1. Let $G$ be a transitive subgroup of $S_n$.
   
   (a) Prove that if $n$ is prime, then $G$ contains an $n$-cycle.
   
   (b) Show that (a) is not true if $n$ is not prime.

   **Solution.** The number of elements in an orbit divides the order of $G$. Since $G$ is transitive, $n$ divides $|G|$. If $n$ is prime, then by Sylow theorems $G$ contains an element of order $n$, which is an $n$-cycle. If $n$ is not prime, the statement is false. For example, let $n = 4$, $G$ be the Klein subgroup of $S_4$.

2. Let $F$ be a field such that the multiplicative group $F^*$ is cyclic. Prove that $F$ is finite.

   **Solution.** Let $u$ be a generator of $F^*$. Assume first that char $F \neq 2$. Then $-1 = u^n$ for some $n$, hence $u^{2n} = 1$, and therefore $F^* \cong \mathbb{Z}_{2n}$ is finite. Let now char $F = 2$. Then $1 + u = u^n$ for some $n$. Hence $F = \mathbb{Z}_2(u)$ is a finite extension of $\mathbb{Z}_2$ and therefore $F$ is finite.

3. Let $G$ be a transitive subgroup of $S_6$ which contains a 5-cycle. Prove that $G$ is not solvable.

   **Solution.** Observe first that $|G|$ divides $6!$. Hence a cyclic 5-subgroup is a Sylow subgroup of $G$. Assume that $G$ is solvable. We have a chain

   $$G = G_0 \supset G_1 \supset \cdots \supset G_k = \{1\}$$

   such that $G_{i+1}$ is normal in $G_i$ and $G_i/G_{i+1}$ is cyclic of prime order. Among such chains of subgroups choose one such that $\mathbb{Z}_5 \cong G_i/G_{i+1}$ appears for maximal $i$. We claim that then $\mathbb{Z}_5 = G_{k-1}$. Indeed, $G_{i+1}/G_{i+2} \cong \mathbb{Z}_p$ for some $p < 5$. Hence $G_i/G_{i+2} \cong \mathbb{Z}_5 \times \mathbb{Z}_p$ and one can find $G'_{i+1}$ normal in $G_i$ such that $G'_{i+1}/G_{i+2} \cong \mathbb{Z}_5$, $G_i/G'_{i+1} \cong \mathbb{Z}_p$. Hence we moved $\mathbb{Z}_5$ to the right.

   Now we claim that $\mathbb{Z}_5 = G_{k-1}$ is normal in $G$. To prove proceed by induction. Assume that $G_{k-1} = \mathbb{Z}_5$ is normal in $G$, then it is the unique Sylow subgroup in $G$. Hence for any $g \in G_{k-1}$, $gG_{k-1}g^{-1} = G_{k-1}$, and therefore $G_{k-1}$ is normal in $G_{k-1}$.

   Finally, let $\mathbb{Z}_5$ be generated by a cycle $s = (12345)$. $G$ is transitive, therefore there is a permutation $t \in G$ such that $t(1) = 6$. Then clearly $tst^{-1} \neq s^n$. Hence $\mathbb{Z}_5$ is not normal. Contradiction.

4. Let $F$ be a field and char $F \neq 2$, $\alpha, \beta \in F$. Prove that $F(\sqrt{\alpha}) = F(\sqrt{\beta})$ if and only if $\alpha \beta$ is a square in $F$.

---

*Date: May 13, 2006.*
Solution. Assume that \( F(\sqrt{\alpha}) = F(\sqrt{\beta}) = E \). The Galois group of \( E \) over \( F \) is \( \mathbb{Z}_2 \). Let \( s \neq 1 \) be the element of the Galois group. Then
\[
s(\sqrt{\alpha}) = -\sqrt{\alpha},\ s(\sqrt{\beta}) = -\sqrt{\beta}.
\]
Write
\[
\sqrt{\beta} = a + b\sqrt{\alpha}
\]
for some \( a, b \in F \). Then
\[
s(\sqrt{\beta}) = a - b\sqrt{\alpha} = -\sqrt{\beta} = -a - b\sqrt{\alpha}
\]
implies \( \sqrt{\beta} = b\sqrt{\alpha} \). Then \( \sqrt{\alpha}\sqrt{\beta} = b\alpha \) and we obtain \( \alpha\beta = b^2\alpha^2 \) is a square. Conversely, if \( \alpha\beta = c^2 \), then \( \sqrt{\beta} = \frac{c}{\sqrt{\alpha}} \). Therefore \( F(\sqrt{\alpha}) = F(\sqrt{\beta}) \).

