Math 463/563 - Homework 9

**Part A:** All Students

1.1 Let $r \in R$ be a nonzero element. The multiplication by $r$ map $R \to R$ given by $x \mapsto rx$ is injective because $R$ is an integral domain. Considered as vector spaces over $F$, we get that this map must be an isomorphism of finite dimensional vector spaces (since they have the same dimension). In particular, it is a bijection so there is some $x \in R$ such that $rx = 1$ proving that $r$ has an inverse.

3.1 Since we have the inclusions $F \subseteq F(\alpha^2) \subseteq F(\alpha)$, we know that the degree of $\alpha^2$ must divide 5. If it is one, then $\alpha^2 \in F$ which means that the degree of $\alpha$ is either 1 or 2, a contradiction. Hence $\alpha^2$ has degree 5, i.e., $F(\alpha^2) = F(\alpha)$.

3.2 First note that the polynomial is irreducible over $\mathbb{Q}$ by Eisenstein’s criterion. Let $\alpha$ be a root of the polynomial, so that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. We have that the composite degree $[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}] \leq 12$. On the other hand it is divisible by $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Hence we must have $[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}] = 12$ which means $[\mathbb{Q}(\alpha, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 4$, i.e., the polynomial is irreducible over $\mathbb{Q}(\sqrt{2})$.

3.3 The minimal polynomial for $\zeta_5$ over $\mathbb{Q}$ is $x^4 + x^3 + x^2 + x + 1$. Hence $\zeta_5$ has degree 4 over $\mathbb{Q}$. Similarly, the degree of $\zeta_7$ is 6. Since 4 does not divide 6, we cannot have $\zeta_5 \in \mathbb{Q}(\zeta_7)$.

3.7a Suppose that $i \in \mathbb{Q}(\sqrt{-2})$. Then $\sqrt{2} \in \mathbb{Q}(\sqrt{-2})$ as well so $\mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(\sqrt{-2})$. Since they both have degree 4 over $\mathbb{Q}$, we have $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{-2})$. Note that $(1 + i)/\sqrt{2} \in \mathbb{Q}(\sqrt{2}, i)$ is a 4th root of $-1$. In fact, every 4th root of $-1$ is in this extension (they all differ by a multiple of $\pm 1$ or $\pm i$), therefore $\sqrt{2} \in \mathbb{Q}(\sqrt{-2})$ as well. But $\sqrt{2}$ also has degree 4, hence $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$, which is a contradiction, since the former contains only real numbers.

3.8 Consider the polynomial $x^2 - (\alpha + \beta)x + \alpha \beta$ over $\mathbb{Q}(\alpha + \beta, \alpha \beta)$. Note that $\alpha$ and $\beta$ are roots of this polynomial, hence $\alpha$ and $\beta$ are algebraic over $\mathbb{Q}(\alpha + \beta, \alpha \beta)$. So each extension in the chain $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \beta, \alpha \beta) \subseteq \mathbb{Q}(\alpha, \beta)$ is of finite degree. Hence $\alpha, \beta$ are also algebraic.

4.1 First note that the degree of $\alpha, \alpha^2, \gamma$ are all the same. Since $(x^3 - x - 1)(x^3 - x + 1) = x^6 - 2x^4 + x^2 - 1$ we get that $\alpha^2$ has minimal polynomial $x^3 - 2x^2 + x - 1$. Thus $\gamma$ has minimal polynomial $(x - 1)^3 - 2(x - 1)^2 + (x - 1) - 1$.

4.2 First we compute

$$
\begin{align*}
\alpha &= \sqrt{3} + \sqrt{5} \\
\alpha^2 &= 8 + 2\sqrt{15} \\
\alpha^3 &= 18\sqrt{3} + 14\sqrt{5} \\
\alpha^4 &= 124\sqrt{3} + 32\sqrt{15},
\end{align*}
$$

which gives the relation $\alpha^4 - 16\alpha^2 + 4 = 0$.

(a) Since $\alpha$ is a root of $f(x) = x^4 - 16x^2 + 4$, and $f$ is irreducible over $\mathbb{Q}$, $f$ is the minimal polynomial for $\alpha$ over $\mathbb{Q}$. Notice that this shows that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ since $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ has degree at most 4 over $\mathbb{Q}$, but it contains $\mathbb{Q}(\alpha)$, which has degree 4 over $\mathbb{Q}$.
(b) Notice that \( \alpha \) is a root of \( f(x) = (x - \sqrt{5})^2 - 3 \). Moreover, since \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{5}) \), we know that \( \alpha \) has degree 2 over \( \mathbb{Q}(\sqrt{5}) \), so \( f \) must be its minimal polynomial over \( \mathbb{Q}(\sqrt{5}) \).

(c) By writing an arbitrary element of \( \mathbb{Q}(\alpha) \) as \( a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} \) with \( a, b, c, d \in \mathbb{Q} \), and computing \((a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15})^2 \), one can show that \( \sqrt{10} \in \mathbb{Q}(\alpha) \). Hence \( \mathbb{Q}(\alpha, \sqrt{10}) \) has degree 2 over \( \mathbb{Q}(\alpha) \), so \( \alpha \) still has degree 4 over \( \mathbb{Q}(\sqrt{10}) \). Therefore it has the same minimal polynomial as in (a).

(d) Notice that \( \alpha \) has degree 2 over \( \mathbb{Q}(\sqrt{15}) \), since \( \mathbb{Q}(\sqrt{15}) \) has degree 2 over \( \mathbb{Q} \) and is contained in \( \mathbb{Q}(\alpha) \), which has degree 4 over \( \mathbb{Q} \). Moreover, it is clearly a root of \( f(x) = x^2 - 8 - 2\sqrt{15} = 0 \), so this must be its minimal polynomial.

Part B: Math 563 Students

3.1 Let \( G \) be a finite abelian group and \( V \) an irreducible representation with \( \rho: G \to \text{GL}(V) \). Given \( s \in G \), \( \rho_t \rho_s = \rho_{st} = \rho_s \rho_t \) for any \( t \in G \) since \( G \) is abelian. By Schur’s lemma, \( \rho_s \) is a homothety, i.e., \( \rho_s = \lambda_s \cdot I \) for some constant \( \lambda_s \). Since this is true for all \( s \in G \), \( V \) is irreducible if and only if \( V \) is 1 dimensional, i.e., of degree 1.

3.2 (a) For each \( s \in C \), we have \( \rho_s = \lambda_s \cdot I \) by Schur’s Lemma. Since \( |C| < \infty \), we have \( \rho_s^g = 1 \) for some positive integer \( g \), so that \( \lambda_s \) is a root of unity. Thus \( |\chi(s)| = |\lambda_s n| = n \).

(b) \( \sum_{s \in C} |\chi(s)|^2 \leq \sum_{s \in G} |\chi(s)|^2 = g \). By (a), \( cn^2 \leq g \) so \( n^2 \leq g/c \).

(c) \( C \) is an abelian subgroup of \( G \). If \( \rho_s \neq 1 \) for \( s \neq 1 \), then \( \lambda_s \neq 1 \). So \( \lambda_s \neq \lambda_t \) for \( s \neq t \). Moreover \( \lambda_s^c = 1 \) implies \( \lambda_s \) is a \( c \)-th root of unity. It follows that the elements of \( C \) corresponds to distinct roots of unity, compatible with the group structure under multiplication, so \( C \simeq \mathbb{Z}/c\mathbb{Z} \).