MAT 452: Introduction to Algebra II
Spring 2011, Final Exam, Answers

Stefan Kohl

Answer to Question 1:

1. $(1,2,3) \cdot (2,3,4) = (1,3)(2,4)$.
2. $(1,2,3,4)^{(1,2,3,4,5)} = (2,3,4,5)$.
3. $\mathrm{ord}((1,2,3)(4,5,6,7)) = \mathrm{lcm}(3,4) = 12$.
4. $\mathrm{sgn}((1,2)(3,4,5)) = -1$.
5. $|\langle(1,2,3,4),(1,3)\rangle| = |\mathrm{D}_4| = 8$.
6. $[\mathrm{S}_4 : \langle(1,2)(3,4)\rangle] = 24/2 = 12$.

Answer to Question 2:

1. The product of two units is again a unit: if $a, b \in R$ are units, we have $b^{-1}a^{-1}ab = 1$, thus ab is a unit as well.
2. The sum of two units of a ring is not always a unit – for example 1 and -1 are units in $\mathbb{Z}$, but $-1 + 1 = 0$ is not a unit.
3. The set of units of a ring does not form a subring, due to (2.).
4. The set of units of a ring does not form an ideal, due to (2.).
5. There is no ring in which the units form a subring or an ideal, since every subring and every ideal contains 0, which is not a unit.
6. It is not true that every element of a ring can be written as a sum of 4 units – for example, expressing an element $n \in \mathbb{Z}$ requires at least $|n|$ summands ± 1.

Answer to Question 3:

1. $|U(\mathbb{Z}^{2\times 2})| = |\,\mathrm{GL}(2,\mathbb{Z})| = \infty$.
2. $|U(\mathbb{F}_{5^3})| = |\,\mathbb{F}_{5^3} \setminus \{0\}| = 5^3 - 1 = 124$.
3. The number of subfields of $\mathbb{F}_{2^{24}}$ is the number of divisors of 24, thus 8.
4. The minimal polynomial of $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$ is $x^4 - 16x^2 + 4$.
5. The nontrivial Galois automorphism of the extension field $\mathbb{Q}[\sqrt{3}]$ of $\mathbb{Q}$ interchanges $a + b\sqrt{3}$ and $a - b\sqrt{3}$, for all $a, b \in \mathbb{Q}$.
6. The isomorphism type of the Galois group of the polynomial $x^3 - 7x - 7$ is $\mathrm{A}_3 \cong \mathrm{C}_3$, since it is irreducible and its discriminant is $4 \cdot 7^3 - 27 \cdot 7^2 = 49$, which is a square in $\mathbb{Q}$.

Answer to Question 4: For any $a, b \in \mathbb{Q}$ put

$$M(a,b) := \begin{pmatrix} a+b & 4b \\ -b & a-b \end{pmatrix}.$$

Then we have:

1. $0 = M(0,0) \in R$.
2. $1 = M(1,0) \in R$.
3. $$\begin{aligned} \forall (a,b),(c,d) \in \mathbb{Q}^2 \quad & M(a,b) + M(c,d) \\ &= M(c,d) + M(a,b) \;=\; M(a+c, b+d) \in R. \end{aligned}$$
4. $\forall (a,b) \in \mathbb{Q}^2 \quad -M(a,b) = M(-a,-b) \in R$.
5. $$\begin{aligned} \forall (a,b),(c,d) \in \mathbb{Q}^2 \quad & M(a,b) \cdot M(c,d) \\ &= M(c,d) \cdot M(a,b) \;=\; M(ac - 3bd, ad + bc) \in R. \end{aligned}$$
6. $\forall (a,b) \in \mathbb{Q}^2 \setminus \{(0,0)\} \quad M(a,b)^{-1} = M(a/(a^2+3b^2), -b/(a^2+3b^2)) \in R$.

Therefore R is a subring of $\mathbb{Q}^{2\times 2}$, and it is also a field.