5. Find the minimal polynomial for \( 1 + 3\sqrt{2} + 3\sqrt{4} \) over \( \mathbb{Q} \).

Solution. Let \( u = 3\sqrt{2} \). Solve the equation
\[
a + b(1 + u + u^2) + c(1 + u + u^2)^2 + (1 + u + u^2)^3 = 0
\]
for \( a, b, c, d \), using the relation \( u^3 = 2 \).
\[
(1 + u + u^2)^2 = 1 + u^2 + u^4 + 2u + 2u^2 + 2u^3 = 1 + u^2 + 2u + 2u^2 + 4 = 5 + 4u + 3u^2,
\]
\[
(1 + u + u^2)^3 = (5 + 4u + 3u^2)(1 + u + u^2) = 5 + 4u + 3u^2 + 5u + 4u^2 + 3u^3 + 5u^2 + 4u^3 + 3u^4 = 5 + 9u + 12u^2 + 7u^3 + 3u^4 = 19 + 15u + 12u^2.
\]
The solution \( a = -1, b = c = -3 \).

The minimal polynomial is \( x^3 - 3x^2 - 3x - 1 \).

6. Prove that any algebraically closed field is infinite.

Solution. Let \( F \) be a finite field and have \( q \) elements. Choose \( n \) relatively prime to \( q - 1 \) and \( q \). Then \( x^n = 1 \) implies \( x = 1 \) by Lagrange’s theorem. Therefore \( x^n - 1 \) does not split in \( F \), and \( F \) is not algebraically closed.

7. Is \( x^3 + x + 1 \) irreducible over \( \mathbb{F}_{256} \)?

Solution. The polynomial is irreducible over \( \mathbb{F}_2 \) because it does not have roots in \( \mathbb{F}_2 \). The degree \( (\mathbb{F}_{256}/\mathbb{F}_2) = 8 \), therefore \( \mathbb{F}_{256} \) does not contain a field of degree 3. Thus, \( \mathbb{F}_{256} \) does not contain a root of the polynomial. Hence \( x^3 + x + 1 \) is irreducible over \( \mathbb{F}_{256} \).

8. Which of the following extensions are normal
\[
\mathbb{Q} \subset \mathbb{Q} \left( \sqrt{1 - \sqrt{2}} \right),
\]
\[
\mathbb{Q} \subset \mathbb{Q} \left( \sqrt[3]{2}, \sqrt[3]{3} \right),
\]
\[
\mathbb{Q} \subset \mathbb{Q} \left( \sqrt[3]{2}, \sqrt[3]{-3} \right) ?
\]
The minimal polynomial of $\sqrt{1 - \sqrt{2}}$ is $x^4 - 2x^2 - 1$, the Galois group of this polynomial is $D_4$. Hence the splitting field has degree 8. But $\left( \mathbb{Q} \left( \sqrt{1 - \sqrt{2}} \right) / \mathbb{Q} \right) = 4$. Hence $\mathbb{Q} \left( \sqrt{1 - \sqrt{2}} \right)$ is not normal.

The extension $\mathbb{Q} \subset \mathbb{Q} \left( \sqrt[3]{2}, \sqrt[3]{3} \right)$ is not normal because it contains a real root of $x^3 - 2$, but does not contain two complex roots since $\mathbb{Q} \left( \sqrt[3]{2}, \sqrt[3]{3} \right)$ is a subfield of $\mathbb{R}$.

The extension $\mathbb{Q} \subset \mathbb{Q} \left( \sqrt[3]{2}, \sqrt[3]{-3} \right)$ is normal, because it is a splitting field of $x^3 - 2$.

Determine if $\mathbb{Q} \left( \sqrt[3]{2} \right)$ is normal? No. The first field is not a normal extension of $\mathbb{Q}$, the second one is normal.

Let $\mathbb{Q} \subset F$ be a finite normal extension such that for any two subfields $E$ and $K$ of $F$ either $K \subset E$ or $E \subset K$. Then the Galois group of $F$ over $\mathbb{Q}$ is cyclic of order $p^n$ for some prime number $p$.

The splitting field of $x^3 - x$ has only one subgroup $H \subset H'$ of $H$. First, we prove that $G$ is cyclic. Indeed, consider an element $g \in G$ of maximal order. For any $h \in G < h > \subset g$, hence $G$ is generated by $g$. Now let us prove that $|G| = p^n$. Assume the contrary, then $|G|$ has two distinct prime divisors $p$ and $q$. Then $G$ has Sylow $p$-subgroup and Sylow $q$-subgroup which have trivial intersection. Contradiction.

