MATH5725: Galois Theory (2014, S2) Revision Problem Set

You should know the meaning of the following terms: ring, field, field extension, finite field extension, algebraic field extension, ideal, prime ideal, maximal ideal, quotient ring, domain, unique factorisation domain, Euclidean domain, group, normal subgroup, quotient group, group homomorphism, ring homomorphism.

A. True or False Questions Write down which of the following statements are true and which are false:

1. If $f : G \longrightarrow H$ be an injective group homomorphism, then $\ker(f) = 1$ (the trivial the group).

2. If G is a finite group with $n > 1$ elements then if $x \in G$ satisfies $x^n = 1$ then $x = 1$ (the identity).

3. If $f : G \longrightarrow H$ is a group homomorphism then $\ker(f)$ is not a normal subgroup of G.

4. If $f : G \longrightarrow H$ is a group homomorphism then $\mathrm{Im}(f)$ is a normal subgroup of H.

5. If $f : G \longrightarrow H$ is a surjective group homomorphism then $\mathrm{Im}(f) = H$.

6. The rings $\mathbf{Q}[X]/(X^2 - 2)$ and $\mathbf{Q}(\sqrt{2})$ are not isomorphic.

7. If k is a field and $f : \mathbf{Z} \longrightarrow k$ is a ring homomorphism, $\ker(f) = 0$ or $\ker(f) = \mathbf{Z}/(p)$ for some prime number p. (Recall that $f(1) = 1_k$).

8. If R is a domain and $f : \mathbf{Z} \longrightarrow R$ is a ring homomorphism then $\ker(f) = (ab)$ with $a, b > 1$.

9. If R is a unique factorisation domain then $R[X]$ is a unique factorisation domain.

10. If k is a field then $k[X]$ is a unique factorisation domain.

11. If k is a field and $f \in k[X]$ is irreducible then $k[X]/(f)$ is a field.

12. If k is a field and $f, g \in k[X]$ have degree greater than 1 then $k[X]/(fg)$ is a domain.

13. If R is a ring there are at most 2 different ring homomorphisms from $\mathbf{Z}$ to R.

14. The ring $\mathbf{Z}[X]/(X^2 + 1, 3)$ has exactly 9 elements.

15. The ring $\mathbf{Z}[X]/(X^2 + 1, 5)$ is a domain.

16. The field extension $\mathbf{Q}(\pi)/\mathbf{Q}$ is algebraic.

17. If R is a ring and $\mathfrak{p} \subset R$ is a prime ideal then $R/\mathfrak{p}$ is a field.

18. If R is a ring and $\mathfrak{m} \subset R$ is a maximal ideal then $R/\mathfrak{m}$ is a domain.

19. If G is a group with 6 elements then it is commutative.

20. If G is a group with 4 elements then it is isomorphic to $\mathbf{Z}/(4)$.

21. If K/k is a field extension $\alpha \in K$ and $f \in k[X]$ is irreducible and $f(\alpha) = 0$ then if $g \in k[X]$ satisfies $g(\alpha) = 0$ then $f \mid g$.

22. Let $\sqrt[3]{2} \in \mathbf{R}$ be a real zero of $X^3 - 2$. The rings $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\sqrt[3]{2}e^{2\pi i/3})$ are isomorphic.

B. Longer answer questions

1. What form do the ideals of the ring $\mathbf{Z}$ have? What about the ring $\mathbf{Q}[X]$?

2. When is an ideal $I \subset \mathbf{Q}[X]$ prime? If it is prime, is it maximal? (You may assume that all ideals of $\mathbf{Q}[X]$ are generated by one element).

3. Let $\alpha \in \mathbf{C}$ be the solution of a polynomial $f(X) \in \mathbf{Q}[X]$. Let $g(X) \in \mathbf{Q}[X]$ be such that $g(\alpha) \neq 0$. Prove that you can always "rationalise the denominator" of $1/g(\alpha)$. (Hint: what is the greatest common divisor of $f(X)$ and $g(X)$ in $\mathbf{Q}[X]$? Can you write down a simple expression for it, for example, by using the Euclidean algorithm.)

4. Let $\alpha \in \mathbf{C}$; show that $\mathbf{Q}[\alpha]$ is a domain; show that it is a field if and only if there is a polynomial $f \in \mathbf{Q}[X]$ such that $f(\alpha) = 0$.

5. Write down two examples of Euclidean domains.

6. Can you give an example of a non-abelian group with 8 elements? (Hint: consider the symmetries of the square, a.k.a., the dihedral group D_4). If so, can you give a second example of an non-abelian group with 8 elements?

7. Let G be a group and let $N, H \subset G$ be sub-groups such that $N.H = G$ and $N \cap H = 1$. Is it true that $G \cong N \times H$ as groups? If not, can you give a counter-example? (See question 2).

8. Let p be a prime and let $\mathbf{F}_p$ be the field with p elements (i.e. $\mathbf{F}_p \cong \mathbf{Z}/(p)$). Let $\mathrm{GL}_2(\mathbf{F}_p)$ be the set of all 2×2 matrices with entries in $\mathbf{F}_p$ which have an inverse under multiplication? What is the cardinality of $\mathrm{GL}_2(\mathbf{F}_p)$?

9. Let G be a group and let N, H be subgroups of G. Is $H \cap N$ a subgroup of G? If N is normal, is $H \cap N$ a normal subgroup of G? Is it a normal subgroup of either H or N?

10. Let K/k be an algebraic field extension and let $\alpha \in K$ and let $f \in k[X]$ be a minimal degree polynomial such that $f(\alpha) = 0$. Show that f is irreducible and unique up to multiplication by an element of k^*. (Hint: use the fact that for any two polynomials f, g different from 0 there exist unique polynomials q and r such that $f = gq + r$ and the degree or r is less than that of g).