1. Set $\phi = \frac{1 + \sqrt{5}}{2}$ and $\overline{\phi} = \frac{1 - \sqrt{5}}{2}$. Set $Z[\phi] = \{a + b\phi : a, b \in Z\}$.

(a) Show that $\overline{\phi} \in Z[\phi]$ by writing it in the form $a + b\phi$.
Solution: $\overline{\phi} = 1 - \phi$

(b) Show that if $\alpha, \beta \in Z[\phi]$ then $\alpha\beta \in Z[\phi]$.
Solution: $(a+b\phi)(c+d\phi) = ac + bc\phi + ad\phi + bd\phi^2$ but $\phi^2 = \phi + 1$ so $(a + b\phi)(c + d\phi) = ac + bc\phi + ad\phi + bd(1 + \phi) \in Z[\phi]$.

(c) (Henceforth assume $Z[\phi]$ is a ring. The hardest part to show this is 1b above.) Define $\sigma$ with domain $Z[\phi]$ by $\sigma(a + b\phi) = a + b\overline{\phi}$. Show the following about $\sigma$ which, together, mean that $\phi$ is what is called a ring automorphism of $Z[\phi]$ over $Z$.

i. $\sigma$ is a bijection from $Z[\phi]$ to itself.
Solution: $\sigma(a + b\phi) = a + b\overline{\phi} = (a + b) - b\phi \in Z[\phi]$. For any $c, d \in Z$ the equation $\sigma(a + b\phi) = c + d\phi$ has the unique solution $b = -d, a = c + d$.

ii. $\sigma(s) = s$ for all $s \in Z$.
Solution: $\sigma(s + 0\phi) = s + 0\overline{\phi} = s$.

iii. $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ for all $\alpha = a + b\phi, \beta = c + d\phi \in Z[\phi]$.
Solution: $\sigma(\alpha + \beta) = (a+c) + (b+d)\overline{\phi} = (a+b\overline{\phi}) + (c+d\overline{\phi}) = \sigma(\alpha) + \sigma(\beta)$.

iv. $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ for all $\alpha = a + b\phi, \beta = c + d\phi \in Z[\phi]$.
Solution: One can do this in gory detail but here is a shorter way. The key is that $\phi, \overline{\phi}$ satisfy the same minimal polynomial, $\phi^2 = \phi + 1$ and $\overline{\phi}^2 = \overline{\phi} + 1$. Write $\alpha\beta = e + f\phi + g\phi^2$ by just multiplying out. Then $\sigma(\alpha)\sigma(\beta)$ gives the same quadratic in $\overline{\phi}$, $\sigma(\alpha)\sigma(\beta) = e + f\overline{\phi} + g\overline{\phi}^2$. When you replace $\phi^2 = \phi + 1$ you get $\alpha\beta = u + v\phi$. When you replace $\overline{\phi}^2 = \overline{\phi} + 1$ you get $\sigma(\alpha)\sigma(\beta) = u + v\overline{\phi}$ with the same $u, v$.

(d) Show that $\alpha + \sigma(\alpha) \in Z$ for all $\alpha = a + b\phi \in Z[\phi]$.
Solution: $\alpha + \sigma(\alpha) = a + b\phi + a + b(1 - \phi) = 2a + b \in Z$.

(e) Using 1d show that $\phi^n + \overline{\phi^n} \in Z$.
Solution: Set $\alpha = \phi^n$ so that $\phi^n + \overline{\phi^n} = \alpha + \sigma(\alpha)$.

(f) Using methods in Assignment 8 show that for $n$ large $\phi^n$ will be very close to an integer.
Solution: As $|\overline{\phi}| < 1$, for $n$ large $\overline{\phi}^n$ will be very small and this is the distance from $\phi^n$ to the integer $\phi^n + \overline{\phi}^n$. 

Algebra V63.0344
Assignment 10 Solutions
(g) Set $u_n = \phi^n + \overline{\phi}^n$. Calculate $u_n$ for $0 \leq n \leq 5$. Hmmmmm, what looks interesting about this sequence?

**Solution:** $u_0 = 1+1 = 2$, $u_1 = \phi + \overline{\phi} = 1$. $u_2 = \frac{3 + \sqrt{5}}{2} + \frac{3 - \sqrt{5}}{2} = 3$.

Grunt work gives $u_3 = 4$, $u_4 = 7$, $u_5 = 11$, 2, 1, 3, 4, 7, 11, · · · .

Each term (starting with $u_2$) is the sum of the two previous terms!

So it is like the Fibonacci sequence but with a different start – these are called the Lucas numbers. One can show directly that $u_{n+2} = u_{n+1} + u_n$ by plugging in the formula and using that $\phi^2 = \phi + 1$ and $\overline{\phi^2} = \overline{\phi} + 1$.

2. Let $F \subset K$, $\alpha, \beta \in K$, and assume $K = F(\alpha, \beta)$. Prove that $K = F(\alpha + q\beta)$ for all but a finite number of rational numbers $q \in Q$.