Let $F \subset B \subset E$ be a chain of extensions such that $F \subset B$ is normal and $B \subset E$ is normal. Is it always true that $F \subset E$ is normal?

Solution. False. Counterexample

$$\mathbb{Q} \subset \mathbb{Q} \left( \sqrt{2} \right) \subset \mathbb{Q} \left( \sqrt[3]{2} \right).$$

Find the Galois group of $(x^2 - 3)(x^2 + 1)(x^3 - 6)$ over $\mathbb{Q}$.

The splitting field of $x^3 - 6$ contains $\sqrt[3]{-3}$. Therefore the splitting field of $(x^2 - 3)(x^3 - 6)$ contains the roots of $x^2 + 1$. Let $E$ be the splitting field of $(x^2 - 3)(x^2 + 1)(x^3 - 6)$. Then $E = FB$, where $B$ is a splitting field of $x^3 - 6$ whose Galois group is $S_3$, and $F$ is a splitting field of $x^2 - 3$, whose Galois group is $\mathbb{Z}_2$. Let us prove that $F \cap B = \mathbb{Q}$. If not, then $F \subset B$. Since $S_3$ has only one subgroup of index 2, then $F = \mathbb{Q} \left( \sqrt[3]{-3} \right)$, but $B$ is real. Contradiction. By Corollary of the natural irrationalities theorem

$$\text{Aut}_\mathbb{Q} F = \text{Aut}_\mathbb{Q} B \times \text{Aut}_\mathbb{Q} F = S_3 \times \mathbb{Z}_2.$$

Find the Galois group of $x^4 + 3x + 5$ over $\mathbb{Q}$.

The polynomial is irreducible over $\mathbb{Z}_2$. Hence the Galois group contains a 4-cycle. The resolvent cubic is $x^3 - 20x + 9$, which is irreducible over $\mathbb{Q}$. So the Galois group is $S_4$ or $A_4$ and contains a 4-cycle. Hence the Galois group is $S_4$. 

12. Find the Galois group of $(x^2 - 3)(x^2 + 1)(x^3 - 6)$ over $\mathbb{Q}$.

Solution. The splitting field of $x^3 - 6$ contains $\sqrt[3]{-3}$. Therefore the splitting field of $(x^2 - 3)(x^3 - 6)$ contains the roots of $x^2 + 1$. Let $E$ be the splitting field of $(x^2 - 3)(x^2 + 1)(x^3 - 6)$. Then $E = FB$, where $B$ is a splitting field of $x^3 - 6$ whose Galois group is $S_3$, and $F$ is a splitting field of $x^2 - 3$, whose Galois group is $\mathbb{Z}_2$. Let us prove that $F \cap B = \mathbb{Q}$. If not, then $F \subset B$. Since $S_3$ has only one subgroup of index 2, then $F = \mathbb{Q} \left( \sqrt[3]{-3} \right)$, but $B$ is real. Contradiction. By Corollary of the natural irrationalities theorem

$$\text{Aut}_\mathbb{Q} E = \text{Aut}_\mathbb{Q} B \times \text{Aut}_\mathbb{Q} F = S_3 \times \mathbb{Z}_2.$$

13. Find the Galois group of $x^4 + 3x + 5$ over $\mathbb{Q}$.

Solution. The polynomial is irreducible over $\mathbb{Z}_2$. Hence the Galois group contains a 4-cycle. The resolvent cubic is $x^3 - 20x + 9$, which is irreducible over $\mathbb{Q}$. So the Galois group is $S_4$ or $A_4$ and contains a 4-cycle. Hence the Galois group is $S_4$. 

SOLUTIONS FOR REVIEW EXERCISES MATH 114 3
14. Let $p$ be a prime number. Prove that $\sqrt[n]{2}$ is constructible if and only if $n = 2^k$ for some $k$.

**Solution.** The minimal polynomial is $x^n - p$ (irreducible by Eisenstein criterion). If $n$ is not a power of 2, a root is not constructible, since the order of the Galois group is not a power of 2. If $n$ is a power of 2, then $\sqrt[n]{2}$ is constructible, because it can be obtained by taking square root several times.

15. Prove that any subfield of $\mathbb{Q}(\sqrt[n]{2})$ coincides with $\mathbb{Q}(\sqrt[n]{d}2)$ for some divisor $d$ of $n$.

