sqrt[3]{2}i, \sqrt[3]{2}i^2$ are distinct. Moreover, $2 = (\sqrt[3]{2})^3 = (\sqrt[3]{2})^3 = (\sqrt[3]{2}i)^3$, so these are the distinct roots of $x^3 - 2$, which gives (i). Part (ii) is clear since $Q(\sqrt[3]{2}, \epsilon)$ is closed under sums, products and quotients.

For part (iii) we first note that since $x^3 - 2$ is irreducible over $\mathbb{Q}$ (by a previously established fact), we have $[Q(\sqrt[3]{2}) : \mathbb{Q}] = 3$, since the degree of a field extension obtained by adjoining a single element equals the degree of the minimal polynomial of the element. On the other hand, $\epsilon$ is a complex number that is not a real number so, $\epsilon \notin Q(\sqrt[3]{2})$. Therefore, since $Q(\sqrt[3]{2}, \epsilon) = (Q(\sqrt[3]{2}))(\epsilon)$, $[Q(\sqrt[3]{2}, \epsilon) : Q(\sqrt[3]{2})] \geq 2$. But $\epsilon$ satisfies $x^2 + x + 1$ over $\mathbb{Q}$, which gives $[Q(\sqrt[3]{2}, \epsilon) : Q(\sqrt[3]{2})] = 2$. Thus, $[Q(\sqrt[3]{2}, \epsilon) : \mathbb{Q}] = [Q(\sqrt[3]{2}, \epsilon) : Q(\sqrt[3]{2})] \cdot [Q(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

For the following problems: If $G$ is a group, a subset $H \subseteq G$ is a **subgroup** of $G$ if it is closed under the group operation on $G$ and closed under taking inverses.

6. Prove that the indicated subsets $H$ are subgroups of the given group $G$.

(i) $G = S_4$ and $H = \{ \sigma \in G \mid \sigma(1) = 1 \}$.

(ii) Let $G$ be a group and $X \subseteq G$ a subset of $G$. Let $H = \langle X \rangle$ denote the intersection of all subgroups of $G$ containing $X$. Prove that $H$ is a subgroup of $G$. It is called the **subgroup of $G$ generated by $X$**.

(iii) How would you give an intrinsic description of $\langle X \rangle$ for $X \subseteq G$? Does this remind you of anything?

**Solution.** For (i), suppose $\alpha, \beta \in H$. Then $\alpha \beta(1) = \alpha(\beta(1)) = \alpha(1) = 1$, which shows $\alpha \beta \in H$. Moreover $1 = i(1) = \alpha^{-1}(\alpha(1)) = \alpha^{-1}(1)$, which shows $\alpha^{-1} \in H$. Thus, $H$ is a subgroup of $S_4$.

For (ii), let $a, b \in H$. Then for any subgroup $K$ of $G$ containing $X$, $a, b \in K$. Thus, $ab$ and $a^{-1}$ are in $K$. Since $H$ is the intersection of all such $K$, $ab$ and $a^{-1}$ are in $H$, and thus $H$ is a subgroup of $G$.

For (iii), notice that to get a subgroup containing $X$, we must close $X$ under the group operation taking inverses. Thus we consider $H_0$ to be the set of all expressions of the form $x_1^{c_1}x_2^{c_2} \cdots x_r^{c_r}$, where each $x_i \in X$ and $c_i = \pm 1$. Clearly, $H_0$ is closed under products and taking inverses, by definition. Thus, $H_0$ is a subgroup of $G$ containing $X$ and hence contains $H$. On the other hand, $H$ is a subgroup of $G$ containing $X$ and therefore must contain all expressions of the form $x_1^{c_1}x_2^{c_2} \cdots x_r^{c_r}$, where each $x_i \in X$ and $c_i = \pm 1$. Thus, $H_0 \subseteq H$, and hence $H = H_0$. In other words, $H_0$ provides an intrinsic description of $H$.

This should remind you of the construction of a field generated over a subfield by a set of elements in a larger field. Recall from class, that if $K \subseteq F$ are two fields and $X \subseteq F$ is a set of elements in $F$, we defined $K(X)$ to be the intersection of all subfields of $F$ containing $K$ and $X$. We then showed that $K(X)$ can be described intrinsically by taking the elements from $K$ and $X$ and writing down all expressions obtained from $K$ and $X$ using field operations.
7. Write a group table for the symmetric group $S_3$. You may use any description of $S_3$ you like, just be sure to label the group elements carefully.

Solution. We set $\sigma = (1, 2)$ and $\tau = (1, 2, 3)$ and use the identities: $\sigma^2 = i = \tau^3$, $\tau \sigma = \sigma \tau^2$ and $\tau^2 \sigma = \sigma \tau$.