**Solution:** For each intermediate subfield $F \subset L \subset K$ with $L \neq K$ there can be only one $q$ with $F(\alpha + q\beta) = L$. The reason is that if $F(\alpha + q_1\beta) = F(\alpha + q_2\beta) = L$ then $\beta = \frac{1}{q_2 - q_1}[(\alpha + q_2\beta) - (\alpha + q_1\beta)] \in L$ and similarly $\alpha \in L$ so $L = K$. We showed in class that there are only a finite number of intermediate fields and for each we only get one (at most) $q$. All the other $q$ must therefore have $F(\alpha + q\beta) = K$.

3. If $a = \alpha + \beta$ and $b = \alpha\beta$, write $a^5 + b^5$ in terms of $a, b$.

**Solution:** $a^5 = (\alpha + \beta)^5 = (\alpha^5 + \beta^5) + 5\alpha\beta(\alpha^3 + \beta^3) + 10\alpha^2\beta^2(\alpha + \beta)$. The first addend is what we want. The last addend $10\alpha^2\beta^2(\alpha + \beta) = 10b^2a$. The middle addend requires further work. As $a^3 = (\alpha + \beta)^3 = (\alpha^3 + \beta^3) + 3\alpha\beta(\alpha + \beta)$ we have $\alpha^3 + \beta^3 = a^3 - 3ab$. So $a^5 = (\alpha^5 + \beta^5) + 5b(a^3 - 3ab) + 10b^2a$ and $a^5 + b^5 = a^5 - 5a^3b + 5ab^2$.

4. Let $\alpha, \beta, \gamma$ be the three roots of $x^3 + 2x^2 + x + 1$. Find $\alpha^3 + \beta^3 + \gamma^3$.

**Solution:** Here we have the three equations

(a) $-2 = \alpha + \beta + \gamma$
(b) $+1 = \alpha\beta + \beta\gamma + \alpha\gamma$
(c) $-1 = \alpha\beta\gamma$

Write $S = \alpha^2\beta + \alpha^2\gamma + \beta^2\alpha + \beta^2\gamma + \gamma^2\alpha + \gamma^2\beta$ for convenience. Thus $-8 = (\alpha + \beta + \gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 3S + 6\alpha\beta\gamma$

The first addend is what we want. The third is $-6$. For the second $S = (\alpha\beta + \alpha\gamma + \beta\gamma)(\alpha + \beta + \gamma) - 3\alpha\beta\gamma = (+1)cdot(-2) - 3(-1) = +1$

So $\alpha^3 + \beta^3 + \gamma^3 = -8 - 3(1) + 6 = -5$
5. In this exercise assume the Galois Correspondence Theorem as a fact. Let $K : Q$ be a normal extension. Assume $\Gamma(K : Q)$ is an Abelian group with size $2^t$. Let $\alpha \in K$. Recall (see Brett’s notes from February 27) that a number is called constructible if it can be written with rationals, $+, -, \cdot, /$ and square root. Show that $\alpha$ is constructible. Point out where you use that $\Gamma(K : Q)$ is Abelian. (You may use the result that any finite Abelian group is isomorphic to the product of cyclic groups.)

**Solution:** Let $H$ be an Abelian Group with $2^s$ elements. Claim: $H$ has a subgroup $H_1$ with $2^{s-1}$ elements. Proof: Write $H$ as the product of cyclic groups $Z_{a_1} \times \cdots \times Z_{a_u}$. All $a_j | 2^s$ so they are powers of two, say $a_1 = 2^b$. But $Z_{2^b}$ has a subgroup, call it $J$, of size $2^{b-1}$, namely the even elements. So $J \times Z_{a_2} \cdots \times Z_{a_u}$ is a subgroup of $H$ of size $2^{s-1}$.

Continuing in this way we find $H = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_{s-1} \supset H_s = \{0\}$ with $H_i$ having $2^{s-i}$ elements. Using the Galois Correspondence theorem, and setting $F_i = H_i^{\uparrow}$, we have $Q = F_0 \subset F_1 \subset \cdots \subset F_{s-1} \subset F_s = K$ and all $[F_{i+1} : F_i] = |H_{i+1}|/|H_i| = 2$. That means each $F_{i+1} = F_i(\sqrt[4]{\alpha_i})$ for some $\alpha_i \in F_i$ which means that all elements of $K$ are constructible.

6. Let $K$ be the splitting field over $Q$ of an irreducible degree six polynomial $p(x)$.

(a) What is the largest that $|\Gamma(K : Q)|$ can be?

**Solution:** $6! = 720$

(b) What is the smallest that $|\Gamma(K : Q)|$ can be?

**Solution:** 6. An example of this is $p(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ discussed previously.

(c) Now further suppose $p(x) = x^6 + ax^4 + cx^2 + d$. What is the largest that $|\Gamma(K : Q)|$ can be?

**Solution:** The key here is that if $\kappa$ is a root so is $-\kappa$ so we can write the roots in three pairs $\alpha, -\alpha, \beta, -\beta, \gamma, -\gamma$. The values $\sigma(\alpha), \sigma(\beta), \sigma(\gamma)$ then determine $\sigma$. These values must be a permutation of $\alpha, \beta, \gamma$ but with arbitrary signs $+1$ or $-1$. There are 6 permutations and $2^3$ choices of signs so this gives at most 48 permutations. (For example, $\sigma(\alpha) = -\beta, \sigma(\beta) = \alpha, \sigma(\gamma) = -\gamma.$)

BTW, the group of 48 allowable permutations is quite interesting by itself!