**Solution.** Since $x^n - 2$ is irreducible over $\mathbb{Q}$, the degree of $\mathbb{Q}(\sqrt[n]{2})$ over $\mathbb{Q}$ is $n$. Let $F$ be a subfield of $\mathbb{Q}(\sqrt[n]{2})$. Consider the minimal polynomial $f(x)$ for $\sqrt[n]{2}$ over $F$. Let $k$ denote the degree of $f(x)$. Since $k = (\mathbb{Q}(\sqrt[n]{2})/F)$, $k$ divides $n$, and $(F/\mathbb{Q}) = d = \frac{n}{k}$. All roots of $f(x)$ are roots of $x^n - 2$, which are $\sqrt[n]{2} \omega^a$, where $\omega$ is a primitive $n$-th root of 1. Let $a_0$ be the free coefficient of $f(x)$. Then $a_0$ equals plus/minus the product of roots of $f(x)$, $a_0 = \pm (\sqrt[n]{2})^k \omega^a$. Since $a_0 \in F \subset \mathbb{R}$, $\omega^a = \pm 1$. Thus, $\pm a_0 = (\sqrt[n]{2})^k = d\sqrt[n]{2} \in F$. But $\mathbb{Q}(\sqrt[d]{2})$ has degree $d$ over $\mathbb{Q}$, because $x^d - 2$ is irreducible over $\mathbb{Q}$. Therefore $F = \mathbb{Q}(\sqrt[d]{2})$.

16. Prove that there exists a polynomial of degree 7 whose Galois group over $\mathbb{Q}$ is $\mathbb{Z}_7$.

**Solution.** For example, consider the splitting field $E$ for $x^{28} - 1$. The Galois group of $E$ over $\mathbb{Q}$ is $\mathbb{Z}_{28}$, which contains a subgroup $\mathbb{Z}_4$. Let $F = E^{24}$. Then the Galois group of $F$ over $\mathbb{Q}$ is $\mathbb{Z}_7$. Pick up an element $\alpha$ in $F, \alpha \notin \mathbb{Q}$. The minimal polynomial of $\alpha$ has the Galois group $\mathbb{Z}_7$.

17. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of odd prime degree $p$ solvable in radicals. Prove that the number of real roots of $f(x)$ equals $p$ or 1.

**Solution.** Let $G$ be the Galois group of $f(x)$. Then $G$ is a subgroup of $Fr_p$. Let $\sigma$ be the complex conjugation. After suitable enumeration of roots by elements of $\mathbb{Z}_p$ we have $\sigma(t) = at + b$, for some $a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p$. The number of real roots is the number of $t$ fixed by $\sigma$. But the number of solutions for the equation $at + b = t$ is 0,1 or $p$. Since any polynomial of odd degree has at least one real root, the number of real roots is either 0 or $p$.

18. Let $f(x) \in \mathbb{F}_2[x]$ be an irreducible polynomial. Prove that $f(x)$ divides $x^{256} - x$ if and only if the degree of $f(x)$ is 1,2,4 or 8.

**Solution.** Let $f(x)$ divide $x^{256} - x$. The elements of $\mathbb{F}_{256}$ are the roots of $x^{256} - x$, therefore $f(x)$ splits in $\mathbb{F}_{256}$. Conversely, if $f(x)$ splits in $\mathbb{F}_{256}$ then $f(x)$ divides $x^{256} - x$. The irreducible polynomial splits in $\mathbb{F}_{256}$ if and only if its degree divides the degree of $\mathbb{F}_{256}$, which is 8.

19. Suppose that the Galois group over $\mathbb{Q}$ of a polynomial $f(x) \in \mathbb{Q}[x]$ has odd order. Prove that all roots of $f(x)$ are real.

**Solution.** Complex conjugation is an element of order 2 unless all roots are real.

20. Find the Galois group of $x^6 - 8$ over $\mathbb{Q}$.
Solution. The polynomial factors
\[ x^6 - 8 = (x^2 - 2) \left( x^4 + 2x^2 + 4 \right) . \]
The Galois group of \( x^4 + 2x^2 + 4 \) is \( \mathbb{Z}_2 \times \mathbb{Z}_2 \). Let \( \alpha \) and \( \beta = \frac{2}{\alpha} \) be two roots of \( x^4 + 2x^2 + 4 \), then
\[ (\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta = -2 + 4 = 2. \]
Hence \( \sqrt{2} \) is in the splitting field of \( x^4 + 2x + 4 \), Thus, the Galois group is \( \mathbb{Z}_2 \times \mathbb{Z}_2 \).