<table>
<thead>
<tr>
<th></th>
<th>$i$</th>
<th>$\tau$</th>
<th>$\tau^2$</th>
<th>$\sigma$</th>
<th>$\sigma \tau$</th>
<th>$\sigma \tau^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>$i$</td>
<td>$\tau$</td>
<td>$\tau^2$</td>
<td>$\sigma$</td>
<td>$\sigma \tau$</td>
<td>$\sigma \tau^2$</td>
</tr>
<tr>
<td>$\tau$</td>
<td>$\tau$</td>
<td>$\tau^2$</td>
<td>$i$</td>
<td>$\sigma \tau^2$</td>
<td>$\sigma$</td>
<td>$\sigma \tau$</td>
</tr>
<tr>
<td>$\tau^2$</td>
<td>$\tau^2$</td>
<td>$i$</td>
<td>$\tau$</td>
<td>$\sigma \tau$</td>
<td>$\sigma \tau^2$</td>
<td>$i$</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>$\sigma$</td>
<td>$\sigma \tau$</td>
<td>$\sigma \tau^2$</td>
<td>$i$</td>
<td>$\tau$</td>
<td>$\tau^2$</td>
</tr>
<tr>
<td>$\sigma \tau$</td>
<td>$\sigma \tau$</td>
<td>$\sigma \tau^2$</td>
<td>$\sigma$</td>
<td>$\tau^2$</td>
<td>$i$</td>
<td>$\tau$</td>
</tr>
<tr>
<td>$\sigma \tau^2$</td>
<td>$\sigma \tau^2$</td>
<td>$\sigma$</td>
<td>$\sigma \tau$</td>
<td>$\tau^2$</td>
<td>$i$</td>
<td>$\tau$</td>
</tr>
</tbody>
</table>

8. The Quaternion group is the group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ subject to the relations:

(i) $i^2 = j^2 = k^2 = -1$
(ii) $ij = k, jk = i, ki = j$
(iii) $ji = -ij, kj = -jk, ik = -ki$.

Write a group table for $Q_8$. Then use the group table to find all subgroups of $Q_8$. For this you may use the following fact, that we will eventually prove: If $G$ is a finite group and $H$ is a subgroup of $G$, then the number of elements in $H$ divides the number of elements in $G$.

Solution.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>$-1$</th>
<th>$i$</th>
<th>$-i$</th>
<th>$j$</th>
<th>$-j$</th>
<th>$k$</th>
<th>$-k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$-1$</td>
<td>$i$</td>
<td>$-i$</td>
<td>$j$</td>
<td>$-j$</td>
<td>$k$</td>
<td>$-k$</td>
</tr>
<tr>
<td>$-1$</td>
<td>$-1$</td>
<td>1</td>
<td>$-i$</td>
<td>$i$</td>
<td>$-j$</td>
<td>$j$</td>
<td>$-k$</td>
<td>$k$</td>
</tr>
<tr>
<td>$i$</td>
<td>$i$</td>
<td>$-i$</td>
<td>1</td>
<td>$-1$</td>
<td>$-k$</td>
<td>$k$</td>
<td>$j$</td>
<td>$-j$</td>
</tr>
<tr>
<td>$-i$</td>
<td>$-i$</td>
<td>$i$</td>
<td>1</td>
<td>$-1$</td>
<td>$-k$</td>
<td>$k$</td>
<td>$j$</td>
<td>$-j$</td>
</tr>
<tr>
<td>$j$</td>
<td>$j$</td>
<td>$-j$</td>
<td>$-k$</td>
<td>$k$</td>
<td>$-1$</td>
<td>$1$</td>
<td>$i$</td>
<td>$-i$</td>
</tr>
<tr>
<td>$-j$</td>
<td>$-j$</td>
<td>$j$</td>
<td>$k$</td>
<td>$-k$</td>
<td>$1$</td>
<td>$-1$</td>
<td>$-i$</td>
<td>$i$</td>
</tr>
<tr>
<td>$k$</td>
<td>$k$</td>
<td>$-k$</td>
<td>$j$</td>
<td>$-j$</td>
<td>$-i$</td>
<td>$i$</td>
<td>$-1$</td>
<td>1</td>
</tr>
<tr>
<td>$-k$</td>
<td>$-k$</td>
<td>$k$</td>
<td>$-j$</td>
<td>$j$</td>
<td>$i$</td>
<td>$-i$</td>
<td>1</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

The subgroups of $Q_8$: are:

(i) $\{1\}$
(ii) $Q_8$
(iii) $\{1, -1\} = \{-1\}$
(iv) $\{1, -1, i, -i\} = \langle i \rangle = \langle -i \rangle$
(v) $\{1, -1, j, -j\} = \langle j \rangle = \langle -j \rangle$
(vi) $\{1, -1, k, -k\} = \langle k \rangle = \langle -k \rangle$

Note that there are no other subgroups, since any proper subgroup has to contain 2 or 4 elements. Therefore any proper subgroup containing more than two elements, must contain one of $\pm i, \pm j, \pm k$ and therefore is accounted for. Any subgroup with two elements must contain 1. Since such a subgroup cannot contain any of the elements $\pm i, \pm j, \pm k$, the only remaining choice is -1, and this subgroup has been accounted for.

9. Let $G$ be a group with an even number of elements. Prove that there exists at least one element $g$ in $G$ such that $e \neq g$ and $g^2 = e$.

Solution. Note that $g^2 = e$ if and only if $g = g^{-1}$. Hence we must find $g \in G$ such that $e \neq g$ and $g = g^{-1}$.

Now, each element in the group has a unique inverse. If we remove $e$, which is its own inverse, then there are an odd number of elements remaining. If each of these non-identity elements had an inverse not equal
to itself, these elements would pair up, and this would give an even number of non-identity elements, a
contradiction. Thus, at least one non-identity element must equal its own inverse.

10. Prove that if \( G \) is a group and \((ab)^2 = a^2b^2\), for all \( a, b \in G \), then \( G \) is abelian.

**Solution.** For all \( a, b \in G \), \( abab = (ab)^2 = a^2b^2 \). From the equation \( abab = aabb \), we may cancel \( a \) from the
left side of the equation and \( b \) from the right side of the equation to infer \( ba = ab \), which is what we want.